CHAPTER 7
INSTRUMENTATION AND CONTROLS
CONTENTS

		Page
7.1	INTRODUCTION	7.1-1
7.1.1	IDENTIFICATION OF SAFETY-RELATED SYSTEMS	7.1-1
7.1.1.1	Protection System	7.1-1
7.1.1.2	Reactor Trip System	7.1-2
7.1.1.3	Engineered Safety Feature Systems	7.1-3
7.1.1.4	Systems Required for Safe Shutdown	7.1-3
7.1.1.5	Safety-Related Display Instrumentation	7.1-5
7.1.1.6	All Other Systems Required for Safety	7.1-5
7.1.1.7	Design Comparison	7.1-6
7.1.2	IDENTIFICATION OF SAFETY CRITERIA	7.1-7
7.1.2.1	Design Bases	7.1-8
7.1.2.2	Conformance to IEEE 279	7.1-9
7.1.2.3	Conformance to IEEE 308	7.1-9
7.1.2.4	Conformance to IEEE 317	7.1-10
7.1.2.5	Conformance to IEEE 323	7.1-10
7.1.2.6	Conformance to IEEE 336 as Augmented by Regulatory Guide 1.30	7.1-10
7.1.2.7	Conformance to IEEE 338	7.1-10
7.1.2.8	Conformance to IEEE 344	7.1-11
7.1.2.9	Conformance to IEEE 379 as Augmented by Regulatory Guide 1.53	7.1-11

CONTENTS (cont)

		Page
7.1.2.10	Conformance to IEEE 384 as Augmented by Regulatory Guide 1.75	7.1-12
7.1.2.11	Conformance to IEEE 387	7.1-14
7.1.2.12	Conformance to IEEE 450	7.1-14
7.1.2.13	Comparison of Design with Regulatory Guide 1.6	7.1-14
7.1.2.14	Comparison of Design with Regulatory Guide 1.11	7.1-14
7.1.2.15	Conformance to Regulatory Guide 1.22	7.1-15
7.1.2.16	Conformance to Regulatory Guide 1.29	7.1-16
7.1.2.17	Conformance to Regulatory Guide 1.30	7.1-17
7.1.2.18	Conformance to Regulatory Guide 1.40	7.1-17
7.1.2.19	Conformance to Regulatory Guide 1.47	7.1-17
7.1.2.20	Conformance to Regulatory Guide 1.53	7.1-20
7.1.2.21	Conformance to Regulatory Guide 1.62	7.1-20
7.1.2.22	Conformance to Regulatory Guide 1.63	7.1-21
7.1.2.23	Conformance to Regulatory Guide 1.68	7.1-21
7.1.2.24	Conformance to Regulatory Guide 1.73	7.1-21
7.1.2.25	Conformance to Regulatory Guide 1.75	7.1-21
7.1.2.26	Conformance to Regulatory Guide 1.80	7.1-22
7.1.2.27	Conformance to Regulatory Guide 1.89, Revision 1	7.1-22
7.1.2.28	Conformance to Regulatory Guide 1.95	7.1-22

CONTENTS (cont)

		Page
7.1.2.29	Conformance to Regulatory Guide 1.97	7.1-22
7.1.2.30	Conformance to Regulatory Guide 1.100	7.1-22
7.1.2.31	Conformance to Regulatory Guide 1.105	7.1-22
7.1.2.32	Conformance to Regulatory Guide 1.118	7.1-22
7.1.2.33	Evaluation of IE Bulletin 79-27	7.1-23
7.1.2.34	Evaluation of IE Bulletin 80-06	7.1-32
7.1.2.35	Evaluation of IE Information Notice 79-22	7.1-38
7.1.3	CESSAR INTERFACES	7.1-40
7.1.3.1	Power	7.1-40
7.1.3.2	Protection from Natural Phenomena	7.1-40
7.1.3.3	Protection from Pipe Failure	7.1-41
7.1.3.4	Missiles	7.1-41
7.1.3.5	Separation	7.1-41
7.1.3.6	Independence	7.1-42
7.1.3.7	Thermal Limitations	7.1-42
7.1.3.8	Monitoring	7.1-42
7.1.3.9	Operational Controls	7.1-43
7.1.3.10	Inspection and Testing	7.1-43
7.1.3.11	Chemistry/Sampling	7.1-43
7.1.3.12	Materials	7.1-43
7.1.3.13	System Component Arrangement	7.1-43
7.1.3.14	Radiological Waste	7.1-44

CONTENTS (cont)

		Page
7.1.3.15	Overpressure Protection	7.1-44
7.1.3.16	Related Services	7.1-44
7.1.3.17	Environmental	7.1-46
7.1.3.18	Mechanical Interaction	7.1-46
7.1.3.19	Plant Monitoring System Inputs	7.1-46
7.1.4	CESSAR INTERFACE EVALUATIONS	7.1-46
7.1.4.1	Power	7.1-46
7.1.4.2	Protection from Natural Phenomena	7.1-47
7.1.4.3	Protection from Pipe Failure	7.1-47
7.1.4.4	Missiles	7.1-47
7.1.4.5	Separation	7.1-47
7.1.4.6	Independence	7.1-47
7.1.4.7	Thermal Limitations	7.1-47
7.1.4.8	Monitoring	7.1-48
7.1.4.9	Operational Controls	7.1-48
7.1.4.10	Inspecting and Testing	7.1-48
7.1.4.11	Chemistry/Sampling	7.1-48
7.1.4.12	Materials	7.1-48
7.1.4.13	System Component Arrangement	7.1-49
7.1.4.14	Radiological Waste	7.1-49
7.1.4.15	Overpressure Protection	7.1-49
7.1.4.16	Related Services	7.1-49

CONTENTS (cont)

		Page
7.1.4.17	Environmental	7.1-49
7.1.4.18	Mechanical Interaction	7.1-50
7.1.4.19	Plant Monitoring System Inputs	7.1-50
7.1.5	REFERENCES	7.1.51
7.2	REACTOR PROTECTIVE SYSTEM	7.2-1
7.2.1	DESCRIPTION	7.2-1
7.2.1.1	System Description	7.2-1
7.2.1.2	Design Bases	7.2-38
7.2.1.3	Final System Drawings	7.2-41
7.2.2	ANALYSIS	7.2-45
7.2.2.1	Introduction	7.2-45
7.2.2.2	Trip Bases	7.2-50
7.2.2.3	Design	7.2-55
7.2.2.4	Failure Modes and Effects Analysis (FMEA)	7.2-201
7.2.3	REACTOR PROTECTIVE SYSTEM INTERFACE REQUIREMENTS	7.2-206
7.2.3.1	Power	7.2-206
7.2.3.2	Protection From Natural Phenomena	7.2-206
7.2.3.3	Protection From Pipe Failure	7.2-206
7.2.3.4	Missiles	7.2-206
7.2.3.5	Separation	7.2-206
7.2.3.6	Independence	7.2-207
7.2.3.7	Thermal Limitations	7.2-207

CONTENTS (cont)

		Page
7.2.3.8	Monitoring	7.2-207
7.2.3.9	Operational/Controls	7.2-207
7.2.3.10	Inspection and Testing	7.2-207
7.2.3.11	Chemistry/Sampling	7.2-207
7.2.3.12	Materials	7.2-207
7.2.3.13	System Component Arrangement	7.2-208
7.2.3.14	Radiological Waste	7.2-208
7.2.3.15	Overpressure Protection	7.2-208
7.2.3.16	Related Services	7.2-208
7.2.3.17	Environmental	7.2-208
7.2.3.18	Mechanical Interaction	7.2-208
7.2.4	REACTOR PROTECTIVE SYSTEM INTERFACE EVALUATION	7.2-208
7.2.4.1	Power	7.2-208
7.2.4.2	Protection From Natural Phenomena	7.2-209
7.2.4.3	Protection From Pipe Failure	7.2-209
7.2.4.4	Missiles	7.2-209
7.2.4.5	Separation	7.2-209
7.2.4.6	Independence	7.2-209
7.2.4.7	Thermal Limitations	7.2-209
7.2.4.8	Monitoring	7.2-209
7.2.4.9	Operational/Controls	7.2-210

CONTENTS (cont)

		Page
7.2.4.10	Inspection and Testing	7.2-210
7.2.4.11	Chemistry/Sampling	7.2-210
7.2.4.12	Materials	7.2-210
7.2.4.13	System Component Arrangement	7.2-210
7.2.4.14	Radiological Waste	7.2-210
7.2.4.15	Overpressure Protection	7.2-210
7.2.4.16	Related Services	7.2-210
7.2.4.17	Environmental	7.2-211
7.2.4.18	Mechanical Interaction	7.2-211
7.2.5	SUPPLEMENTARY PROTECTION SYSTEM	7.2-211
7.2.5.1	Functional Description of the SPLA	7.2-212
7.2.5.2	Supplementary Protection System (SPS) Diversity to the Reactor Protective System (RPS)	7.2-216
7.2.6	REFERENCES	7.2-218
7.3	ENGINEERED SAFETY FEATURE SYSTEMS	7.3-1
7.3.1	DESCRIPTION	7.3-1
7.3.1.1	NSSS Engineered Safety Features Actuation System (ESFAS)	7.3-3
7.3.1.2	Design Basis Information	7.3-53
7.3.1.3	Final System Drawings	7.3-64
7.3.1.4	Engineered Safety Features Actuation System Supporting Systems	7.3-64

CONTENTS (cont)

		Page
7.3.2	ANALYSIS	7.3-65
7.3.2.1	Introduction	7.3-65
7.3.2.2	Actuation Bases	7.3-68
7.3.2.3	Design	7.3-71
7.3.2.4	Failure Modes and Effects Analysis	7.3-99
7.3.3	CESSAR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM INTERFACE REQUIREMENTS	7.3-99
7.3.3.1	Power	7.3-99
7.3.3.2	Protection from Natural Phenomena	7.3-99
7.3.3.3	Protection from Pipe Failure	7.3-99
7.3.3.4	Missiles	7.3-101
7.3.3.5	Separation	7.3-101
7.3.3.6	Independence	7.3-101
7.3.3.7	Thermal Limitations	7.3-101
7.3.3.8	Monitoring	7.3-101
7.3.3.9	Operational/Controls	7.3-101
7.3.3.10	Inspection and Testing	7.3-101
7.3.3.11	Chemistry/Sampling	7.3-101
7.3.3.12	Materials	7.3-101
7.3.3.13	System Component Arrangement	7.3-102
7.3.3.14	Radiological Waste	7.3-102
7.3.3.15	Overpressure Protection	7.3-102

CONTENTS (cont)

		Page
7.3.3.16	Related Services	7.3-102
7.3.3.17	Environmental	7.3-102
7.3.3.18	Mechanical Interaction	7.3-102
7.3.3.19	Plant Monitoring System Inputs	7.3-102
7.3.4	CESSAR INTERFACE EVALUATION	7.3-102
7.3.4.1	Power	7.3-102
7.3.4.2	Protection from Natural Phenomena	7.3-103
7.3.4.3	Protection from Pipe Failure	7.3-103
7.3.4.4	Missiles	7.3-103
7.3.4.5	Separation	7.3-103
7.3.4.6	Independence	7.3-103
7.3.4.7	Thermal Limitations	7.3-103
7.3.4.8	Monitoring	7.3-103
7.3.4.9	Operational/Controls	7.3-103
7.3.4.10	Inspection and Testing	7.3-103
7.3.4.11	Chemistry/Sampling	7.3-104
7.3.4.12	Materials	7.3-104
7.3.4.13	System Component Arrangement	7.3-104
7.3.4.14	Radiological Waste	7.3-104
7.3.4.15	Overpressure Protection	7.3-104
7.3.4.16	Related Services	7.3-104
7.3.4.17	Environmental	7.3-104

CONTENTS (cont)

		Page
7.3.4.18	Mechanical Interaction	7.3-104
7.3.4.19	Plant Monitoring System Inputs	7.3-104
7.3.5	DIVERSE AUXILIARY FEEDWATER ACTUATION SYSTEM (DAFAS)	7.3-105
7.3.5.1	Design Bases and Design Considerations	7.3-105
7.3.5.2	Functional Description of the DAFAS	7.3-116
7.3.5.3	DAFAS Diversity From Existing Reactor Protective System	7.3-121
7.3.5.4	Failure Modes and Effects	7.3-121
7.3.6	REFERENCES	7.3-125
7.4	SYSTEMS REQUIRED FOR SAFE SHUTDOWN	7.4-1
7.4.1	DESCRIPTION	7.4-1
7.4.1.1	System Description	7.4-2
7.4.1.2	Design Basis Information	7.4-16
7.4.1.3	Final System Drawings	7.4-16
7.4.2	ANALYSIS	7.4-16
7.4.2.1	Conformance to IEEE 279-1971	7.4-16
7.4.2.2	Conformance to IEEE 308-1971	7.4-20
7.4.2.3	Conformance to General Design Criterion 19	7.4-20
7.4.2.4	Consideration of Selected Plant Contingencies	7.4-21

CONTENTS (cont)

		Page
7.4.2.5	Emergency Shutdown from Outside the Control Room	7.4-21
7.5	SAFETY-RELATED DISPLAY INSTRUMENTATION	7.5-1
7.5.1	DESCRIPTION	7.5-1
7.5.1.1	System Description	7.5-2
7.5.2	ANALYSIS	7.5-21
7.5.2.1	Analysis of Safety-Related Plant Process Display Instrumentation	7.5-21
7.5.2.2	Analysis of Reactor Trip System Monitoring	7.5-22
7.5.2.3	Analysis of Engineered Safety Features Monitoring	7.5-23
7.5.2.4	Analysis of CEA Position Indication	7.5-24
7.5.2.5	Analysis of Post-Accident Monitoring Instrumentation	7.5-25
7.5.2.6	Analysis of Automatic Bypass Indication on a System Level	7.5-30
7.5.3	REFERENCES	7.5.32
7.6	ALL OTHER INSTRUMENTATION SYSTEMS REQUIRED FOR SAFETY	7.6-1
7.6.1	INTRODUCTION	7.6-1
7.6.1.1	System Descriptions	7.6-2
7.6.1.2	Design Bases	7.6-10
7.6.1.3	Final System Drawings	7.6-11
7.6.2	ANALYSIS	7.6-12

CONTENTS (cont)

		Page
7.6.2.1	Analysis of Design Criteria	7.6-12
7.6.2.2	Analysis of Equipment Design Criteria	7.6-14
7.6.2.3	Fire Protection Instrumentation and Detection System	7.6-21
7.7	CONTROL SYSTEMS NOT REQUIRED FOR SAFETY	7.7-1
7.7.1	DESCRIPTION	7.7-1
7.7.1.1	Control Systems	7.7-2
7.7.1.2	Design Comparison	7.7-19
7.7.1.3	Monitoring Systems	7.7-23
7.7.2	ANALYSIS	7.7-43
7.7.3	REFERENCES	7.7-44
APPENDIX 7A	RESPONSE TO NRC REQUESTS FOR INFORMATION	

TABLES

		Page
7.1-1	Deleted	7.1-28
7.1-2	Instrument Parameters and Controls Required to Achieve Cold Shutdown	7.1-29
7.1-3	Identification of Actuated Devices Which Change Position on Reset of ESF Actuation Signal	7.1-34
7.2-1	Reactor Protective System Design Inputs	7.2-3
7.2-1A	Core Protection Calculator System Additional Trip Functions	7.2-9
7.2-2	Reactor Protective System Bypasses	7.2-6
7.2-3	Reactor Protective System Sensors	7.2-15
7.2-4	Reactor Protective System Monitored Plant Variable Ranges	7.2-16
7.2-4AA	Reactor Protective Instrumentation Response Times	7.2-43
7.2-4A	Plant Protection System Failure Modes and Effects Analysis	7.2-60
7.2-5	Control Systems Considered to Have Potential Impacts Upon Plant Safety Due to Common Power Source or Common Sensor Failures	7.2-197
7.2-6	Control Systems Sharing a Common Sensor or Common Instrument Tap	7.2-200
7.3-1	One-Out-of-Two ESFAS Bypasses	7.3-12
7.3-1A	DAFAS Bypasses	7.3-13
7.3-1B	Engineered Safety Features Response Times	7.3-25

TABLES (cont)

		Page
7.3-1C	NSSS ESFAS Bypasses	7-3-28
7.3-2	Design Basis Events Requiring ESF System Action	7.3-29
7.3-3	Monitored Variables for ESF System Protective Action	7.3-31
7.3-3a	Engineered Safety Features Actuation System Plant Variable Ranges	7.3-33
7.3-4	Containment Spray Actuation Signal Actuated Devices List	7.3-34
7.3-5	Recirculation Actuation Signal Actuated Devices List	7.3-35
7.3-6	Safety Injection Actuation Signal Actuated Devices List	7.3-39
7.3-7	Auxiliary Feedwater Actuation Signal Actuated Devices List	7.3-42
7.3-8	Fuel Building Essential Ventilation Actuation Signal Actuated Devices List	7.3-45
7.3-9	Control Room Essential Filtration Actuation Signal Actuated Devices List	7.3-50
7.3-10	Control Room Ventilation Isolation Actuation Signal Actuated Devices List	7.3-51
7.3-11	Containment Combustible Gas Control System Actuated Devices List	7.3-54
7.3-11A	Engineered Safety Features Actuation System Setpoints and Margins to Actuation	7.3-55

TABLES (cont)

		Page
7.3-12	BOP ESF System Actuation Setpoints and Margins to Actuation	7.3-56
7.3-13A	BOP ESF Systems Actuation Sensors	7.3-59
7.3-13B	NSSS Engineered Safety Features Actuation System Sensors	7.3-60
7.3-14	One-Out-of-Two ESFAS Fuel Building Essential Ventilation Actuation Signal Failure Modes and Effects Analysis	7.3-84
7.3-15	One-Out-of-Two ESFAS Containment Purge Isolation Actuation Signal Failure Modes and Effects Analysis	7.3-87
7.3-16	One-Out-of-Two ESFAS Control Room Ventilation Isolation Actuation Signal Failure Modes and Effects Analysis	7.3-90
7.3-17	One-Out-of-Two ESFAS Control Room Essential Filtration Actuation Signal Failure Modes and Effects Analysis	7.3-93
7.3-18	Failure Modes and Effects Analysis Containment Combustible Gas Control System	7.3-100
7.4-1	Remote Shutdown Panel Instrumentation and Controls	7.4-14

TABLES (cont)

		Page
7.5-1	Engineered Safety Feature System Monitoring	7.5-10
7.5-2	Safety Related Plant Process Display Instrumentation	7.5-17
7.6-1	Shutdown Cooling (SDC) System and Safety Injection Tank (SIT) Interlocks	7.6-7
7.7-1	COLSS Monitored Plant Variables	7.7-32

FIGURES

7.1-1 HELBA Process

7.2-0 Typical Low Reactor Coolant Flow Trip Setpoint Operation

7.2-0A Typical Measurement Channel Functional Diagram (Pressurizer Pressure Wide Range)

7.2-0B Reed Switch Position Transmitter Assembly Schematic Diagram

7.2-0C Reed Switch Position Transmitter Cable Assemblies

7.2-0D CEA Position Signals Within Reactor Protective System

7.2-0E Excore Neutron Flux Monitoring System

7.2-0F Reactor Coolant Pump Speed Sensors Typical for Each Reactor Coolant Pump

7.2-0G Core Protection Calculator Functional Block Diagram

7.2-1 Instrument Location Layout for Plant Protection System Containment Building Between El. 120’-0” and El. 140’-0”

7.2-2 Instrument Location Layout for Plant Protection System Containment Building at El. 100’-0’

7.2-3 Instrument Location Layout for Plant Protection System Containment Building Between El. 40’-0” and El. 100’-0”

7.2-4 Deleted

7.2-5 SPLA Functional Block Diagram

7.2-6 Bistable Block Diagram

FIGURES (cont)

7.2-7 Basic PPS Testing System (Shown for Reactor Protective System)

7.2-8 Plant Protection System Simplified Functional Diagram

7.2-9 Matrix, Bistable Trip and Log Trip Interlock Ckt.

7.2-10 Typical Trip Channel Bypass

7.2-11 Plant Protection System Interface Logic Diagram

7.2-12 Simplified P.P.S Cabinet Layout (Rear View)

7.2-13 Typical PPS Bay Layout

7.2-14 Auxiliary Relay Cabinet A (Front View)

7.3-1 ESFAS Signal Logic

7.3-2 ESFAS Signal Logic

7.3-3 One-Out-of-Two ESFAS Logic

7.3-4 ESF Component Control Logic

7.3-5 ESF Component Control Logic

7.3-6 Containment Combustible Gas Control System Device Control Logic

7.3-7a ESFAS Signal Logic (SIAS)

7.3-7b ESFAS Signal Logic (CSAS, CIAS, RAS)

7.3-7c ESFAS Signal Logic (MSIS)

7.3-7d ESFAS Signal Logic (EFAS 1, EFAS 2)

7.3-7e DAFAS Block Diagram

FIGURES (cont)

7.3-7f DAFAS Logic Diagram

7.3-8a ESFAS Auxiliary Relay Cabinet Schematic Diagram for Typical Actuation Signal

7.3-8b ESFAS Auxiliary Relay Cabinet Schematic Diagram for the EFAS

7.3-9a Reactor Protective System Simplified Functional Logic Diagram

7.3-9b Simplified Functional Diagram of the Reactor Protective System

7.3-9c Plant Protection System 2/4 Logic Matrix

7.3-10 Function Diagram of a Typical Engineering Safety Feature Actuation

7.3-11a Control Circuit for a Solenoid Actuated, Air Operated Valve

7.3-11b Control Circuit for a Motor Operated Valve

7.3-11c Control Circuit for a Pump Motor

7.4-1 Control Logic Diagram Diesel Generator Fuel Oil Transfer Pumps

7.4-2 Control Logic Diagram Essential Spray Pond Pumps

7.4-3 Control Logic Diagram Essential Cooling Water Pumps

7.4-4 Control Logic Diagram Auxiliary Feedwater Pump B

7.4-5 Control Logic Diagram Override Mode as Applied to ESFAS Control

7.4-6 Control Logic Diagram – Shutdown Cooling System

FIGURES (cont)

7.5-1 Main Control Room and Computer Room Arrangement

7.5-2 Safety Equipment Status System Control Panel

7.6-1 Safety Related Interlock Logic Circuit

7.6-2 Safety Injection Tank Isolation Valve Interlocks

7.7-1 Feedwater Control System Block Diagram

7.7-2 Steam Bypass Control System Block Diagram

7.7-3 Functional Diagram of the Core Operating Limit Supervisory System

7.7-4 RPCS Block Diagram

7.7-5 Reactor Regulating System

7.7-6 CEDMCS – RPS Interface Block Diagram

7.7-7 Pressurizer Pressure Control System Block Diagram

7.7-8 Pressurizer Level Control System Block Diagram

7.7-9 Reactor Power Cutback System Simplified Block Diagram

7.7-10 Deleted

7.7-11 Boron Dilution Alarm System Simplified Block Diagram

7. INSTRUMENTATION AND CONTROLS

7.1 INTRODUCTION

Instrumentation and control systems that monitor and perform safety-related functions are discussed in this chapter. Complete descriptions and analyses of these systems are provided in sections 7.2 through 7.6. Systems that are not required for safety are discussed in section 7.7.

7.1.1 IDENTIFICATION OF SAFETY-RELATED SYSTEMS

The safety-related instrumentation and controls, including supporting systems, are identified below. The responsibility for the design of each system is identified as follows:

Combustion Engineering (C-E)/Westinghouse Electric Company LLC

Bechtel (Bechtel)

Identification of supplier/builder not identified below can be found in table 1.9-1.

7.1.1.1 Protection System

The PPS includes the electrical and mechanical devices and circuitry required to perform the protective functions defined below.

A. Reactor Protective System (RPS)

The RPS is the portion of the PPS that acts to trip the reactor when required. The RPS is described in section 7.2.

B. Engineered Safety Features Actuation System (ESFAS)

The ESFAS is the portion of the PPS which activates the Engineered Safety Features Systems listed in section 7.1.1.3 and described in section 7.3.

C Supplementary Protection System (SPS)

The Supplementary Protection System (SPS) augments reactor protection by utilizing a separate and diverse trip logic from the Reactor Protective System for initiation of reactor trip. The addition of the SPS provides a simple, reliable, yet diverse mechanism to initiate a reactor trip. The SPS will initiate a reactor trip when pressurizer pressure exceeds a predetermined value.

The SPS is provided with sensors and circuitry which are diverse from those of the RPS. A selective two-out-of-four logic to interrupt the power supplied to the CEDM's and thereby cause the CEA's to drop into the core by gravity is used. The system is independent and separate from all control systems.

7.1.1.2 Reactor Trip System

The RTS includes the RPS portion of the PPS, Reactor Trip Switchgear System (RTSS) and the arrangement of components that perform a reactor trip after receiving a signal from the RPS or SPS automatically or manually by the operator. The RTS initiates a reactor trip based on the signals from the sensors which monitor various NSSS parameters and the containment pressure.

7.1.1.3 Engineered Safety Feature Systems

The ESF Systems include the NSSS and BOP ESFAS and the arrangement of components that perform protective actions after receiving a signal from the NSSS or BOP ESFAS or the operator. The instrumentation and controls for ESF Systems are described in section 7.3.

The NSSS ESF Systems are:

A. Containment Isolation System; (C-E)/(Bechtel)

B. Main Steam Isolation System; (Bechtel)

C. Safety Injection System; (C-E)

D. Auxiliary Feedwater System; (Bechtel)

E. Containment Spray System; (C-E)

F. Supporting Systems. (Bechtel)

The BOP ESF Systems are:

A. Fuel building essential ventilation system

B. Containment purge isolation system

C. Control room essential filtration system

D. Control room essential ventilation system

E. Containment combustible gas control system (manual)

7.1.1.4 Systems Required for Safe Shutdown

Systems required for safe shutdown are defined as those essential for pressure and reactivity control, coolant inventory makeup, and removal of residual heat once the reactor has been brought to a subcritical condition. These systems are categorized according to the following shutdown modes:

A. Hot Shutdown

Systems required for maintenance of the primary system at, or near, operating temperature and pressure.

B. Cold Shutdown

Systems required to cool down and maintain the primary system at or near ambient conditions.

The systems required for safe shutdown are listed below and described in section 7.4.

The safe shutdown systems required to place the reactor in hot shutdown include:

1. Diesel Generator; (Bechtel)
2. Diesel Generator Fuel Storage and Transfer System; (Bechtel)
3. Class 1E AC System; (Bechtel)
4. Emergency Power Distribution System; (Bechtel)
5. Auxiliary Feedwater System; (Bechtel)
6. Atmospheric Steam Dump System; (Bechtel)
7. Chemical and Volume Control System (portions only, see section 9.3.4) (C-E)
8. Essential Spray Pond System; and (Bechtel)
9. Condensate Storage System (Bechtel)

In addition, equipment and systems are provided to allow emergency shutdown from outside the control room.

The safe shutdown systems or portions of systems required to place the reactor in cold shutdown include those in 1. through 9. above, plus the following:

10. Nuclear Cooling Water System; (Bechtel)
11. Essential Cooling Water System; (Bechtel)
12. Shutdown Cooling System. (C-E)

7.1.1.5 Safety-Related Display Instrumentation

The Safety-Related Display Instrumentation provides information to the operator to allow him to adequately monitor plant operating conditions and to perform any required manual safety functions. Safety-Related Display Instrumentation is described in section 7.5.

Safety-related displays are provided for:

A. Safety-Related Plant Process Display Instrumentation; (C-E)/(Bechtel)
B. Reactor Trip System Monitoring; (C-E)
C. Engineered Safety Features Systems Monitoring; (C-E)/(Bechtel)
D. CEA Position Indication; (C-E)/(Bechtel)
E. Post-Accident Monitoring; and (C-E)/(Bechtel)
F. Automatic Bypass Indication. (Bechtel)

7.1.1.6 All Other Systems Required for Safety

Other systems required for safety include the interlocks required to prevent overpressurization of the Shutdown Cooling System and to ensure safety injection availability. These are provided as listed below and described in section 7.6.

A. Shutdown Cooling System Suction Line Isolation Valve Interlocks; and (C-E)

B. Safety Injection Tank Isolation Valve Interlocks. (C-E)

7.1.1.7 Design Comparison

The Reactor Protective System (RPS) is designed by Combustion Engineering. The system will be functionally identical to the system provided for the Arkansas Nuclear One - Unit 2 (ANO-2) plant (NRC Docket No. 50-368) with the following exceptions:

A. High Linear Power Level Trip is replaced by a Variable Overpower Trip. The Variable Overpower Trip provides protection to the NSSS for rapid power changes from low initial power levels.

B. The Reactor Trip Switchgear (RTSG), which had consisted of nine trip circuit breakers on ANO-2, is now four circuit breakers in a Reactor Trip Switchgear System (RTSS). The change to the RTSS was performed to implement the SPS requirements.

C. The Supplementary Protection System (SPS) is new to the CESSAR licensing scope. This system is specifically designed to increase the reliability of reactor trip initiation.

D. A low reactor coolant flow trip has been added to provide protection in the event of a reactor coolant pump sheared shaft.

The Engineered Safety Features Actuation System (ESFAS) is designed by Combustion Engineering. Each initiation system logic, including testing features, is similar to the logic for the RPS and is contained in the same physical enclosure. The

actuation logic and devices are contained in the ESFAS Auxiliary Relay Cabinets. The design of this system is described in section 7.3. The following changes from ANO-2 make the ESFAS more diverse and responsive to the situation requiring its actuation:

A. CIAS initiation logic now includes low pressurizer pressure;

B. MSIS initiation logic now includes high steam generator level and high containment pressure;

C. RAS has had manual initiation added;

D. AFAS initiation logic is modified by removing a steam generator low pressure permissive and by adding interlocks between AFAS-1 and AFAS-2.

Balance of Plant engineered safety features actuation systems (BOP ESFASs) designed to actuate ESF systems presented in paragraph 7.1.1.3 F, A through E employ one-out-of-two logic, described in section 7.3, as opposed to the two-out-of-four logic for this NSSS ESFAS.

7.1.2 IDENTIFICATION OF SAFETY CRITERIA

Comparison of the design with applicable Regulatory Guide recommendations and the degree of compliance with the appropriate design bases, General Design Criteria, standards, and other documents used in the design of the systems listed in Section 7.1.1 are described in Sections 7.1.2.1 through 7.1.2.35, and in each of the sections describing the system. (Refer to sections 7.2 through 7.6.)

7.1.2.1 Design Bases

The design bases for the safety-related instrumentation and control of each safety-related system are presented in the section of this chapter that discusses the system to which the information applies.

Consideration has been given to instrument error in the selection of all safety system setpoints. Where setpoints are listed in Chapter 7, it is understood that these are nominal values. The actual setpoint may vary within prescribed accuracies which have been considered in selection of the values.

7.1.2.1.1 Systems Required for Plant Protection

The instrumentation and controls for the Reactor Protective System and Engineered Safety Features Systems conform to the following:

A. The PPS and the ESF Systems conform to IEEE Standard 279-1971. Detailed discussion of conformance for these and other safety-related system instrumentation and controls is provided in the applicable section of this chapter. Conformance to the other IEEE Standards is discussed in sections 7.1.2.3 through 7.1.2.12.

B. Comparison with Regulatory Guide recommendations for Water-Cooled Nuclear Power Plants, Division of Reactor Standards, Nuclear Regulatory Commission, is discussed in sections 7.1.2.6, 7.1.2.9, 7.1.2.10, and 7.1.2.13 through 7.1.2.32.

C. Quality assurance procedures are described in CENPD-210A, "Description of the C-E Nuclear Steam Supply System Quality Assurance Program (Reference 1).

D. General Design Criteria for Nuclear Power Plants, Appendix A to 10CFR50, July 7, 1971, as described in section 3.1.

E. The standards the upgraded Core Protection Calculator System (CPCS) were designed to are described in CENPD-396-P, "Common Qualified Platform Topical Report"[4]. However, Palo Verde has not increased its commitments to these new or revised standards.

7.1.2.1.2 Systems Required for Safe Shutdown

The design bases for the systems required for safe shutdown are described in section 7.4.

7.1.2.1.3 Safety-Related Display Instrumentation

The design bases for Safety-Related Display Instrumentation are described in section 7.5.

7.1.2.1.4 All Other Systems Required for Safety

The design bases for all other systems required for safety are described in section 7.6.

7.1.2.2 Conformance to IEEE 279

Conformance to IEEE 279-1971, is discussed in paragraphs 7.1.2.1, 7.1.2.1.1, 7.2.1.2, 7.2.2.3.2, 7.3.1.2, 7.3.2.3.1, 7.3.2.3.2, 7.4.2.1, 7.5.2.5 and 7.6.2.1.

7.1.2.3 Conformance to IEEE 308

Conformance to IEEE 308-1974, is discussed in section 8.3.

7.1.2.4 Conformance to IEEE 317

Electric penetrations and their conformance to IEEE 317-1972 are discussed in section 8.3.

7.1.2.5 Conformance to IEEE 323

The CESSAR Licensing scope compliance with IEEE 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations", for instrumentation is discussed in Combustion Engineering Topical Report CENPD-255, "Qualification of Combustion Engineering Class 1E Instrumentation", (Reference 2). The basic qualification requirements of CESSAR Licensing scope equipment are discussed in section 3.11.

Qualification of Class IE electrical equipment not supplied by C-E, is discussed in sections 8.3 and 3.11.

7.1.2.6 Conformance to IEEE 336 as Augmented by Regulatory Guide 1.30

A planned quality assurance (QA) program, in compliance with IEEE 336-1971, has been implemented. This includes a comprehensive quality control and QA program.

7.1.2.7 Conformance to IEEE 338

The PPS and ESFAS Auxiliary Relay Cabinet circuits, as well as the RTSS, are designed so that they can be periodically tested in accordance with the criteria of IEEE 338-1971, "Periodic Testing of Nuclear Power Generating Station Protection Systems".

Testing criteria are specified in sections 7.2.2.3.3 and 7.3.2.3.3. Minimum testing frequency requirements are provided in the Technical Specifications.

Since operation of the ESF Systems is not expected, the systems are periodically tested to verify operability. Complete channels, in the NSSS ESFAS systems, can be individually tested without initiating protective action and without inhibiting the operation of the system.

The system can be checked from the sensor signal through the actuation devices. The functional modules in the sensors system can be tested during reactor operation. The sensors can be checked by comparison with similar channels.

Those actuated devices, which are not tested during the reactor operation will be tested during scheduled reactor shutdown to show that they are capable of performing the necessary functions.

In addition, in conformance to IEEE 338-1971, response time testing for all plant protection system (PPS) channels and equipment is performed during preoperational testing and each refueling interval. The Technical Specifications describe testing frequency.

7.1.2.8 Conformance to IEEE 344

The CESSAR Licensing scope compliance with IEEE 344-1971, "IEEE Guide for Seismic Qualification of Class 1 Electric Equipment for Nuclear Power Generating Stations" is discussed in Combustion Engineering Topical Report CENPD-182, "Seismic Qualification of Instrumentation Equipment" (Reference 3).

Conformance to IEEE 344-1975, is discussed in section 3.10.

7.1.2.9 Conformance to IEEE 379 as Augmented by Regulatory Guide 1.53

Instrumentation for the PPS and ESFAS Auxiliary Relay Cabinets, and the RTSS conform to the requirements of IEEE 379-1972,

"IEEE Trial-Use Guide for the Application of the Single Failure Criterion to Nuclear Power Generating Station Protection Systems", as augmented by Regulatory Guide 1.53, "Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems". A discussion of the application of the single failure criterion is provided in sections 7.2.2.3.2 and 7.3.2.3.2 for these systems.

In addition, the essential safety-related supporting systems listed in paragraph 7.1.1.4 comply with the requirements of IEEE 379-1972 as augmented by Regulatory Guide 1.53. The single failure criterion is discussed in subsection 7.3.2.

7.1.2.10 Conformance to IEEE 384 as Augmented by Regulatory Guide 1.75

The instrumentation for the safety-related electric systems conforms to the requirements of IEEE 384-1974, "IEEE Trial-Use Standard Criteria for Separation of Class 1E Equipment and Circuits", as augmented by Regulatory Guide 1.75, "Physical Independence of Electric Systems". A discussion of the physical independence is provided below which describes the compliance with section 4.6 of IEEE 279-1971 and General Design Criteria 3 and 21.

The PPS cabinet is divided into four bays which are separated by mechanical and thermal barriers. Each bay contains one of the four redundant channels of the RPS and ESFAS. This provides the separation and independence necessary to meet the requirements of section 4.6 of IEEE 279-1971.

Separation of redundant Class 1E circuits within the PPS cabinet is accomplished through 6 inch separation or barriers or conduit. However, in the formation of the logic matrices (AB, AC, BC, AD, BD, CD), initiation circuits, and actuation

circuits, 6 inch separation is not maintained, nor can barriers or conduit be utilized. An analysis has been performed to show that the separation achieved is acceptable. Tests and analyses have also been completed to demonstrate that no single credible event in one PPS bay can prevent the circuitry in any other bay from performing its safety function.

The ESFAS Auxiliary Relay Cabinets provide separation and independence for the selective two-out-of-four actuation logics and actuation relays of the two redundant ESF Systems' Trains. Each train's logic and relays are contained in a separate cabinet with all of the train A actuation circuits in one cabinet and all of the train B actuation circuits in the other cabinet. There are mechanical and thermal barriers within the cabinets to protect different portions of the selective two-out-of-four logic from spurious actuation. The two cabinets are physically separated from each other.

The RTSS consists of four RTSG. Each RTSG and its associated switches, contacts, relays, etc. is contained in a separate cabinet. Each cabinet is physically separated from the other cabinets. This method of construction ensures that a single credible failure in one RTSG cannot cause malfunction or failure in another cabinet.

The separation and independence of the power supplies for each of the above systems is discussed in Chapter 8.0. The interface requirements appear in section 7.1.3 while the implementation will appear in section 7.1.4. Protection system analog signals, sent to the Plant Monitoring System (PMS), are isolated from the protection system. Digital signals are also isolated for the associated signals coming from the protection system.

All of these isolation techniques ensure that no credible failures on the output side of the isolation device will effect the PPS side and that the independence of the PPS is not jeopardized.

In addition, compliance to General Design Criterion 17, IEEE 384-1974, and Regulatory Guide 1.75 is described in section 8.3 and section 1.8. Additionally, instrumentation for the safety-related electrical instrumentation and control systems supplied by C-E was designed using Regulatory Guide 1.75, Revision 0, 2/74.

7.1.2.11 Conformance to IEEE 387

Conformance to IEEE 387-1972 is discussed in section 8.1.

7.1.2.12 Conformance to IEEE 450

Conformance to IEEE 450 is discussed in subsection 8.3.2.

7.1.2.13 Comparison of Design with Regulatory Guide 1.6

A comparison of the design with Regulatory Guide 1.6 is provided in paragraph 8.1.4.3.1.

7.1.2.14 Comparison of Design with Regulatory Guide 1.11

Containment penetrations for the eight containment pressure detectors are consistent with the recommendations of Regulatory Guide 1.11. All other containment penetrations are in accordance with NRC General Design Criteria 55, 56, or 57. Isolation of containment penetrations is discussed in detail in subsection 6.2.4.

7.1.2.15 Conformance to Regulatory Guide 1.22

The PPS, ESFAS Auxiliary Relay Cabinets, and the RTSS, as described in section 7.1.1, conform to the guidance of Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions". This conformance is described below.

A. Provisions are made to permit periodic testing of the complete PPS, ESFAS Auxiliary Relay Cabinets, and RTSS with the reactor operating at power or when shutdown. These tests cover the trip action from sensor input to the PPS cabinets through the protection system or ESFAS Auxiliary Relay Cabinets to and including the RTSS and the ESFAS actuated devices. Those ESFAS actuated devices which could affect operations are not tested while the reactor is operating but during reactor shutdown.

B. The provisions of this position are incorporated in the testing of the PPS, from sensor to actuation device, including the ESFAS and ESFAS Auxiliary Relay Cabinets and the RTSS.

1. No provisions are made in the design of the PPS, ESFAS Auxiliary Relay Cabinets, and RTSS at the systems level to intentionally bypass an actuation signal that may be required during power operation. All bypasses are on a channel level to prevent an operator from inadvertently bypassing a trip function.

2. The manual testing circuitry for an RPS channel is interlocked to prevent testing in more than one redundant channel simultaneously. Testing

requiring a channel bypass is automatically indicated in the main control room.

3. Manual testing of an ESFAS channel requiring a channel bypass is automatically indicated in the main control room.

C. Actuated devices which cannot be tested during reactor operation will be tested by the ESFAS circuitry when the reactor is shutdown.

Additional information regarding conformance with Regulatory Guide 1.22 for non-C-E portions of the safety-related systems is provided in subsection 7.3.2.

7.1.2.16 Conformance to Regulatory Guide 1.29

The PPS and ESFAS and other instrumentation and controls necessary for safety conform to the guidance of Regulatory Guide 1.29, "Seismic Design Classification". This conformance is described below.

The systems designated as Seismic Category I are items listed in Regulatory Guide 1.29, Sections C.1.k, C.1.1, and C.1.q. The seismic classification and qualification are discussed in Combustion Engineering Topical Report CENPD-182 (Reference 3) and section 3.10. The Class 1E electric systems identified in C.1.q are discussed in section 8.3.

Those portions of structures, systems, or components whose continued function is not required, are designed so that the SSE will not cause a failure which will reduce the functioning of any plant safety feature to an unacceptable level, including incapacitating injury to the occupants of the control room. This is a qualification to Regulatory Guide 1.29 position C.1.r which would classify these items as Seismic Category I.

The classifications of non-CE systems and components which are described in sections 7.2, 7.3, 7.4, 7.5, and 7.6 are listed in section 3.2. The design methods are described in section 3.7, and test/analysis methods and results are given in section 3.10. Refer to section 1.8 for a discussion of PVNGS interpretation of Regulatory Guide 1.29.

7.1.2.17 Conformance to Regulatory Guide 1.30

Refer to section 1.8 for a discussion of PVNGS conformance to Regulatory Guide 1.30.

7.1.2.18 Conformance to Regulatory Guide 1.40

There are no Class 1E continuous-duty motors installed inside the containment.

7.1.2.19 Conformance to Regulatory Guide 1.47

The design of the RPS and the ESFAS as indicated in sections 7.2 and 7.3, is consistent with the recommendations of Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plants Safety System". Conformance is described below.

Bypasses can be classified into two groups: operating bypasses and trip channel bypasses.

7.1.2.19.1 Operating Bypasses

The operating bypass is used during routine startup and shutdown. These bypasses must be manually inserted. They utilize permissive contact inputs generated from the parameter(s) being bypassed to ensure the bypass is removed if plant conditions deviate to the point where the bypass is no

longer safe. (Example: If the coolant system pressure rises above a predetermined setpoint, the RPS/ESFAS pressurizer pressure bypass is automatically removed.) Once a bypass is automatically removed, the manual switch must be turned to the normal (unbypassed) position and then returned to bypass in order to reinsert the bypass for all systems except the CPC system. This prevents cycling the bypass with the permissive contact status. Separate contacts from the manual switch and permissive relay are combined to provide a plant annunciator output. Indicator lamps are provided in the bypass circuit to monitor directly the application of the bypass. These are located on the PPS remote operator's modules and display bypass status for each channel. Operating bypasses include the RPS/ESFAS pressurizer pressure bypass, the high log power bypass and the DNBR/LPD trip bypass.

7.1.2.19.2 Trip Channel Bypasses

These bypasses are used to individually bypass channel trip inputs to the protection system logic for maintenance or testing. The trip logic is converted from a two-of-four to a two-of-three logic for the parameters being bypassed, while maintaining a coincidence two for actuation. Only one channel for any one parameter may be bypassed at any one time. This is accomplished by electrically interlocking the manual bypass switches. These bypasses must be manually initiated and removed. Individual bypass indicator lights are provided locally at the PPS and at the PPS remote operator's modules located in the control room. The wiring for these indicators is run within their respective channels so that faults in any one module will not affect the other channel bypass indication or bypass status. A separate signal is provided to the plant

annunciator when any trip channel bypass is present. In addition, the status of each bypass is provided to the Plant Monitoring System.

A. Annunciator outputs are provided to indicate, at the system level, the bypassing or deliberate inducing of inoperability of a protection system. The system level alarms are actuated when a component actuated by a protection system is bypassed or deliberately rendered inoperable.

B. Those auxiliary and support systems within the CESSAR Licensing scope provide automatic annunciator activation to indicate, on a system level, the bypassed or deliberately induced inoperability of an auxiliary or support system that effectively bypasses or renders inoperable a protection system and the systems actuated or controlled by a protection system.

C. Annunciation shall be provided in the control room, at the system level, for each bypassed or deliberately induced inoperable status in a protection system.

   1. These are supplied for those systems discussed in A. and B. above.

   2. All of these bypasses are expected to be used at least once a year.

   3. All of these bypasses are expected to be usable when the annunciated system is expected to be operable.

D. The operator shall be able to activate each system level bypass indicator manually in the control room.

For a discussion of the non-CE systems listed in paragraph 7.1.1.3 regarding conformance with Regulatory Guide 1.47, see section 7.5.

7.1.2.20 Conformance to Regulatory Guide 1.53

The conformance to Regulatory Guide 1.53 is discussed in paragraph 7.1.2.9.

7.1.2.21 Conformance to Regulatory Guide 1.62

Manual initiation of the RPS is described in sections 7.2.1.1.1.11, and 7.2.2.3.2. Manual initiation of the ESFAS is described in sections 7.3.1.2 and 7.3.2.3.2. Conformance to Regulatory Guide 1.62, "Manual Initiation of Protective Actions", is as follows:

A. Each of the above systems has means for manual actuation.

B. Manual initiation of a protective action causes the same actions to be performed by the protection system as would be performed if the protection system had been initiated by automatic action.

C. Manual switches are located in the control room and at the RTSS for use by the operator. Some functions also have actuation at remote locations.

D. The amount of equipment common to the manual and automatic initiation paths is kept to a minimum, usually just the actuation devices. No single credible failure in the manual, automatic, or common portions of the protective system will prevent initiation of a protective action by manual or automatic means.

E. Manual initiation requires a minimum of equipment consistent with the needs of A., B., C., and D. above.

F. Once initiated, manual protective action will go to completion. (Refer to section 7.3.1.1.10.7.)

In addition, manual initiation of the portions of the ESFAS not supplied by C-E is discussed in section 7.3.

7.1.2.22 Conformance to Regulatory Guide 1.63

Conformance to Regulatory Guide 1.63 is discussed in section 1.8.

7.1.2.23 Conformance to Regulatory Guide 1.68

Conformance with Regulatory Guide 1.68, Preoperational and Initial Start-Up Test Program for Water-Cooled Power Reactors, is discussed in section 14.2.

7.1.2.24 Conformance to Regulatory Guide 1.73

The CESSAR Licensing scope electric valve operators intended to be installed inside the containment are qualified in compliance with Regulatory Guide 1.73, "Qualification Tests of Electric Valve Operators Installed Inside the Containment of Nuclear Power Plants", (see section 3.11).

In addition, non-CE supplied electric valve operators installed within the containment are in compliance with Regulatory Guide 1.73 and are discussed in section 3.11.

7.1.2.25 Conformance to Regulatory Guide 1.75

The conformance to Regulatory Guide 1.75 is discussed in section 1.8. Procurement specifications for 1E systems and components required conformance to Regulatory Guide 1.75. A

further description of the conformance is contained in paragraphs 8.3.1.2 and 8.3.1.4.

7.1.2.26 Conformance to Regulatory Guide 1.80

Regulatory Guide 1.80 has been withdrawn. It is replaced by Regulatory Guide 1.68.3.

7.1.2.27 Conformance to Regulatory Guide 1.89, Revision 1

The conformance to Regulatory Guide 1.89, Rev. 1 is given in section 1.8.

7.1.2.28 Conformance to Regulatory Guide 1.95

Not applicable; see section 1.8.

7.1.2.29 Conformance to Regulatory Guide 1.97

Conformance to Regulatory Guide 1.97 is presented in section 1.8. The post-accident monitoring instrumentation is described in paragraph 7.5.2.5.

7.1.2.30 Conformance to Regulatory Guide 1.100

Conformance to Regulatory Guide 1.100 is presented in section 3.10.

7.1.2.31 Conformance to Regulatory Guide 1.105

Conformance to Regulatory Guide 1.105 is presented in section 1.8.

7.1.2.32 Conformance to Regulatory Guide 1.118

Conformance to Regulatory Guide 1.118 is given in section 1.8 and implemented in the Technical Specifications. Specific test

capabilities within the reactor protective system and the engineered safety features systems are described in paragraphs 7.1.2.7 and 7.3.1.1 and subsection 7.2.1.

7.1.2.33 Evaluation of IE Bulletin 79-27

Action Item 1.

IE Bulletin 79-27 addressed three review areas, as follows:

[Area] 1. Review the Class 1E and non-Class 1E buses supplying power to safety- and nonsafety-related instrumentation and control systems which could affect the ability to achieve a cold shutdown condition using existing procedures or procedures developed under [Area] 2 below. For each bus:

a. Identify and review the alarm and/or indication provided in the control room to alert the operator to the loss of power to the bus.

b. Identify the instrument and control system loads connected to the bus and evaluate the effects of loss of power to these loads including the ability to achieve a cold shutdown condition.

c. Describe any proposed design modifications resulting from these reviews and evaluations, and your proposed schedule for implementing those modifications.

[Area] 2. Prepare emergency procedures or review existing ones that will be used by control room operators, including procedures required to achieve a cold shutdown condition, upon loss of power to each Class 1E and non-Class 1E bus supplying power to safety and nonsafety-related instrument and control systems. The emergency procedures should include:

a. The diagnostics/alarms/indicators/ symptom resulting from the review and evaluation conducted per [Area] 1 above.

b. The use of alternate indication and/or control circuits which may be powered from other non-Class 1E or Class 1E instrumentation and control buses.

c. Methods for restoring power to the bus.

Describe any proposed design modifications or administrative controls to be implemented resulting from these procedures, and your proposed schedule for implementing the changes.

[Area] 3. Re-review IE Circular No. 79-02, Failure of 120 Volt Vital AC Power Supplies, dated January 11, 1979, to include both Class 1E and non-Class 1E safety-related power supply inverters. Based on a review of operating experience and your re-review of IE Circular No. 79-02, describe any proposed design

modifications or administrative controls to be implemented as a result of the re-review.

Evaluation

Our review has determined that the PVNGS design consists of two ungrounded non-Class 1E, 120 V-ac instrument distribution panels E-NNN-D11 and E-NNN-D12 and four ungrounded vital (Class 1E) 120 V-ac instrument distribution panels E-PNA-D25, E-PNB-D26, E-PNC-D27, and E-PND-D28.

Each ungrounded non-Class 1E volt ac instrument distribution panel is normally supplied from a 480 V-ac, non-Class 1E motor control center through a voltage regulator-transformer to a transfer switch. A backup source is provided from a 480 V-ac, Class 1E motor control center through a Class 1E voltage regulator-transformer as an isolation device to the transfer switch. The transfer switch automatically transfers, upon loss of power on the normal source, to the backup source. Manual transfer is required to return to the normal source. The distribution panel is fed from the transfer switch through a panel feeder breaker. Distribution to the instrument cabinets is through branch circuit breakers.

Each ungrounded vital (Class 1E), 120 V-ac instrument distribution panel is normally supplied from a 125 V-dc, Class 1E control center through an inverter to a manual transfer switch. A backup source is provided from a 480 V-ac, non-Class 1E motor control center through a voltage regulator-transformer to the manual transfer switch. The distribution panel is fed from the transfer switch through a panel feeder breaker.

Our specific response to [Area] 1.a is that an alarm for each non-Class 1E instrument distribution panel is provided to the

operator in the control room. Annunciation will occur on the following:

- Normal source undervoltage
- Backup source undervoltage
- Ground detection
- Overload tripping of the panel feeder breaker
- Overload tripping of any branch circuit breaker

An alarm is provided for each Class 1E instrument distribution panel and an alarm for each Class 1E inverter and transfer switch. Annunciation will occur on the following:

- Inverter output or input breaker tripped
- Inverter output voltage low or high
- Inverter overcurrent (overload)
- Input dc voltage low
- Loss of synchronization (of the inverter only)
- Transfer switch not on normal source
- Inverter fan failure
- Distribution panel undervoltage
- Ground detection
- Overload tripping of the panel feeder breaker

For [Area] 1.b, the instrument and control system loads connected to each instrument distribution panel are provided as noted on table 8.3-4.

Those specific instrument parameters and controls detailed in 7.4.1.1.10.2 as being required to achieve cold shutdown are listed in table 7.1-2. Instrument loop displays and controls available to the control room operator and the instrument distribution panel supply are identified.

Motor-operated valves, pumps, pressurizer heaters, and solenoids required to achieve cold shutdown are powered from buses other than the instrument distribution panels.

Table 7.1-1

DELETED

Table 7.1-2

INSTRUMENT PARAMETERS AND CONTROLS REQUIRED TO ACHIEVE COLD SHUTDOWN

Parameter or Control	Class 1E Instrument Distribution Panels				Non-Class 1E Instrument Distribution Panels	
	E-PNA-D25	E-PNB-D26	E-PNC-D27	E-PND-D28	E-NNN-D11	E-NNN-D12
Neutron log power	J-SEA-JI-1A	J-SEB-JI-1B	J-SEC-JI-1C	J-SED-JI-1D	-	-
Hot leg temperature & TR-112HA	J-RCA-TI-112HA	J-RCB-TI-112HB	J-RCC-TI-112HC	J-RCD-TI-112HD	J-RCN-TI-111X	J-RCN TI-111X
Pressurizer pressure	J-RCA-PI-102A & PR-102A	J-RCB-PI-102B	J-RCC-PI-102C	J-RCD-PI-102D	-	J-RCN-PIK-110 & PR-100
Pressurizer level	J-RCA-LI-110X & LR-110X	J-RCB-LI-110Y	-	-	J-RCN-LIC-110 LR-110 & LI-113	-
SG pressure	J-SGA-PI-1013A PI-1023A & PR-1013A	J-SGB-PI-1013B & PI-1023B	J-SGC-PI-1013C & PI-1023C	J-SGD-PI-1013D & PI-1023D	-	-
SG level	J-SGA-LI-1113A & LR-1113A	J-SGB-LI-1113B	J-SGC-LI-1113C	J-SGD-LI-1113D	-	-
RWT level	J-CHA-LI-203A & J-CHA-LI-200-1	J-CHB-LI-203B & LI-201	J-CHC-LI-203C	J-CHD-LI-203D	J-CHN-LI-200	J-CHN-LI-200
Charging flow	J-CHA-FI-212	-	-	-	-	-
Charging pressure	-	J-CHB-PI-212	-	-	-	-
SIT pressure	J-SIA-PI-331 & PI-333	J-SIB-PI-311 & PI-313	-	-	J-SIN-PI-332	J-SIN-PI-312
LPSI pump flow	J-SIA-FI-306	J-SIB-FO-307	-	-	-	-
Shutdown cooling heat exchanger diff. temp.	J-SIA-TR-351 & TI-303X	J-SIB-TR-352 & TI-303Y	-	-	-	-
Atmospheric dump valve control	J-SGA-HIC-179A & HIC-184A	J-SGB-HIC-178A & HIC-185A	-	-	-	-

In response to [Area] 1.c, we have determined that loss of a single instrument distribution panel, Class 1E or non-Class 1E, will cause a loss of some of the indicators and recorders available to the control room operator. This failure mode is distinguishable and will not offer confusing information to the operator since the instrumentation and control systems lost will generate alarms and actuation of some equipment as the loop output contacts fail to their deenergized states. In addition, the loss of power to each analog instrument cabinet is alarmed in the control room. In the non-Class 1E instrument loops affecting safe shutdown circuits, i.e., pressurizer level control of the pressurizer backup heaters, selector switches are provided on the main control panel to enable the operator to provide control from the unaffected control loop. No control action generated by the loss of an instrument distribution panel will prevent the operator from controlling the required safe shutdown equipment or interfere with the safe shutdown functions. Upon detection of loss of an instrument distribution panel, adequate instrumentation and control functions from the list provided above will be available to the operator to enable the operator to achieve a cold shutdown condition. No design modifications are proposed.

Action Item 2.

Emergency procedures that will be used by control room operators, including procedures required to achieve a cold shutdown condition, upon loss of power to each Class 1E and non-Class 1E bus supplying power to safety- and nonsafety-related instruments and control systems will be prepared and then reviewed at least 3 months prior to the operating license. The procedures will include the following information:

A. The diagnostics/alarms/indicators/symptom resulting from the review and evaluation conducted per Item 1 of IE Bulletin No. 79-27.

B. The use of alternate indication and/or control circuits which may be powered from other non-Class 1E or Class 1E instrumentation and control buses.

C. Methods for restoring power to the bus.

A description of any proposed design modifications or administrative controls to be implemented resulting from these procedures, and the proposed schedule for implementing the changes will also be provided.

Action Item 3.

IE Circular No. 79-02, Failure of 120 Volt Vital AC Power Supplies, has been re-reviewed in consideration of item 3 to include both Class 1E and non-Class 1E instrument distribution panel supplies. For the Class 1E inverters, the PVNGS design precludes the possibility of a transient causing a failure of a Class 1E inverter by utilizing a battery source in parallel with a dc charger. The battery source serves to eliminate any undervoltage transients that the charger may experience.

The non-Class 1E instrument distribution panels are not supplied through inverters. Both the normal and backup supplies are fed from 480 V-ac through a voltage regulator-transformer. The transfer switch will automatically transfer, upon loss of power on the normal source, to the backup source. Manual transfer is required to return to the normal source. The switch is also equipped with a mechanical handle which bypasses electric circuitry and can switch to either source. No design modifications are proposed.

7.1.2.34 Evaluation of IE Bulletin 80-06

The ESF actuation signals incorporated in the PVNGS design include:

A. NSSS ESFAS

- Containment isolation actuation signal (CIAS)
- Containment spray actuation signal (CSAS)
- Main steam isolation signal (MSIS)
- Safety injection actuation signal (SIAS)
- Recirculation actuation signal (RAS)
- Auxiliary feedwater actuation signals (AFAS) 1 and 2

B. BOP ESFAS

- Fuel building essential ventilation actuation signal (FBEVAS)
- Containment purge isolation actuation signal (CPIAS)
- Control room ventilation isolation actuation signal (CRVIAS)
- Control room essential filtration actuation signal (CREFAS)

Manual reset of the ESF actuation signals in both the NSSS and BOP systems design can be performed only after the initiating signals, i.e., low pressurizer pressure, have cleared. Reset switches are located at the PPS, ESFAS auxiliary relay, and BOP ESFAS cabinets.

PVNGS equipment which may change position from the safety or emergency state on reset of an ESF actuation signal is identified in table 7.1-3. These actuated devices can be categorized as follows:

A. Certain actuated devices, i.e., jog type valves or the ESF load sequencer, require a maintained ESF signal through completion of their safety function. If an ESF actuation signal is reset prior to completion of the valve stroke or completion of ESF load sequencing, the valve will stop mid-travel or the sequencer will not complete sequencing on the required equipment (equipment already sequenced or does not stop). Since completion of these actions takes no more than 60 seconds, ESF actuation signal reset is not considered. Engineered safety features actuation, followed by clearing of the initiating signals with the requirement of manual reset at the appropriate cabinet, all occurring within a short period of time (<1 minute), is not credible under true accident conditions. No modification to these equipment control circuits is required.

B. An SIAS trips non-ESF equipment (CEDM normal ACU fans, containment normal ACU fans, pressurizer backup heaters, normal chillers) off the 1E buses. On reset of SIAS, this equipment will not be automatically loaded onto the 1E buses, but will be manually loaded onto the 1E buses at the discretion of the operator.

Table 7.1-3

IDENTIFICATION OF ACTUATED DEVICES WHICH CHANGE POSITION

ON RESET OF ESF ACTUATION SIGNAL (Sheet 1 of 4)

Actuated Device	Tag No.	Elementary Diagram	ESF Actuation Signal	Safety Mode	Action of ESF Actuation Signal Reset	Corrective Action
Auxiliary feedwater regulating valves to SG 1	J-AFB-HV-30 J-AFA-HV-32	13-E-AFB-003 13-E-AFB-004	AFAS-1	Open/ Close	Valves cycle on AFAS-1	None[a]
Auxiliary feedwater regulating valves to SG 2	J-AFB-HV-31 J-AFC-HV-33	13-E-AFB-003 13-E-AFB-006	AFAS-2	Open/ Close	Valves cycle on AFAS-2	None[a]
Auxiliary feedwater isolation valves to SG 1	J-AFB-UV-34 J-AFC-UV-36	13-E-AFB-005 13-E-AFB-006	AFAS-1	Open/ Close	Valves cycle on AFAS-1	None[a]

a. See Paragraph 7.1.2.34, listing D.

b. See Paragraph 7.1.2.34, listing C.

c. See Paragraph 7.1.2.34, listing A.

Table 7.1-3

IDENTIFICATION OF ACTUATED DEVICES WHICH CHANGE POSITION

ON RESET OF ESF ACTUATION SIGNAL (Sheet 2 of 4)

Actuated Device	Tag No.	Elementary Diagram	ESF Actuation Signal	Safety Mode	Action of ESF Actuation Signal Reset	Corrective Action
Auxiliary feedwater isolation valves to SG 2	J-AFB-UV-35 J-AFA-UV-37	13-E-AFB-005 13-E-AFB-010	AFAS-2	Open/ Close	Valves cycle on AFAS-2	None[a]
Fuel building essential exhaust AFU dampers	M-HFA-M05 M-HFB-M05	13-E-HFB-005	SIAS FBEVAS	Closes Opens	SIAS is the priority mode. On reset of SIAS, dampers will reopen if FBEVAS is present.	None[b]
Auxiliary building essential exhaust AFU dampers	M-HFA-M06 M-HFB-M06	13-E-HFB-011	SIAS FBEVAS	Opens Closes	SIAS is the priority mode. On reset of SIAS, dampers will reopen if FBEVAS is present.	None[b]
Control room essential AHU OSA intake dampers	M-HJA-M02 M-HJA-M03 M-HJB-M02 M-HJB-M03	13-E-HJB-024	SIAS CREFAS CRVIAS	Opens Closes	CRVIAS is the priority mode. On reset of CRVIAS, dampers will reopen if SIAS or CREFAS is present.	None[b]

Table 7.1-3

IDENTIFICATION OF ACTUATED DEVICES WHICH CHANGE POSITION

ON RESET OF ESF ACTUATION SIGNAL (Sheet 3 of 4)

Actuated Device	Tag No.	Elementary Diagram	ESF Actuation Signal	Safety Mode	Action of ESF Actuation Signal Reset	Corrective Action
ESF load sequencers	J-SSA-C02A J-SAB-C02B	13-E-SAB-004	CSAS SIAS AFAS-1 AFAS-2 FBEVAS CRIVAS CREFAS	Sequential starting of ESF pumps and fans	Reset of sequencer outputs depending on ESF actuation signals present. Reset of sequencer outputs does not reset any actuated equipment. Reset prior to completion of sequencing terminates sequence.	None[c]
LP safety injection pumps	M-SIA-P01 M-SIB-P01	13-E-SIB-002	SIAS (via sequencer) RAS	Starts Stops	RAS is the priority mode. On reset of RAS, pumps will restart if SIAS (via sequencer) is present.	None[b]

Table 7.1-3

IDENTIFICATION OF ACTUATED DEVICES WHICH CHANGE POSITION

ON RESET OF ESF ACTUATION SIGNAL (Sheet 4 of 4)

Actuated Device	Tag No.	Elementary Diagram	ESF Actuation Signal	Safety Mode	Action of ESF Actuation Signal Reset	Corrective Action
Safety injection tank isolation valves	J-SIA-UV-634 and -644 J-SIB-UV-614 and -624	13-E-SIB-005 13-E-SIB-006	SIAS	Opens	Jog-type valves may stop mid-travel. Breakers are locked open during power operation.	None[c]
LPSI flow control to reactor coolant valves	J-SIB-UV-615 and -625 J-SIA-UV-635 and -645	13-E-SIB-007 13-E-SIB-008	SIAS	Opens	Jog-type valves may stop mid-travel	None[c]
HPSI flow control to reactor coolant valves	J-SIA-UV- -617, -627, -637, -647 J-SIB-UV- -616, -626, -636, -646	13-E-SIB-009 13-E-SIB-010 13-E-SIB-011 13-E-SIB-012	SIAS	Opens	Jog-type valves may stop mid-travel	None[c]
Containment spray control valves	J-SIA-UV-672 J-SIB-UV-671	13-E-SIB-020	CSAS	Opens	Jog-type valves may stop mid-travel	None[c]

C. Certain actuated devices have different safety modes in response to different ESF actuation signals. In the event that ESF actuation signals requiring both safety modes occur, one safety mode by design will have priority. On reset of that particular ESF actuation signal, the actuated device will change position to the safety mode required by the remaining ESF actuation signal. This means of control does not defeat required ESF system functions, and no modification is required to these equipment control circuits.

D. The AFAS 1 and AFAS 2 signals to the auxiliary feedwater valves are designed to cycle based on steam generator level. This automatic resetting of the AFAS 1 and AFAS 2 does not affect the AFAS 1 and AFAS 2 signals to other actuated equipment. The auxiliary feedwater valve cycling represents the desired ESF system function and no modification is required to the equipment control circuits.

7.1.2.35 Evaluation of IE Information Notice 79-22

The high energy line break (HELB)/control system interaction analysis process employed in the review of the PVNGS Units 1, 2, and 3 design is illustrated by the logic diagram of figure 7.1-1. The events considered are those defined in chapters 6 and 15 of the PVNGS FSAR. The process consists of the following steps:

A. Identification of all nonsafety grade systems or control systems of significance to the FSAR chapters 6 and 15 analyses.

B. Identification of potential adverse control system malfunctions induced by HELB events.

C. Detailed system design reviews of control systems with a potentially significant impact on the course of FSAR chapters 6 and 15 events to determine which, if any, failure modes can be postulated to cause the adverse malfunctions.

D. Identification of the physical locations of control systems components whose malfunctions could be postulated to cause the adverse malfunction and determination if the components can be impacted by the HELB of concern.

E. Resolution of potential HELB/control system interaction issues through the use of backup systems and/or quantitative analyses to determine if the malfunctions effects are acceptable, and through detailed evaluations of the qualification status of control system components.

The HELBs considered in this analysis are: loss-of-coolant accident (LOCA) steam line break (SLB), feedwater line break (FWLB), and reactor coolant system (RCS) breaks which occur outside of the containment. Completion of listings A through D disclosed four potential HELB/control system interactions which could exacerbate event consequences. These are:

1. Failure of the pressurizer pressure control system (PPCS) to deenergize pressurizer heaters when the low level cutout signal is given. This malfunction is of concern during a LOCA, or SLB due to the potential for the heater failure mode to impact the RCS pressure boundary.

2. Failure of the reactor regulating system (RRS) such that CEAs are withdrawn prior to reactor trip. The

resultant core power increase is of concern during LOCA, SLB, and FWLB events.

3. Failure of the steam bypass control system (SBCS) such that the steaming rate is increased. This malfunction is of concern during SLBs because of the potential for a post-trip return to power.

4. Failure of the PLCS such that the RCS inventory is increased. This malfunction is of concern during FWLB events where a potential to fill the pressurizer could exist.

The impacts of the assumed malfunctions were determined in listing E. The results of these investigations demonstrate that the HELB/control system malfunction event consequences are bounded by the event consequences presented in the FSAR. Therefore, no design modifications or operator procedure revisions are needed to mitigate the consequences of HELB/control system interactions.

7.1.3 CESSAR INTERFACES

The following NSSS general interface requirements are repeated from CESSAR Section 7.1.3.

7.1.3.1 Power

Vital instrument power requirements for the safety-related systems are discussed in Section 8.3.1.

7.1.3.2 Protection from Natural Phenomena

Refer to Section 3.1.2. CESSAR Design Scope Class 1E equipment shall be located within the plant so as to ensure the various natural phenomena specified in GDC 2 which are applicable to

the Applicant's site will not result in degradation of that equipment below the level required to allow it to perform required protective action assuming a single failure.

7.1.3.3 Protection from Pipe Failure

The location of safety-related instrumentation and control components shall take into account their potential damage due to piping failures, such as pipe whip, jet impingement, etc., from high or medium energy fluid systems.

The location of these components and the routing of 1E and associated cables and sensing lines should avoid such hazards or shall be provided with adequate protection such that required protective action can be performed assuming a single piping failure, its associated effects, and a single failure.

7.1.3.4 Missiles

The safety-related equipment shall be protected from potential missile sources. The 1E and associated cabling and sensing lines shall be handled in a similar fashion.

7.1.3.5 Separation

The routing of 1E and associated cabling and sensing lines from sensors shall be arranged to minimize the possibility of common mode failure. This requires that the cabling for the four safety channels be routed separately, however, the cables of different safety functions within one channel, may be routed together. Low energy signal cables shall be routed separately from all power cables. Safety-related sensors wired to separate channels shall be physically and electrically separated. The separation of their safety-related cables requires that the cables be routed in separate cable trays.

Associated circuit cabling from redundant channels shall be separated, provided with isolation, analyzed, or tested to demonstrate that no single credible failure can adversely affect more than one redundant channel.

Non-Class 1E instrumentation circuits and cables (low level) which may be in proximity to associated circuits and cables, are to be treated as associated circuits if analyses or tests demonstrate that credible failures therein could adversely affect Class 1E circuits.

7.1.3.6 Independence

Cabling associated with redundant channels of safety-related circuits shall be installed such that a single credible event cannot cause multiple channel malfunctions or interactions between channels.

7.1.3.7 Thermal Limitations

The safety-related equipment shall be located so as not to violate the temperature and humidity limits of Section 3.11.

7.1.3.8 Monitoring

Auxiliary and supporting systems for the safety-related instrumentation and controls shall be designed to cause a systems level bypass indication, when they are bypassed or deliberately made inoperable, for the safety-related system which would be affected by the bypassing or deliberate inoperability of the auxiliary or supporting system.

The RPS and ESFAS alarms and the remote PPS and DNBR/LPD Calculator Operator's Modules shall be located in the main control room.

7.1.3.9 Operational Controls

The RPS and ESFAS manual actuation devices shall be located in the control room. The instrumentation and control components of the safe shutdown systems on the Remote Shutdown Panel or at local locations shall be manually operable.

7.1.3.10 Inspection and Testing

The PPS, including sensors, shall be capable of being periodically tested in accordance with the Technical Specifications. Those portions which could adversely affect reactor operations shall be capable of being tested when the reactor is shut down. All other safety-related instrumentation shall be capable of being tested during normal operation.

7.1.3.11 Chemistry/Sampling

The components of the safety-related equipment shall be located so as not to exceed the chemistry limits specified in Section 3.11.

7.1.3.12 Materials

Not applicable to the safety-related instrument and controls equipment.

7.1.3.13 System Component Arrangement

Safety-related components shall be located so as to conform to the separation, independence, and other criteria specified in this section. The safety-related components shall be located to provide access for maintenance, testing and operation as required.

Analog and digital signals provided to the safety-related components shall not share the same multiconductor cable, unless specifically called for or approved by Combustion Engineering.

7.1.3.14 Radiological Waste

Radiological waste discharge lines or components shall not be routed or located next to protection system electronic components in a manner that will result in exceeding the radiation limits specified in Section 3.11.

7.1.3.15 Overpressure Protection

The components of the safety-related equipment shall be located so as not to exceed the pressure limits specified in Section 3.11.

7.1.3.16 Related Services

A fire protection system shall be provided to protect the safety-related equipment, including sensors, consistent with GDC 3. This shall include facilities for detection, alarming, and extinguishing of fires. Facilities and methods for minimizing the probability and effects of fires, including fire barriers, fire resistant and non-combustible materials, and other such items, shall be employed whenever possible. Adequate drainage shall be provided if water is used to extinguish fires.

Inadvertent operation or rupture of fire protection systems shall not result in the reduction of the functional capability of safety-related systems or components below that required to perform their safety function.

Physical identification shall be provided to enable plant personnel to recognize that PPS, ESFAS Auxiliary Relay Cabinets, RTSS, and their cabling are safety-related. The cabinets shall be identified by nameplates. A color coding scheme shall be used to identify the physically separated channel cabling from sensor to the PPS (refer to section 7.1.3.5); the same color code shall be used for interbay or intercabinet identification.

Cabling or wiring within a bay at the cabinet which is in the channel of its circuit classification shall not be color coded.

The cabinet nameplates and cabling shall be color coded as follows:

Protective	ESF Trains	Associated
Channel A: Red	A: Red	White Stripe with Red Stripe over Black Jacket or White Stripe over Red Jacket
Channel B: Green	B: Green	White Stripe with Green Stripe over Black Jacket or White Stripe over Green Jacket
Channel C: Yellow		White Stripe with Yellow Stripe over Black Jacket or White Stripe over Yellow Jacket
Channel D: Blue		White Stripe with Blue Stripe over Black Jacket or White Stripe over Blue Jacket

All non-panel mounted protection system instrumentation and control components are identified with a name tag which provides the channel number and the suffix A, B, C, or D to specifically identify the protection channel with which the component is identified.

7.1.3.17 Environmental

Environmental support systems shall be provided to ensure that the environmental conditions of the safety-related systems do not exceed the requirements for 1E equipment as defined in Section 3.11.

7.1.3.18 Mechanical Interaction

Seismic requirements for safety-related equipment are specified in Section 3.10.

7.1.3.19 Plant Monitoring System Inputs

The inputs to the RPS and ESFAS can be sent to the PMS for trending, data logging and other historical functions but are not used for other control functions. These inputs shall have proper isolation to prevent any failure in the PMS from adversely affecting the RPS or ESFAS.

7.1.4 CESSAR INTERFACE EVALUATIONS

Interface requirements listed in CESSAR Section 7.1.3 are met by the PVNGS design as follows:

7.1.4.1 Power

A. Vital instrument power interfaces are discussed in section 8.3.

B. Emergency diesel generator interfaces are discussed in section 8.3.

C. Power source failures are discussed in appendix 7A, Question 7A.4 response.

7.1.4.2 Protection from Natural Phenomena

Refer to subsection 3.1.2 for a description of applicable natural phenomena and references to the appropriate FSAR sections for methods of compliance.

7.1.4.3 Protection from Pipe Failure

Refer to section 3.6 for a description of the design to protect against pipe failures. Also, figures 7.2-1 through 7.2-3 and engineering drawing 13-J-ZYF-009 show locations of Class 1E instruments.

7.1.4.4 Missiles

Refer to section 3.5 for a description of designs provided for protection of 1E systems and components against missile damage.

7.1.4.5 Separation

A. Separation of cabling associated with redundant channels is provided as discussed in paragraph 8.3.1.4.

B. Separation of sensing lines associated with redundant channels is as discussed in subsection 7.1.3.

7.1.4.6 Independence

The installing methods used for redundant channels of safety-related circuits are described in paragraph 8.3.1.4.

7.1.4.7 Thermal Limitations

The C-E environmental criteria are presented in CESSAR Section 3.11 and the environmental qualification parameters for PVNGS are given in Appendix A of the Equipment Qualification Program Manual.

7.1.4.8 Monitoring

A. The bypass/inoperable status system is discussed in subsection 7.5.2.

B. The reactor protective system (RPS) and ESFAS alarms and the remote PPS and DNBR/LPD calculator operator's modules are located in the main control room.

7.1.4.9 Operational Controls

The RPS and ESFAS manual actuation devices are located in the main control room. A description of the remote shutdown capabilities which include manual actuation is in subsection 7.4.1.

7.1.4.10 Inspecting and Testing

PPS and ESFAS sensors are located to permit testing either during reactor operation or during shutdown. The test features are described in subsections 7.2.2 and 7.3.2.

7.1.4.11 Chemistry/Sampling

The components of the safety-related equipment are located to conform to the criteria listed in CESSAR Section 3.11 for C-E scope of supply and Appendix A of the Equipment Qualification Program Manual for the corresponding PVNGS environmental qualification parameters.

7.1.4.12 Materials

Not applicable.

7.1.4.13 System Component Arrangement

Locations have been selected to provide separation and access for maintenance, testing, and operation as discussed in section 7.2.

7.1.4.14 Radiological Waste

Criteria for radiation exposure limits for 1E system electronic components are given in Section 3.11. The methods by which these criteria are met are discussed in sections 3.11 and 12.3.

7.1.4.15 Overpressure Protection

The locations for C-E-furnished 1E equipment shown in figures 7.2-1 through 7.2-3 and engineering drawing 13-J-ZYF-009 meet the overpressure criteria given in CESSAR Section 3.11.

7.1.4.16 Related Services

A. Fire protection design is discussed in subsection 9.5.1.

B. Physical identification of safety-related systems, components, cabinets, and interconnecting cables is described in paragraph 8.3.1.3. The one-out-of-two ESF systems will be identified as follows:

- Channel A - Red
- Channel B - Green

7.1.4.17 Environmental

Environmental support systems are provided and discussed in CESSAR Section 3.11 for C-E scope of supply and sections 6.4 and 9.4 for the PVNGS specific design.

7.1.4.18 Mechanical Interaction

Refer to CESSAR Section 3.10 for C-E scope of supply and to section 3.10 for PVNGS specific design.

7.1.4.19 Plant Monitoring System Inputs

Isolation per Regulatory Guide 1.75 is provided for alarm signals originating from safety-related circuits that terminate in the plant monitoring system.

7.1.5 REFERENCES

1. CENPD-210A, "Description of the C-E Nuclear Steam Supply System Quality Assurance Program", Combustion Engineering, Inc.

2. CENPD-255, "Qualification of Combustion Engineering Class 1E Instrumentation", Combustion Engineering, Inc.

3. CENPD-182, "Seismic Qualification of Instrumentation Equipment", Combustion Engineering, Inc.

4. CENPD-396-P, "Common Qualified Platform Topical Report," Rev. 01, May 2000

This page intentionally blank

7.2 REACTOR PROTECTIVE SYSTEM

7.2.1 DESCRIPTION

7.2.1.1 System Description

The reactor protective system (RPS) consists of sensors, calculators, logic, and other equipment necessary to monitor selected nuclear steam supply system (NSSS) conditions and to effect reliable and rapid reactor shutdown (reactor trip), if any or a combination of the monitored conditions approach specified limiting safety system settings. The system's functions are to protect the core specified acceptable fuel design limits and reactor coolant system (RCS) pressure boundary for incidents of moderate frequency, and also to provide assistance in limiting conditions for certain infrequent events and limiting faults. Four measurement channels with electrical and physical separation are provided for each parameter used in the direct generation of trip signals, with the exception of control element assembly (CEA) position. A coincidence of two like trip signals is required to generate a reactor trip signal. The fourth channel is provided as a spare and allows bypassing of one channel while maintaining a two-out-of-three system.

The reactor trip signal deenergizes the control element drive mechanism (CEDM) coils, allowing all CEAs to drop into the core.

The reactor protective instrumentation setpoints shall be set consistent with the Trip Setpoint values shown in Table 7.2-1.

7.2.1.1.1 Trips

7.2.1.1.1.1 RPS Variable Overpower. The RPS variable overpower trip (RPS VOPT) is provided to trip the reactor when

indicated neutron flux power either (1) increases at a great enough rate, or (2) reaches a preset value. The flux signal used is the average of the three linear subchannel flux signals originating in each nuclear instrument safety channel. The trip setpoints are provided in table 7.2-1.

Pre-trip alarms are initiated below the trip value to provide audible and visible indication of approach to a trip condition.

7.2.1.1.1.2 High Logarithmic Power Level. The high logarithmic power level trip is provided to trip the reactor when indicated neutron flux power reaches a preset value. The flux signal used is the logarithmic power signal originating in each nuclear instrument safety channel. The setpoint is provided in table 7.2-1. The trip may be manually bypassed by the operator. This bypass point is provided in table 7.2-2.

Pre-trip alarms are initiated below the trip value to provide audible and visible indication of approach to a trip condition. The trip bypass also bypasses the pre-trip alarms.

7.2.1.1.1.3 High Local Power Density. The high local power density trip is provided to trip the reactor when calculated core peak local power density reaches a preset value. The preset value is less than that value which would cause fuel centerline melting. The calculation of the peak local power density is performed by the core protection calculators (CPCs), which compensate the calculated peak local power density to account for the thermal capacity of the fuel. A trip results if the compensated peak local power density reaches the preset value. The calculated trip assures that the safety limit for peak fuel centerline temperature is not exceeded. The trip setpoint is given in table 7.2-1. The

Table 7.2-1

REACTOR PROTECTIVE SYSTEM DESIGN INPUTS

(Sheet 1 of 3)

Type	Typical Value (full power)	Trip Setpoint	Typical Margin To Trip
High logarithmic power level	NA	≤0.010% of neutron rated thermal power	NA
RPS Variable overpower	100% power 0%/min NA	≤110% of rated thermal power[m] ≤10.6%/min[m] ≤9.7% band[a][m]	10% power 10.6% min NA
Low DNBR	1.79[b]	≥1.34[k]	≤0.55
High local power density, kW/ft	≤13.5 (peak)[c]	≤21.0[k]	≥7.5
High pressurizer pressure, psia	2,250	≤2,383	133
Low pressurizer pressure, psia	2,250	≥1,837[d]	413
Low steam generator water level, %[f]	82	≥44.2	37.8
Low steam generator pressure, psia	1039	≥960[e]	79
High containment pressure, psig	0	≤3.0	3.0
High steam generator water level, %[g]	55	≤91.0	36
Low reactor coolant flow, floor rate band	25.2 psid[h] 0.0 psi/sec NA	≥12.81 psid[j] ≤0.112 psid/sec[j] ≤16.87 psid[j]	12.39 psid N/A 12.39 psid[n]
Supplementary Protection System Pressurizer Pressure - High, psia	2,250	≤2409	159

Table 7.2-1

REACTOR PROTECTIVE SYSTEM DESIGN INPUTS

(Sheet 2 of 3)

a. % band is percent above measured excore power level.

b. Calculated value of DNBR assures trip conservatively considering all sensor and processing time delays and inaccuracies. Calculated DNBR will be less than or equal to actual core DNBR.

c. Peak value is unit and cycle specific.

d. In MODES 3-4, the value may be decreased manually, to a minimum of 100 psia, as pressurizer pressure is reduced, provided:

   (1) the margin between the pressurizer pressure and this value is maintained at less than or equal to 400 psi; and

   (2) when the RCS cold leg temperature is greater than or equal to 485 degrees F, this value is maintained at least 140 psi greater than the saturation pressure corresponding to the RCS cold leg temperature.

   The setpoint shall be increased automatically as pressurizer pressure is increased until the trip setpoint is reached. Trip may be manually bypassed below 400 psia; bypass shall be automatically removed whenever pressurizer pressure is greater than or equal to 500 psia.

e. In MODES 3-4, value may be decreased manually as steam generator pressure is reduced, provided the margin between the steam generator pressure and this value is maintained at less than or equal to 200 psi; the setpoint shall be increased automatically as steam generator pressure is increased until the trip setpoint is reached.

Table 7.2-1

REACTOR PROTECTIVE SYSTEM DESIGN INPUTS

(Sheet 3 of 3)

f. % of the distance between steam generator upper and lower level wide range instrument nozzles.

g. % of the distance between steam generator upper and lower level narrow range instrument nozzles.

h. Average full power steam generator primary differential pressure.

i. Not Used

j. RATE is the maximum rate of decrease of the trip setpoint. There are no restrictions on the rate at which the setpoint can increase.

FLOOR is the minimum value of the trip setpoint.

BAND is the amount by which the trip setpoint is below the input signal unless limited by Rate or Floor.

Setpoints are based on steam generator differential pressure.

k. As stored within the Core Protection Calculator (CPC). Calculation of the trip setpoint includes measurement, calculational and processor uncertainties. Trip may be bypassed when logarithmic power is < 1E-4% NRTP. Bypass shall be automatically removed when logarithmic power is ≥ 1E-4% NRTP.

l. not used

m. RATE is the maximum rate of increase of the trip setpoint. (The rate at which the setpoint can decrease is no slower than five percent per second.)

CEILING is the maximum value of the trip setpoint.

BAND is the amount by which the trip setpoint is above the steady state input signal unless limited by the rate or the ceiling.

n. Value reported here is the same as the value reported for the floor because the floor overrides the band.

Table 7.2-2

REACTOR PROTECTIVE SYSTEM BYPASSES

Title	Function	Initiated By	Removed By	Notes
DNBR and local power density bypass	Disable low DNBR and high local power density trips	Key-operated switch (1 per channel) (Note 1)	Automatic if power is $\geq 10^{-4\%}$	Allows low power testing
Pressurizer pressure bypass	Disables low pressurizer pressure trip, SIAS, and CIAS	Manual switch (1 per channel) if pressure is <400 psia	Automatic if pressure is ≥500 psia	Allows testing at low pressure and, heatup and cooldown with CEA's withdrawn
High log power level bypass	Disables high logarithmic power level trip	Manual switch (1 per channel) if power is $>10^{-4\%}$	Automatic if power is $\leq 10^{-4\%}$	Bypassed during reactor startup
Trip channel bypass	Disables any given trip channel	Manually by controlled access switch	Same switch	Interlocks allow only one channel for any one type trip to be bypassed at one time

NOTE 1 DNBR and LPD Bypass may be performed from the operations module and the maintenance and test panel by a "soft" switch (i.e., touch screen). A hard-wired key-operated switch is also located in each CPCS cabinet.

effects of core burnup are considered in the determination of the local power density trip.

Pre-trip alarms are initiated below the trip value to provide audible and visible indication of approach to a trip condition.

7.2.1.1.1.4 Low Departure from Nucleate Boiling Ratio. The low departure from nucleate boiling ratio (DNBR) trip is provided to trip the reactor when the calculated DNBR approaches a preset value. The calculation of DNBR is performed by the CPCs based on core average power, reactor coolant pressure, reactor inlet temperature, reactor coolant flow, and the core power distribution. The calculation includes allowances for sensor and processing time delays and inaccuracies, such that a trip is generated within the CPCs before violation of the DNBR safety limit occurs in the limiting coolant channel in the core, during incidents of moderate frequency. The trip setpoint is given in table 7.2-1.

Pre-trip alarms are initiated above the trip value to provide audible and visible indication of approach to a trip condition.

The CPCs also have several trip functions that monitor parameters to limits other than low DNBR or High Local Power Density. These trip functions are called Auxiliiary Trips and, if a trip is generated, the DNBR and Local Power Density trip contact outputs are set. Auxiliary Trips do not set the pre-trip contact outputs.

The low DNBR trip incorporates a low pressurizer pressure floor, with the value given in table 7.2-1A. At this pressure, a low DNBR auxiliary trip will automatically occur.

There are two additional trip functions that are based on the analyzed operating space of the limits of the DNBR correlation. The first trip function is a reactor coolant low flow trip, which is set at a low limit for pump rotational speed. If one or more reactor coolant pumps slow down sufficiently to exceed this low limit, penalties are applied to the DNBR and Local Power Density calculated values that are large enough to ensure DNBR and Local Power Density trips are generated. The low flow trip will set the DNBR and Local Power Density trip and pre-trip contact outputs. The second trip function is a quality margin trip that is based on the updated quality at the node of minimum DNBR. If the quality margin exceeds the limit, the DNBR trip and pre-trip contact outputs are set. The quality margin does not affect the Local Power Density trip and pre-trip conditions.

Table 7.2-1A summarizes these additional trip functions (including the CPC Auxliary Trips).

The CPC auxiliary trip response times are consistent with DNBR – low values listed in UFSAR table 7.2-4AA (Reactor Protective Instrumentation Response Times). The CPC program response time is based on the CPC execution periods and functions. All of the trips have a response time of 0.75 seconds with the exception of pump speed, which has a response time of 0.3 seconds.

7.2.1.1.1.5 <u>High Pressurizer Pressure</u>. The high pressurizer pressure trip is provided to trip the reactor when measured pressurizer pressure reaches a high preset value. The trip setpoint is provided in table 7.2-1.

Pre-trip alarms are initiated below the trip setpoint to provide audible and visible indication of approach to a trip condition.

Table 7.2-1A

CORE PROTECTION CALCULATOR SYSTEM

ADDITIONAL TRIP FUNCTIONS[a]

(Sheet 1 of 2)

Type	Trip Setpoint	Typical Margin to Trip
AUXILIARY TRIP FUNCTIONS[g]		
1. Core conditions outside analyzed operating space:		
Cold leg temperature, °F(Tc)	Tcmin ≥ 505.0, Tcmax < 590.0	50.0 35.0
Primary pressure, psia (P)	1860 ≥ P < 2388	390 (low), 138 (hi)
Hot pin axial shape index (AHP)	-0.5 ≥ AHP < +0.5	0.5
Integrated one pin radial peak (P1)	1.28 ≥ P1 < 7.0	0.2 (low), 5.5 (hi)
2. Variable Overpower Trip (VOPT)[b]		
Ceiling (% power)	< 110.0	10.0
Rate of change up (% RTP/execution)[c]	≤ 0.000835[h] (≤ 1% power/min)	0.000835[h]
Rate of change down (% RTP/execution)[c]	≤ 0.01389[h] (≤ 16.67% power/min)	0.01389[h]
Step or band (% power)	≤ 8.0	NA
Floor (% power)	= 30.0	NA
3. Asymmetric Steam Generator Transient Trip (ASGT)		
Cold leg temperature difference trip setpoint (°F)	≤ 15.0	12.5
Power dependent bias for cold leg temperature difference trip (°F)	= 0.0 At 100% power	0.0
4. Hot leg temperature saturation trip (°F)[d]		
a. Thmax = max hot leg temperature (°F)	Thmax + Therr ≥ TSAT NA	23 NA
b. Hot leg temperature measurement uncertainty bias (°F) (Therr)	= 19.0	NA
5. Number of Reactor Coolant Pumps Running[e]	< 2	NA
6. CPC not in normal operating mode (e.g., in test, in initialization, memory unprotected)[e]	NA	NA

Table 7.2-1A
CORE PROTECTION CALCULATOR SYSTEM
ADDITIONAL TRIP FUNCTIONS[a]
(Sheet 2 of 2)

Type	Trip Setpoint	Typical Margin to Trip
7. Internal processor fault detected[e]	NA	NA
OTHER TRIP FUNCTIONS		
1. Low Reactor Coolant Pump Rotational Speed (fraction of nominal rotational speed)[f]	≥ 0.95	0.05
2. Quality margin at node of minimum DNBR.	> 0.0	0.3

a. CPCS Auxiliary Trip conditions set only the DNBR and LPD trip contact outputs.

b. The VOPT conditions are defined as follows:
CEILING is the maximum value of the trip setpoint.
RATE (up or down) is the maximum rate of increase or decrease of the trip setpoint.
STEP OR BAND is the amount by which the trip setpoint is above the steady state input signal unless limited by the rate or the ceiling.
FLOOR is the minimum value of the trip setpoint.

c. Execution = 50 milliseconds (0.05 seconds) in CPC DNBR and Power Density UPDATE program.

d. The difference between the maximum hot leg temperature including uncertainties and the saturation temperature of water. The saturation temperature of water is based on the primary (pressurizer) pressure input.

e. These trip conditions are yes/no decisions. For CPC operating mode and internal processor faults, the system is either in the condition or not. Normal operation is with all 4 pumps operating. Operations with less than two pumps running is not allowed in Modes 1 and 2.

f. If one or more pumps are determined to be running at or below the trip setpoint, then penalties are applied to the DNBR and Local Power Density values to ensure a trip condition is reached and the trip contact outputs are set.

g. CPC pre-trip annunciators are provided for the following trips, strictly as operator aids; Variable Overpower Trip (VOPT), Axial Shape Index (ASI) Trip, Asymmetric Steam Generator Trip (ASGT), and Hot Leg Saturation Trip.

7.2.1.1.1.6 Low Pressurizer Pressure. The low pressurizer pressure trip is provided to trip the reactor when the measured pressurizer pressure falls to a low preset value. The trip setpoint for normal operation is provided in table 7.2-1. At pressures below the normal operating range, this setpoint can be manually decreased to a fixed increment below the existing pressurizer pressure down to a minimum value. The incremental and minimum values are given in table 7.2-1. This ensures the capability of a trip when required during plant cooldown.

The trip may be manually bypassed by the operator. This bypass point is provided in table 7.2-2. The bypass is automatically removed as pressure is increased above a fixed value and the low pressure setpoint automatically increases, maintaining the fixed increment between the plant pressure and the setpoint until it reaches and limits at the value for normal operation. These values are shown in table 7.2-1.

Pre-trip alarms are initiated above the trip setpoint to provide audible and visible indication of approach to a trip condition.

7.2.1.1.1.7 Low Steam Generator Water Level. The low steam generator water level trip is provided to trip the reactor when measured steam generator water level falls to a low preset value. Separate trips are provided from each steam generator. The trip setpoint is provided in table 7.2-1.

Pre-trip alarms are initiated above the trip setpoint to provide audible and visible indication of approach to a trip condition.

7.2.1.1.1.8 Low Steam Generator Pressure. The low steam generator pressure trip is provided to trip the reactor when the measured steam generator pressure falls to a low preset

value. Separate trips are provided from each steam generator. The trip setpoint during normal operation is provided in table 7.2-1. At steam generator pressures below normal, the operator has the ability to manually decrease the setpoint to a fixed increment below existing system pressure. This is used during plant cooldown. During startup, this setpoint is automatically increased and remains at the fixed increment below generator pressure until it reaches and limits at the value for normal operation. These values are provided in Table 7.2-1.

Pre-trip alarms are initiated to provide audible and visible indication of approach to a trip condition.

7.2.1.1.1.9 High Containment Pressure. The high containment pressure trip is provided to trip the reactor when measured containment pressure reaches a high preset value. The trip setpoint is provided in table 7.2-1. The trip is provided as additional design conservatism (i.e., additional means of providing a reactor trip). The high containment pressure trip setpoint is selected in conjunction with the high-high containment pressure setpoint to prevent exceeding the containment design pressure during a design basis LOCA or main steam line break accident.

Pre-trip alarms are initiated to provide audible and visible indication of approach to a trip condition.

7.2.1.1.1.10 High Steam Generator Water Level. A high steam generator water level trip is provided to trip the reactor when measured steam generator water level rises to a high preset value. Separate trips are provided from each steam generator. The trip setpoint is provided in table 7.2-1.

Pre-trip alarms are initiated to provide audible and visible indication of approach to a trip condition.

7.2.1.1.1.11 Manual Trip. A manual reactor trip is provided to permit the operator to trip the reactor. There are four Manual Trip pushbuttons, each of the pushbuttons operates one of the reactor trip breakers. Depressing either of the pushbuttons in both trip legs will result in a reactor trip. There are also manual reactor trip switches at the reactor trip switchgear.

The remote manual initiation portion of the reactor protective system is designed as an input to the reactor trip switchgear system (RTSS). This design is consistent with the recommendations of Regulatory Guide 1.62. The amount of equipment common to both automatic and manual initiation is kept to a minimum. Once initiated, the manual trip will go to completion as required in Section 4.16 of IEEE Standard 279-971.

7.2.1.1.1.12 Low Reactor Coolant Flow. The low reactor coolant flow trip is provided to trip the reactor when the pressure differential across the primary side of either steam generator decreases below a rate limited variable setpoint, as shown in figure 7.2-0. A separate trip is provided for each steam generator. This function is used to provide a reactor trip for a reactor coolant pump sheared shaft event.

Pre-trip alarms are provided.

7.2.1.1.2 Initiating Circuits

7.2.1.1.2.1 Process Measurements. Various pressures, levels, and temperatures associated with the NSSS and the containment

building are continuously monitored to provide signals to the RPS trip bistables. All protective parameters are measured with four independent process instrument channels. A detailed listing of the parameters measured is contained in table 7.2-3. The monitored ranges associated with these parameters are listed in table 7.2-4.

A typical protective channel, as shown in figure 7.2-0A, consists of a sensor/transmitter, converter/power supply, current loop resistors, indicating meter or recorder, trip bistable/calculator inputs, and outputs for the plant monitoring system (PMS).

The piping, wiring, and components of each channel are physically separated from that of other like protective channels to provide independence. The output of each transmitter is an ungrounded current loop. Exceptions are (1) the nuclear instruments, and (2) the reactor coolant pump speed sensors which provide a pulsed voltage signal. Signal isolation is provided for computer inputs. Each redundant channel is powered from a separate vital ac bus.

Table 7.2-3

REACTOR PROTECTIVE SYSTEM SENSORS

Monitored Variable	Type	Number of Sensors	Location
Neutron flux power	Fission chamber	12	Biological shield
Cold leg temperature	Precision RTD	8	Cold leg piping
Hot leg temperature	Precision RTD	8	Hot leg piping
Pressurizer pressure (wide range)	Pressure transducer	4[a]	Pressurizer
Pressurizer pressure (narrow range)	Pressure transducer	4	Pressurizer
CEA positions	Reed switch assemblies	2/CEA	Control element drive mechanism
Reactor coolant pump speed	Proximity device	4/pump	Reactor coolant pump
Steam generator level (wide range)	Differential pressure transducer	4/steam generator[a]	Steam generators
Steam generator level (narrow range)	Differential pressure transducer	4/steam generator[a]	Steam generators
Steam generator pressure	Pressure transducer	4/steam generator[a]	Steam generators
Containment pressure	Pressure transducer	4[a]	Containment structure
Low steam generator primary differential pressure	Differential pressure transducer	4/steam generator	Steam generators

a. Common with engineered safety feature actuation system.

Table 7.2-4

REACTOR PROTECTIVE SYSTEM MONITORED PLANT VARIABLE RANGES

Monitored Variable	Minimum	Typical (full power)	Maximum
Neutron flux power, %	$2x10^{-7}$ of full power	100 power	200 of full power
Cold leg temperature, °F	465	557	615
Hot leg temperature, °F	375	614	675
Pressurizer pressure (narrow range), psia	1.500	2,250	2,500
Pressurizer pressure (wide range), psia	0	2,250	3,000
CEA positions	full in	NA	full out
Reactor coolant pump speed, rpm	700	1,188	1,200
Steam generator water level, % [(a)]	0	82	100
Steam generator water level, % [(b)]	0	55	100
Steam generator pressure, psia	0	1039	1,524
Containment pressure, psig	-4	0	0
Steam generator primary pressure differential, psid	0	31.0	70

a. % of the distance between the wide range level instrument nozzles (above the lower nozzle).

b. % of the distance between the narrow range level instrument nozzles (above the lower nozzle).

7.2.1.1.2.2 CEA Position Measurements The position of each CEA is an input to the RPS. These positions are measured by means of redundant and independent reed switch position transmitters (RSPTs) on each CEA. The RSPTs transmit analog signals to eight redundant and independent control element assembly calculators (CEACs), two for each CPC channel. CEAC 1 in each CPC channel monitors RSPT1 on all CEAs. CEAC 2 in each CPC channel monitors RSPT2 on all CEAs.

Each RSPT consists of a series of magnetically actuated reed switches spaced at intervals along the CEA housing and wired with precision resistors in a voltage divider network (see figure 7.2-0B). A magnet attached to the CEA extension shaft actuates the adjacenet reed switches, causing voltages proportional to position to be transmitted for each RSPT. The RSPT assemblies and wiring are physically and electrically separated from each other (see figure 7.2-0C).

The CEAs are arranged into subgroups that are controlled as control groups of CEAs. The subgroups are symmetric about the core center. The subgroups of a control group are required to move together and to follow a set insertion sequence.

Each CEAC monitors the position of all CEAs within each subgroup. Should a CEA deviate by more than a specific deadband limit, the CEACs will detect the event, sound an annunciator alarm, and transmit appropriate “penalty” factors to the CPCs.

The CPCS displays the position of each regulating, shutdown, and part-strength CEA to the operator in a bar chart format on a visual display. Optical isolation is utilized at each CPC channel to the CEA position display. The operator has the capability to select any channel for display. Selecting CPC

7.2.1.1.2.2 (continued)

channel A or B will display RSPT1. Selecting channels C or D will display RSPT2.

The CPCs utilize 22 selected "target" CEA position reed switch signals as a measure of CEA subgroup and group position. When the CPCs determine that the subgroups of a control group are not moving together, or that the control groups are not moving in the required sequence, they generate penalty factors. The CPCs utilize single CEA deviation penalty factors from the CEACs to modify calculational results in a conservative manner. These factors may result in a reduction in margins-to-trip for low DNBR and high LPD. This assures conservative operation of the RPS during CEA deviations which require a RPS trip. The detailed signal paths of CEA position information within the RPS are shown in figure 7.2-0D. Raw analog RSPT inputs undergo analog to digital conversion in each of two redundant CEA position processors (CPPs) in each CPC channel. Each CPP transmits CEA position to the appropriate CEAC in all four CPC channels over isolated data links. The CPP also transmits target CEA position to the CPC processor in the same channel over the CEAC to CPC data link.

7.2.1.1.2.3 Excore Neutron Flux Measurements. The excore nuclear instrumentation includes neutron detectors located around the reactor core, and signal conditioning equipment located within the containment and the auxiliary building. Neutron flux is monitored from source levels through full power operation, and signal outputs are provided for reactor protection and information display. There are four channels of safety instrumentation (see figure 7.2-0E).

The four safety channels provide neutron flux information from startup neutron flux levels to 200% of rated power covering a single range of approximately 2 x 10^{-7} to 200% power (9 decades). Each safety channel consists of three fission chambers, a preamplifier and a signal conditioning drawer containing power supplies, a logarithmic amplifier (including combination counting and mean square variation techniques), linear amplifiers, test circuitry, and a rate-of-change of power circuit. These channels provide signals for the rate-of-change power display, RPS for logarithmic power level high and variable over power trips, and CPCs for use in calculations for low DNBR and high LPD trips.

The detector assembly provided for each safety channel consists of three identical fission chambers stacked vertically along the length of the reactor core. The use of multiple subchannel detectors in this arrangement permits the determination of axial power shape during power operation.

The fission chambers are mounted in holder assemblies which in turn are located in four dry instrument wells (thimbles) at the primary shield. The wells are spaced around the reactor vessel to provide optimum neutron flux information.

Preamplifiers for the fission chambers are mounted outside the primary shield, with two inside containment, and two outside containment in the auxiliary building. Physical and electrical separation of the preamplifiers and cabling between redundant channels are provided.

7.2.1.1.2.4 Reactor Coolant Flow Measurements. The speed of each reactor coolant pump motor is measured to provide a basis for calculation of reactor coolant flow through each pump. The measurement of reactor coolant pump speed is accurate to within

0.43% of the actual pump speed. This requirement is only applicable to pump speeds greater than 700 rpm. Two metal discs, each with 44 uniformly spaced slots about its periphery, are scanned by proximity devices. The metal discs are attached to the pump motor shaft, one to the upper portion and one to the lower portion (see Figure 7.2-0F). Each scanning device produces a voltage pulse signal. The pulse train that is input to the CPCs to calculate flow rate is based upon every n^{th} pulse from the scanning device. The frequency of this pulse train is proportional to pump speed. Adequate separation between proximity devices is provided.

The mass flow rate is obtained using the pump speed inputs from the four reactor coolant pumps, the cold leg temperatures, and the hot leg temperatures. The volumetric flow rate through each reactor coolant pump is dependent upon the rotational speed of the pump and the pump head. This relationship is typically shown in pump characteristic curves. Flow changes resulting from changes in the loop flow resistances occur slowly (i.e., core crud buildup, increase in steam generator resistance, etc.). Calibration of the calculated mass flow rate will be performed periodically using instrumentation which is not part of the reactor coolant pump speed sensing system.

Flow reductions associated with pump speed reductions are more rapid than those produced from loop flow resistance changes. Mass flow rate is calculated for each pump from the pump speed, the density of the cold leg coolant, and a correction term based on hot leg temperature.

The mass flow rates calculated for each pump are summed to give a core mass flow rate. This flow rate is then used in the CPC DNBR and ΔT power algorithms.

7.2.1.1.2.5 Core Protection Calculators. The core protection calculator (CPC) system and CEA calculators provide their outputs and a number of their inputs as inputs to the plant monitoring system (PMS) by means of fiber-optic communication.

The CPC/CEAC data processing programs within the PMS perform cross-channel comparisons for each input signal and generate an alarm whenever the difference between any single channel's value and the average value of all four channels is greater than a constant. On operator demand, a report is printed to show the results of the latest cross-channel comparison. Some CPC and CEAC parameters are also used to calculate and alarm CPC Aux trip pretrips on the CMC. The CPC and CEAC parameters are not supplied to or used by any program in the plant computer.

Four independent CPCs are provided, one in each protection channel. Calculations of DNBR and LPD are performed in each CPC, utilizing the input signals described below. The DNBR and LPD calculated are compared with trip setpoints for initiation of a low DNBR trip (paragraph 7.2.1.1.1.4) and high LPD trip (paragraph 7.2.1.1.1.3).

Two independent CEA calculators (CEACs) in each channel are provided as part of the CPC system to calculate individual CEA deviations from the position of the other CEAs in their subgroup.

7.2.1.1.2.5 (continued)

Redundant CEA position processors (CPPs) mounted within each CPCs channel process all channel RSPT inputs. CPPs process target CEA position for use by the CPC in the channel of origin. CPPs also process CEA position for use in the CEACs in all four channels. CPPs in channels A and B provide RSPT 1 CEA positional data on all CEAs to CEAC 1 in all four CPC channels. CPPs in channels C and D provide RSPT 2 CEA positional data on all CEAs to CEAC 2 in all four CPC channels. Cross channel communication of CEA positional information from the CPPs to CEACs utilizes one-way isolated data links.

As shown in figure 7.2-0G, each CPC receives the following inputs: core inlet and outlet temperature, pressurizer pressure, reactor coolant pump speed, excore nuclear instrumentation flux power (each subchannel from the safety channel), selected CEA positions, and penalty factors for CEA deviations within a subgroup from the CEACs. Input signals are conditioned and processed. The following calculations are performed in the CPC or the CEACs:

A. CEA deviations;

B. Correction factor for excore flux power for shape annealing and CEA shadowing;

C. Reactor coolant flowrate from reactor coolant pump speeds and temperatures;

D. ΔT power from reactor coolant temperatures, pressure, and flow information;

E. Excore flux power: excore flux power signals are summed and corrected for CEA shadowing, shape annealing, and cold leg temperature shadowing. This

7.2.1.1.2.5 (continued)

corrected flux power is periodically calibrated to the actual core power measured independently of the reactor protective system. This calibration does not modify the inherent fast time response of the excore signals to power transients;

F. Axial power distribution from the corrected excore flux power signals;

G. Fuel rod and coolant channel planar radial peaking factors, selection of predetermined coefficients based on CEA positions;

H. DNBR;

I. Comparison of DNBR with a fixed trip setpoint;

J. Local power density;

K. Comparison of local power density with a fixed trip setpoint;

L. CEA deviation alarm;

M. Variable overpower trip (VOPT) and comparison of maximum power with VOPT setpoint;

N. Reactor coolant pump (RCP) speed and comparison of RCP speed with a minimum RCP speed trip setpoint; and

O. Compensated cold leg temperature difference and comparison of the compensated cold leg temperature difference to a cold leg temperature difference trip setpoint.

The Primary Outputs of each CPC are:

- Low DNBR trip and pretrip;

7.2.1.1.2.5 (continued)

- DNBR margin (to control board indication);
- High local power density trip and pretrip;
- Local power density margin (to control board indication);
- Calibrated neutron flux power (to control board indication); and
- Control element assembly withdrawal prohibit (CWP).

Each calculator is mounted in the auxiliary protective cabinet with an operator's display and control module located on the main control board. From the four modules an operator can monitor all calculators, including specific inputs or calculated functions.

7.2.1.1.2.6 Trip Generation. Signals from the trip parameter process measurement loops are sent to voltage comparator circuits (bistables) where the input signals are compared to predetermined trip values (Figure 7.2-6). Whenever a channel trip parameter reaches the trip value, the channel bistable deenergizes the bistable output relay. The bistable output relay or, in the case of trips generated by the Core Protection Calculators, an external trip contact deenergizes trip relays. Outputs of the trip relays are in the trip logic (refer to Section 7.2.1.1.3).

The trip bistable setpoints are adjustable from the PPS cabinet. Access is limited, however, by means of a key-operated cover with an annunciator indicating cabinet door access. All bistable setpoints are capable of being read out on a meter located on the PPS cabinet.

Pretrip bistables and relays are also provided to generate audible and visible alarms.

7.2.1.1.2.7 CPC Software Design. The CPC software requirements specification descriptions of the CEAC and CPC algorithms in Reference 23 includes symbolic algebra. It includes system requirements affecting the software, hardware, and man-machine interface design.

Typical software test results of Phase I and Phase II software testing are provided in Reference 17 and Reference 18. Typical CPC database material is provided in Reference 19.

The generation of detailed software design documentation and test documentation is included as part of the structured quality assurance design documentation. These types of design documents have been used in the design process on PVNGS 1, 2, and 3 and include the CPC system requirements specifications[23] and a data base document.

Subsequent to the completion of the PVNGS CPC software base design, any revisions to the PVNGS software base design and test documentation will be prepared in accordance with the protection algorithm software change procedure in Reference 20.

The algorithms associated with the CPC Improvement Program as described in CEN-304-P[6], CEN-305-P[1], CEN-308-P-A[15], CEN-310-P-A[16], and CEN-330-P-A[11], were implemented in Cycle 2 and apply to all subsequent cycles. Values for the Reload Data Block (RDB) constants will be evaluated for applicability and consistent with the cycle design, performance, and safety analyses. Any necessary changes to the RDB constants will be accomplished by a vendor in accordance with Reference 21 or by

7.2.1.1.2.7 (continued)

the Nuclear Fuel Management (NFM) Department in accordance with the NFM Design Control.[14]

Trip setpoints, uncertainty factors, and other addressable constants are determined consistent with the methodology and software established in the CPC Improvement Program. Uncertainty factors are determined using the methods contained in CEN-356(V)-P-A.[13]

7.2.1.1.3 Logic

Tripping of a bistable (or trip contact opening in the case of a calculated trip) results in a channel trip which is characterized by the deenergization of three bistable trip relays (see Figure 7.2-8).

Contacts from the bistable relays of the same parameter in the four protective channels are arranged into six logic AND's, designated AB, AC, AD, BC, BD, and CD, which represent all possible coincidence of two combinations. To form an AND circuit, the bistable trip relay contacts of two like protective measurement channels are connected in parallel (e.g., one from A and one from B). This process is continued until all combinations have been formed.

Since there is more than one parameter that can initiate a reactor trip, the parallel pairs of bistable trip relay contacts for each monitored parameter are connected in series (Logic OR) to form six logic matrices. The six matrices are designated AB, AC, AD, BC, BD and CD.

Each logic matrix is connected in series with a set of four matrix output relays (matrix relays). Each logic matrix is powered from two separate 120V vital ac distribution buses

through dual dc power supplies, as shown on Figure 7.2-8. The power supplies are protected from overload by means of input and/or output fuses or circuit breakers.

The contacts of the matrix relays are combined into four initiation circuits, one initiation circuit per channel.

Each reactor initiation circuit is formed by connecting six contacts (one matrix relay contact from each of the six logic matrices) in series. The six series contacts are in series with the initiation output relay. The initiation output relays serve to deenergize the Reactor Trip Switchgear System (RTSS) breakers as discussed in section 7.2.1.1.4.

7.2.1.1.4 Actuated Devices

The above logic causes the deenergizing of the four initiation relays whenever any one of the logic matrices is deenergized as described. Each initiation circuit output relay in turn will cause one trip circuit breaker in the RTSS to open. See Figure 7.2-8.

Power input to the RTSS comes from two full-capacity motor-generator sets, so that the loss of either set does not cause a release of the CEAs. Each line passes through two trip circuit breakers (each actuated by a separate initiation circuit) in series so that, although both sides of the branch lines must be deenergized to release the CEAs, there are two separate means of interrupting each side of the line. Upon removal of power to the CEDM power supplies, the CEAs fall into the reactor core by gravity.

Two sets of manual trip pushbuttons are provided to open the trip circuit breakers, if desired. The manual trip completely bypasses the trip logic. As can be seen in Figure 7.2-8, both

manual trip pushbuttons in a set must be depressed to initiate a reactor trip.

The trip switchgear is housed in separate cabinets from the RPS. In addition to the trip circuit breakers, the cabinet also contains current monitoring devices for testing purposes and pushbuttons on each RTSG which allow for reactor trip from a location other than the control room.

7.2.1.1.5 Bypasses

The bypasses listed in table 7.2-2 are provided to permit testing, startup, and maintenance. The bypass setpoints are provided in table 7.2-2.

The DNBR and local power density bypass, which bypasses the low DNBR and high local power density trips from the CPC, is provided to allow system tests at low power when pressurizer pressure may be low or reactor coolant pumps may be off. The bypass may be manually initiated if power is below the bypass setpoint and is automatically removed when the power level increases above the bypass setpoint.

The RPS/ESFAS pressurizer pressure bypass is provided for two conditions: (1) system tests at low pressure, and (2) heatup and cooldown with shutdown CEA's withdrawn. The bypass may be manually initiated if pressurizer pressure is below the bypass setpoint. The bypass is automatically removed as pressure is increased above the bypass setpoint.

The high logarithmic power level bypass is provided to allow the reactor to be brought to the power range during a reactor startup. The bypass may be manually initiated above the bypass setpoint and is automatically removed when power decreases below the bypass setpoint.

The trip channel bypass is provided to remove a trip channel from service for maintenance or testing. The trip logic is thus converted to a two-out-of-three basis for the trip type bypassed; other type trips that do not have a bypass in any of their four channels remain in a two-out-of-four logic. The bypass is manually initiated and manually removed. The circuit utilized to accomplish the trip channel bypass is shown in Figure 7.2-10. This circuit, which is repeated for each type trip, contains an electrical interlock which allows only one channel for any one type trip to be bypassed at one time.

All bypasses are annunciated visibly to the operator.

7.2.1.1.6 Interlocks

The following interlocks are provided:

A. Trip Channel Bypasses

An interlock prevents the operator from bypassing more than one trip channel at a time for any one type of trip. Different type trips may be simultaneously bypassed, either in one channel or in different channels.

B. Matrix Tests

During system testing an electrical interlock will allow only the matrix relays in one of the six matrix test modules to be held at a time. The same circuit will allow only one bistable input signal to be perturbed at a time (see Figure 7.2-9).

C. Nuclear Instrumentation Test

Placement of the linear calibration switch on the NI drawer to other than "operate" will cause a channel variable overpower trip. Placement of the logarithmic

calibration switch to other than "operate" will cause a channel high logarithmic power trip. In addition to these two trips, placing either of these calibration switches, or any other calibration switch on the NI drawer to other than "operate" will cause a Power Trip Test interlock to generate a low DNBR and high LPD trip in that channel.

D. Core Protection Calculation Test

The low DNBR and high local power density channel trips are interlocked such that they both must be bypassed to test a CPC channel.

7.2.1.1.7 Redundancy

Redundant features of the RPS include:

A. Four independent channels, from process sensors through and including channel trip relays. The CEA position input is from two independent channels.

B. Six logic matrices which provide the coincidence of two logic. Dual power supplies are provided for the matrix relays.

C. Four initiation circuits, including four control logic paths and four initiation relays.

D. Four manual trip pushbuttons with either of the pushbuttons in both trip legs being sufficient to cause a reactor trip.

E. AC power for the system from four separate vital instrument buses. DC power for the trip switchgear circuit breakers control logic is provided from four separate battery buses.

The result of the redundant features is a system that meets the single failure criterion, can be tested during reactor

operation, and can be indefinitely shifted to two-out-of-three logic and retain a coincidence of two for trip.

The benefit of a system that includes four independent and redundant channels is that the system can be operated, if need be, with up to two channels out of service (one bypassed and another tripped) and still meet the single failure criterion. The only operating restriction while in this condition (effectively one-out-of-two logic) is that no provision is made to bypass another channel for periodic testing or maintenance. The system logic must be restored to at least a three operating channel condition prior to removing another channel for maintenance.

7.2.1.1.8 Diversity

The system is designed to eliminate credible multiple channel failures originating from a common cause. The failure modes of redundant channels and the conditions of operation that are common to them are analyzed to assure that a predictable common failure mode does not exist (Reference 2). The design provides reasonable assurance that:

a. The monitored variables provide adequate information during design basis events (design basis events are listed in Sections 7.2.2.1.1 and 7.2.2.1.2).

b. The equipment can perform as required.

c. The interactions of protective actions, control actions and the environmental changes that cause, or are caused by, the design basis events do not prevent the mitigation of the consequences of the event.

d. The system will not be made inoperable by the inadvertent actions of the operating and maintenance personnel.

In addition, the design is not encumbered with additional components or channels without reasonable assurance that such additions are beneficial.

7.2.1.1.9 Testing

Provisions are made to permit periodic testing of the complete RPS with the reactor operating at power or when shutdown. These tests cover the trip actions from sensor input through the protective system and the trip switchgear. The system test does not interface with the protective function of the system. The testing system meets the criteria of IEEE 338-1971, "IEEE Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection System", and is consistent with the recommendations of NRC Regulatory Guide 1.22, "Periodic Testing of Protection System Actuator Functions."

The individual tests are described briefly below. Overlap between individual tests exists so that the entire RPS can be tested. Frequency of accomplishing these tests are listed in the Technical Specifications.

7.2.1.1.9.1 Sensor Check

During reactor operation, the measurement channels providing an input to the RPS are checked by comparing the outputs of similar channels and cross-checking with related measurements.

During extended shutdown periods or refueling, these measurement channels (where possible) are checked and calibrated against known standards.

7.2.1.1.9.2 Trip Bistable Tests

Testing of the trip bistables is accomplished by manually varying the input signal up to or down to the trip setpoint level on one bistable at a time and observing the trip action (Figure 7.2-6).

Varying the input signal is accomplished by means of a trip test circuit consisting of a digital voltmeter and a test circuit used to vary the magnitude of the trip signal supplied by the measurement channel to the trip input. The trip test circuit is interlocked electrically so that it can be used in only one channel at a time. A switch is provided to select the measurement channel, and a pushutton is provided to apply the test signal. The digital voltmeter indicates the value of the test signal. Trip action (deenergizing) of each of the bistable trip relays is indicated by individual lights on the front of the cabinet, indicating that these relays operate as required for a bistable trip condition.

The variable setpoint bistable can be tested by manually varying a simulated process input signal. Upon decreasing this input the setpoint is verified to remain constant and the trip setpoint is within specified tolerances. By manually decreasing this input and then depressing the setpoint reset, the setpoint incremental change can be tested and verified. The tracking ability of the circuit can be tested by manually increasing the test input and observing that the setpoint tracks.

The rate limited variable setpoint bistable is tested in three different ways. Using a test ramp generator, the rate of change limit on the setpoint is verified to be within specified limits. The circuit is tested to verify that the setpoint will track the signal when it increases or decreases and maintains the proper

separation (it should be noted that the setpoint is still rate limited so that a rapid change in the test signal may cause it to catch the setpoint as it increases and cause a trip). The third test verifies the trip setpoint limit accuracy by use of a manual test system. When one of the bistables of a protective channel is in the tripped condition, a channel trip exists and is annunciated on the control room annunciator panel. In this condition, a reactor trip would take place upon receipt of a trip signal in one of the other three like trip channels. The trip channel under test is therefore bypassed for this test, converting the RPS to a two-out-of-three logic for the particular trip parameter. In either case, full protection is maintained.

7.2.1.1.9.3 Core Protection Calculator Tests

The sensor inputs to each calculator are compared between units. Predetermined test inputs are then inserted into one calculator at a time. The calculator outputs are then checked for specific values. Multiple tests can be performed to check each phase of the calculator program.

The checking of the trip relays for the calculator-generated trips is conducted as described in Paragraph 7.2.1.1.9.2 by initiating a calculator trip and observing the individual bistable relay trip lights.

7.2.1.1.9.4 Logic Matrix Test

This test is carried out to verify proper operation of the six two-out-of-four logic matrices, any of which will initiate a bonafide system trip for any possible coincidence of two trip conditions from the signal inputs from each measurement channel.

Only the matrix relays in one of the six logic matrix test modules can be held in the energized position during tests. If, for example, the AB logic matrix hold switch is rotated to the "HOLD" or "TRIP" positions, actuation of the other matrix hold switches will have no effect upon their respective logic matrices.

Rotating the switch to the hold position will apply a test voltage to the test system hold coils of the selected double coil matrix relays. This voltage will provide the power necessary to hold the relays in their energized position when deactuation of the bistable trip relay contacts in the matrix ladder being tested causes deenergization of the primary matrix relay coils. The bistable trip relay contacts are deactuated when the matrix hold switch is rotated to the "TRIP" position.

The logic matrix to be tested is selected using the system channel trip select switch. Then while holding the matrix hold switch in the "TRIP" position, rotation of the channel trip select switch will release only those bistable trip relays that have operating contacts in the logic matrix under test. The channel trip select switch applies a test voltage of opposite polarity to the bistable trip relay test coils, so that the magnetic flux generated by the coils opposes that of the primary coil of the relay. The resulting flux will be zero, and the relays will release. A simplified diagram of this testing system is shown in Figure 7.2-7 using the AB matrix.

Trip action can be observed by illumination of the trip relay indicators located on the front panel and by loss of voltage to the four matrix relays, which is indicated by extinguishing indicator lights connected across each matrix relay coil.

During this test, the matrix relay "hold" lights will remain on, indicating that a test voltage has been applied to the holding coils of the matrix relays of the logic matrix module under test.

The test is repeated for all six matrices and for each actuation signal. This test will verify that the bistable relay contacts operate correctly and that the logic matrix relays will deenergize if the matrix continuity is violated. The opening of the matrix relay contacts is tested in the trip path tests (see Section 7.2.1.1.9.5).

Each logic matrix test module provides the associated test circuitry for both the RPS and ESFAS logic matrices. The system channel trip select switch permits the selection of the desired actuation logic matrix to be tested as can be seen in Figure 7.2-8.

7.2.1.1.9.5 Trip Path/Circuit Breaker Tests

Each trip path is tested individually by rotating a matrix hold switch to the "TRIP" position (holding matrix relays), selecting any trip position on the channel trip select switch (opening the matrix), and selecting a matrix relay on the matrix relay trip select switch (deenergizing one of the matrix relays). This will cause one, and only one, of the trip paths to deenergize, causing one trip circuit breaker to open. CEDMs remain energized via the other trip circuit breakers.

The dropout lamps shown on Figures 7.2-7 and 7.2-8 are used to provide additional verification that the matrix relay has been deenergized, (e.g., the 6AB-1 matrix relay contact energizes the dropout lamp). Since the matrix test modules are also utilized for the ESFAS logic matrix testing, this dropout lamp is also shared via contacts 1AB-1 through 5AB-1 as shown on Figure 7.2-8. Proper

operation of the actual trip path matrix relay contacts is verified by the trip path lamp located on the trip status panel.

Proper operation of all coils and contacts is verified by lights on a trip status panel; final proof of opening of the trip circuit breakers is the lack of indicated current through the trip breakers.

The matrix relay trip select switch is turned to the next position, reenergizing the tested matrix relay and allowing the trip breakers to be manually reset.

This sequence is repeated for the other three trip paths from the selected matrix. Following this the entire sequence is repeated for the remaining five matrices. Upon completion, all 24 matrix relay contacts and all 4 trip paths and breakers will have been tested.

7.2.1.1.9.6 Manual Trip Test

The manual trip feature is tested by depressing one of the four manual trip pushbuttons, observing a trip of a trip breaker, and resetting the breaker prior to depressing the next manual trip pushbutton.

7.2.1.1.9.7 Bypass

The system bypasses, as itemized in Table 7.2-2, are tested by appropriate test circuitry. Testing includes both initiation and removal features.

7.2.1.1.9.8 Response Time Tests

Time testing is addressed in the Technical Specifications. The methods, equipment, and test frequency are also provided in the Technical Specifications. The reactor protective

instrumentation response time limits are identified in table 7.2-4AA.

7.2.1.1.10 Vital Instrument Power Supply

The vital instrument power supply requirements are discussed in section 7.2.3 and Chapter 8.0.

7.2.1.2 Design Bases

The RPS is designed to assure adequate protection of the fuel, fuel cladding, and RCS boundary during Incidents of Moderate Frequency. In addition, the system is designed to assist the ESF Systems in limiting the consequences of certain Infrequent Events and Limiting Faults. To ensure that these design bases are achieved, the reactor must be maintained within the limiting conditions of operation, as defined in Technical Specifications and the limiting safety system settings.

The system is designed on the following bases to assure adequate performance of its protective function:

A. The system is designed in compliance with the applicable criteria of the "General Design Criteria for Nuclear Power Plants", Appendix A of 10CFR50, July 15, 1971.

B. Instrumentation, function, and operation of the system conforms to the requirements of IEEE Standard 279-1971, "Criteria for Protective Systems for Nuclear Power Generating Stations".

C. System testing conforms to the requirements of IEEE Standard 338-1971, "Trial Use Criteria for Periodic Testing of Nuclear Power Generating Station Protection Systems".

D. The system is designed in consistence with the recommendations of Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protective Systems", and Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions".

E. The system is designed to determine the following generating station conditions in order to provide adequate protection during Incidents of Moderate Frequency:

1. Core power (neutron flux);
2. Reactor coolant system pressure;
3. DNBR in the limiting coolant channel in the core;
4. Peak local power density in the limiting fuel pin in the core; and
5. Steam generator water level.

F. The system is designed to determine the following generating station conditions in order to provide protective action assistance to the ESF during certain Infrequent Events and Limiting Faults:

1. Core power;
2. RCS pressure;
3. Steam generator pressure; and
4. Containment pressure.

G. The system is designed to monitor all generating station variables that are needed to assure adequate determination of the conditions given in listings E. and F. above, over the entire range of normal operation and transient conditions. The full power nominal values and the maximum and minimum values that can be sensed for each monitored

plant variable are given in Table 7.2-4. The type, number, and location of the sensors provided to monitor these variables are given in Table 7.2-3.

H. The system is designed to alert the operator when any monitored plant condition is approaching a condition that would initiate protective action.

I. The system is designed so that protective action will not be initiated due to normal operation of the generating station.

Nominal full power values of monitored conditions and their corresponding protective action (trip) setpoints are given in Table 7.2-1.

The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays and inaccuracies are taken into account. Response times and analysis setpoints used in the safety analyses are given in Chapter 15.0.

The trip delay times and analysis setpoints provided in Chapter 15.0 are representative of the manner in which the RPS and associated instrumentation will operate. These quantities are used in the transient analysis done in Chapter 15.0. Actual RPS uncertainties and delay times will be obtained from calculations and tests performed on the RPS and associated instrumentation. The verified system uncertainties are factored into all RPS settings and/or setpoints to assure that the system adequately performs its intended function when the errors and uncertainties combine in an adverse manner.

J. All system components are qualified for environmental and seismic conditions in accordance with IEEE Standard 323-1974,

and IEEE Standard 344-1971. Compliance is addressed in section 3.11 and in CENPD-255, "Qualification of Combustion Engineering Class 1E Instrumentation", (Reference 3); and in section 3.10 and CENPD-182, "Seismic Qualification of Instrumentation and Electrical Equipment", (Reference 4). In addition, the system is capable of performing its intended function under the most degraded conditions of the energy supply, as addressed in section 8.3.

K. The Regulatory Guides and IEEE standards the upgraded Core Protection Calculator System (CPCS) were designed to are listed in reference 22. However, Palo Verde has not increased its commitments to these new or revised regulatory guides and standards.

Instrument location layout drawings are presented in figures 7.2-1, 7.2-2, 7.2-3, and engineering drawing 13-J-ZYF-009.

7.2.1.3 Final System Drawings

The signal logics, block diagrams, layout drawings, and test circuit block diagrams are shown in Figures 7.2-0A through 7.2-0G and 7.2-5 through 7.2-14.

The following discussion compares the logics to be found in the preliminary CESSAR with those contained herein. The figure numbers refer to the numbers used here and are not necessarily those of the preliminary CESSAR.

Figure 7.2-5 shows a simplified block diagram for the SPS.

The simplified functional diagram of Figure 7.2-8 has several changes incorporated. On the table of trip inputs the High Linear Power Level has been replaced with the Variable Overpower Trip. The undervoltage and shunt trip circuits have

had contacts from the SPS circuit added. The Reactor Trip Switchgear consisting of nine breakers has been replaced with a four breaker Reactor Trip Switchgear System. These changes create a more reliable means of providing a reactor trip when it is required.

Figure 7.2-11 shows some changes in the interface logic from the PSAR. The first change is that the high-high containment pressure is now provided with a separate transmitter. Secondly, MSIS has added steam generator level signals and containment pressure. Third, the AFAS logic has been added. Finally, the turbine trip has been removed from the RPS.

In addition, for a list of applicable drawings and diagrams, see section 1.7.

Table 7.2-4AA

REACTOR PROTECTIVE INSTRUMENTATION RESPONSE TIMES

(Sheet 1 of 2)

FUNCTIONAL UNIT	RESPONSE TIME
I. TRIP GENERATION	
A. Process	
1. Pressurizer Pressure - High	≤ 0.50 seconds
2. Pressurizer Pressure – Low	≤ 1.15 seconds
3. Steam Generator Level – Low	≤ 1.15 seconds
4. Steam Generator Level – High	≤ 1.15 seconds
5. Steam Generator Pressure – Low	≤ 1.15 seconds
6. Containment Presssure – High	≤ 1.15 seconds
7. Reactor Coolant Flow – Low	≤ 1.00 seconds
8. Local Power Density - High	
a. Neutron Flux Power from Excore Neutron Detectors	≤ 0.75 second[a]
b. CEA Positions	≤ 1.35 second[b]
c. CEA Positions: CEAC Penalty Factor	≤ 0.75 second[b]
9. DNBR - Low	
a. Neutron Flux Power from Excore Neutron Detectors	≤ 0.75 second[a]
b. CEA Positions	≤ 1.35 second[b]
c. Cold leg Temperature	≤ 0.75 second[d]
d. Hot leg Temperature	≤ 0.75 second[d]
e. Primary Coolant Pump Shaft Speed	≤ 0.30 second[c] [f]
f. Reactor Coolant Pressure from Pressurizer	≤ 0.75 second[e]
g. CEA Positions: CEAC Penalty Factor	≤ 0.75 second[b]
B. Excore Neutron Flux	
1. Variable Overpower Trip	≤ 0.45 second[a]
2. Logarithmic Power Level – High	
a. Startup and Operating	≤ 0.50 second[a]
b. Shutdown	≤ 0.50 second[a]

Table 7.2-4AA

REACTOR PROTECTIVE INSTRUMENTATION RESPONSE TIMES

(Sheet 2 of 2)

FUNCTIONAL UNIT	RESPONSE TIME
C. Core Protection Calculator System	
1. CEA Calculators	Not Applicable
2. CEA Protection Calculators	Not Applicable
D. Supplementary Protection System	
Pressurizer Pressure - High	≤ 1.15 second
II. RPS LOGIC	
A. Matrix Logic	Not Applicable
B. Initiation Logic	Not Applicable
III. RPS ACTUATION DEVICES	
A. Reactor Trip Breakers	Not Applicable
B. Manual Trip	Not Applicable

a. Neutron detectors are exempt from response time testing. The response time of the neutron flux signal portion of the channel shall be measured from the detector output or from the input of first electronic component in channel.

b. Response time shall be measured from the output of the sensor.

c. The pulse transmitters measuring pump speed are exempt from response time testing. The response time shall be measured from the pulse shaper input.

d. Response time shall be measured from the output of the resistance temperature detector (sensor). RTD response time shall be measured in accordance with the Technical Specifications. The measured response time of the slowest RTD shall be less than or equal to 8 seconds.

e. Response time shall be measured from the output of the pressure transmitter. The transmitter response time shall be less than or equal to 0.7 second.

f. The response time for the Seized Rotor Event, 0.865 second, is a theoretical maximum value based on an instantaneous RCP seizure and is not tested.

7.2.2 ANALYSIS

7.2.2.1 Introduction

The RPS is designed to provide the following protective functions:

- Initiate automatic protective action to assure that acceptable RCS and fuel design limits are not exceeded during specified incidents of moderate frequency.
- Initiate automatic protective action during limiting faults to aid the ESF systems in limiting the consequences of certain infrequent events and limiting faults.

A description of the reactor trips provided in the RPS is given in paragraph 7.2.1.1.1. Paragraph 7.2.2.2 provides the bases for all the RPS trips and table 7.2-1 gives the applicable trip setpoints.

Most of the trips in the RPS are single parameter trips (i.e., a trip signal is generated by comparing a single measured variable with a fixed setpoint). The RPS trips that do not fall into this category are as follows:

A. Low pressurizer pressure trip

This trip employs a setpoint that is determined as a function of the measured pressurizer pressure or that is varied by the operator.

B. Low steam generator pressure trip

This trip employs a setpoint that is determined as a function of the measured steam generator pressure or that is varied by the operator.

C. High local power density trip

This trip is calculated as a function of several measured variables.

D. Low DNBR trip

This trip is calculated as a function of several measured variables.

E. Variable overpower trip

This trip employs a setpoint that will track the reactor power as indicated by neutron flux measurements as long as the rate of change is low enough. A fixed ceiling on the setpoint is also incorporated.

F. Low reactor coolant flow trip

This trip employs a setpoint that is determined as a function of the rate of change of the differential pressure across the primary side of the steam generator, a fixed setpoint rate, a predetermined offset from the measured variable, and a minimum limit.

The low DNBR and high LPD trips are provided in the CPCs. All RPS trips are provided with a pre-trip alarm in addition to the trip alarm. Pre-trip alarms are provided to alert the operator to an approach to a trip condition and play no part in the safety evaluation of the plant.

Each RPS setpoint is chosen to be consistent with the function of the respective trip. The adequacy of all RPS trip setpoints,

with the exception of the low DNBR and high LPD trips, is verified through an analysis of the pertinent system transients reported in chapter 15. These analyses utilize an analysis setpoint (assumed trip initiation point) and system delay times associated with the respective trip functions. The analysis setpoint along with instrument uncertainties provides the basis for the calculation of the final equipment setpoints to be reported in the Technical Specifications and UFSAR. Limiting trip delay times are given in chapter 15. The manner by which these delay times and uncertainties will be verified is discussed in paragraph 7.2.1.2.

The adequacy of the low DNBR and high LPD trips was certified by a combination of static and dynamic analyses. These analyses provide assurance that the low DNBR and high LPD trips function as required, and provide the justification for the CPC time response assumed in the chapter 15 safety analyses. This is accomplished by certifying that algorithms used in these two trips predict results that are conservative with respect to the results obtained from standard design methods, models, and computer codes used in evaluating plant performance. This verification also takes into account all errors and uncertainties associated with these two trips, in addition to trip delay times, and will assure that the consequences of any incidents of moderate frequency do not include violation of specified acceptable fuel design limits. Examples of the computer codes that will be used in this verification are given in chapter 15.

7.2.2.1.1 Incidents of Moderate Frequency and Infrequent Events

Incidents of moderate frequency and infrequent events that are accommodated by the system are those conditions that may occur

one or more times during the life of the plant. In particular, the occurrences considered include single component or control system failures resulting in transients which may require protective action.

The fuel design and RCPB limits used in the RPS design for incidents of moderate frequency are:

- The DNBR, in the limiting coolant channel in the core, shall not be less than the DNBR safety limit;
- The peak LPD in the limiting fuel pin in the core shall not cause the peak fuel centerline temperature safety limit to be exceeded; and
- The RCS pressure shall not exceed established pressure boundary limits.

The incidents of moderate frequency and infrequent events that provide the basis for the system design requirements are:

A. Insertion or withdrawal of full-strength or part-strength CEA groups, including:
    - Uncontrolled sequential withdrawal of CEA groups,
    - Out-of-sequence insertion or withdrawal of CEA groups,
    - Malpositioning of the part-strength CEA group, or
    - Excessive sequential insertion of full-strength CEA groups;

B. Insertion or withdrawal of full-strength or part-strength CEA subgroups, including:
    - Uncontrolled insertion or withdrawal of a CEA subgroup,

- Dropping of one CEA subgroup, or
- Misalignment of CEA subgroups assigned to a designated CEA group;

C. Insertion or withdrawal of a single full-strength or part-strength CEA, including:

- Uncontrolled insertion or withdrawal of a single full-strength or part-strength CEA,
- A dropped full- or part-strength CEA,
- A single CEA sticking, with the remainder of the CEAs in that group moving, or
- A statically misaligned CEA;

D. Uncontrolled boron dilution;

E. Excess heat removal due to secondary system malfunctions;

F. Change of forced reactor coolant flow resulting from a simultaneous loss of electrical power to all reactor coolant pumps;

G. Inadvertent pressurization or depressurization of RCS resulting from anticipated single control system malfunctions;

H. Change of normal heat transfer capability between steam and reactor coolant systems resulting from improper feedwater flow or a loss of external load and/or turbine trip;

I. Complete loss of ac power to the station auxiliaries;

J. Asymmetric steam generator transient due to instantaneous closure of one MSIV; and

K. Uncontrolled axial xenon oscillations.

7.2.2.1.2 Limiting Faults

The limiting faults for which the system will take action are those unplanned events under any conditions that may occur once during the life of several stations, and certain combinations of unplanned events and degraded systems that are never expected to occur. The consequences of most of these limiting faults will be limited by the ESF systems; the RPS will provide action to assist in limiting these conditions for these limiting faults. The limiting faults for which the RPS will provide protective action assistance are:

- RCS pipe rupture, including double-ended rupture;
- Ejection of any single CEA;
- Steam system pipe rupture, including a double-ended rupture;
- Feedwater system pipe rupture, including a double-ended rupture;
- Reactor coolant pump shaft seizure;
- Depressurization due to inadvertent actuation of primary or secondary safety valves at 100% power;
- A reactor coolant pump sheared shaft; and
- Steam generator tube rupture.

7.2.2.2 Trip Bases

The RPS consists of fifteen trips in each RPS channel that will initiate the required automatic protective action utilizing a coincidence of two like trip signals.

A brief description of the inputs and purpose of each trip is presented in paragraphs 7.2.2.2.1 through 7.2.2.2.11.

7.2.2.2.1 Variable Overpower Trip

7.2.2.2.1.1 Input. The input is neutron flux power from the excore neutron flux monitoring system.

7.2.2.2.1.2 Purpose. This trip assures the integrity of the fuel cladding and RCS boundary in the event of a very rapid power increase, resulting from an uncontrolled withdrawal of CEAs from an initial Hot Zero Power condition. This trip also provides a reactor trip to assist the ESF systems in the event of an ejected CEA limiting fault.

7.2.2.2.2 High Logarithmic Power Level Trip

7.2.2.2.2.1 Input. The input is neutron flux power from the excore neutron flux monitoring system.

7.2.2.2.2.2 Purpose. This trip assures the integrity of the fuel cladding and RCS boundary in the event of unplanned criticality from a shutdown condition, resulting from either dilution of the soluble boron concentration or uncontrolled withdrawal of CEAs. In the event that CEAs are in the withdrawn position, automatic trip action will be initiated. If all CEAs are inserted, the boron dilution alarm system provides an alarm to alert the operator to take appropriate action in the event of an unplanned criticality. The boron dilution alarm system provides high neutron flux alarms to the main control room from the startup channels. This system is separate from, and independent of, the high logarithmic power level trip. The boron dilution alarm system is described in Section 7.7.1.1.11.

7.2.2.2.3 High Local Power Density Trip

7.2.2.2.3.1 Inputs. The inputs are

- Neutron flux power and axial power distribution based on the excore neutron flux monitoring system;
- Radial peaking factors based on CEA position measurement system (RSPTs);
- ΔT power based on coolant temperatures, pressure, and RCP speed measurements;
- Penalty factors from CEACs for CEA deviation within a subgroup; and
- Penalty factors generated within the CPC for subgroup deviation and groups out-of-sequence.

7.2.2.2.3.2 Purpose. This trip prevents the linear heat rate (kW/ft) in the limiting fuel pin in the core from exceeding fuel design limits for incidents of moderate frequency, and also to provide assistance in limiting conditions for certain infrequent events and limiting faults.

7.2.2.2.4 Low DNBR Trip

7.2.2.2.4.1 Inputs. The inputs are

- Neutron flux power and axial power distribution based on the excore neutron flux monitoring system;
- RCS pressure from pressurizer pressure measurement;
- Delta T power based on coolant temperatures, pressure, and RCP speed measurements;
- Radial peaking factors based on CEA position measurement (RSPTs);

- Reactor coolant mass flow based on reactor coolant pump speeds and temperatures;
- Core inlet temperature from reactor coolant cold leg temperature measurements;
- Penalty factors from CEACs for CEA deviation within a subgroup; and
- Penalty factors generated within the CPC for subgroup deviation and groups out-of-sequence.

7.2.2.2.4.2 Purpose. This trip prevents the DNB ratio in the limiting coolant channel in the core from exceeding the fuel design limit in the event of defined incidents of moderate frequency. In addition, this trip will provide a reactor trip to assist the ESF systems in limiting the consequences of the steam line break outside containment, steam generator tube rupture, and reactor coolant pump shaft seizure limiting faults.

7.2.2.2.5 High Pressurizer Pressure Trip

7.2.2.2.5.1 Input. The input is reactor coolant pressure from narrow range (1500 to 2500 psia) pressurizer pressure measurement.

7.2.2.2.5.2 Purpose. This trip helps assure the integrity of the RCS boundary for any defined incident of moderate frequency or infrequent incident that could lead to an overpressurization of the RCS.

7.2.2.2.6 Low Pressurizer Pressure Trip

7.2.2.2.6.1 Input. The input is reactor coolant pressure from wide range (0 to 3000 psia) pressurizer pressure measurement.

7.2.2.2.6.2 Purpose. This trip provides a reactor trip in the event of reduction in system pressure, in addition to the DNBR trip, and to provide a reactor trip to assist the ESF systems in the event of a LOCA.

7.2.2.2.7 Low Steam Generator Water Level Trips

7.2.2.2.7.1 Input. The input is the level of water in each steam generator downcomer region from wide range differential pressure measurements.

7.2.2.2.7.2 Purpose. These trips provide protective action to assure that there is sufficient time for actuating the auxiliary feedwater pumps to remove decay heat from the reactor in the event of a reduction of steam generator water inventory.

7.2.2.2.8 Low Steam Generator Pressure Trips

7.2.2.2.8.1 Input. The input is the steam pressure in each steam generator.

7.2.2.2.8.2 Purpose. These trips provide a reactor trip to assist the ESF systems in the event of a steam line break.

7.2.2.2.9 High Containment Pressure Trip

7.2.2.2.9.1 Input. The input is pressure inside reactor containment.

7.2.2.2.9.2 Purpose. This trip assists the ESF systems by tripping the reactor coincident with the initiation of safety injection caused by excess pressure in containment.

7.2.2.2.10 High Steam Generator Water Level Trips

7.2.2.2.10.1 Input. The input is the level of water in each steam generator downcomer region from narrow range differential pressure measurements.

7.2.2.2.10.2 Purpose. These trips assist the ESF systems by tripping the reactor coincident with initiation of main steam isolation caused by a high steam generator water level.

7.2.2.2.11 Low Reactor Coolant Flow

7.2.2.2.11.1 Input. The input is pressure differential measured across the steam generator primary side.

7.2.2.2.11.2 Purpose. This trip provides a reactor trip in the event of a reactor coolant pump sheared shaft.

7.2.2.3 Design

7.2.2.3.1 General Design Criteria

Appendix A of 10CFR50, "General Design Criteria for Nuclear Power Plants", establishes minimum requirements for the principle design criteria for water-cooled nuclear power plants. This section describes how the requirements that are applicable to the RPS are satisfied.

Criterion 1 - Quality Standards and Records: Refer to subsection 3.1.1 for compliance.

Criterion 2 - Design Bases for Protection Against Natural Phenomenon: Refer to subsection 3.1.2 for compliance.

Criterion 3 - Fire Protection: Refer to subsection 9.5.1 for compliance.

Criterion 4 - Environmental and Missile Design Bases: Refer to subsection 3.1.4 for compliance.

Criterion 5 - Sharing of Structures, Systems, and Components: Refer to section 3.1.5 for compliance.

Criterion 10 - Reactor Design: Refer to subsection 3.1.6 for compliance. Typical margins between the normal operating value and the trip setpoint are given in table 7.2-1.

Criterion 12 - Suppression of Reactor Power Oscillations: Refer to subsection 3.1.8 for compliance.

The axial power distribution is continuously monitored by the RPS and factored into the low DNBR and high LPD trips. This assures that acceptable fuel design limits are not exceeded in the event of axial power oscillations. Allowances are made in the trip setpoints for azimuthal power tilts.

Criterion 13 - Instrumentation and Control: Refer to subsection 3.1.9 for compliance.

Criterion 15 - Reactor Coolant System Design: Refer to subsection 3.1.11 for compliance.

Criterion 16 - Containment Design: Refer to subsection 6.2.4 and subsection 3.1.12.

Criterion 20 - Protection System Functions: Refer to subsection 3.1.16 for compliance.

Criterion 21 - Protection System Reliability and Testability: Refer to subsection 3.1.17 for compliance.

Criterion 22 - Protection System Independence: Refer to subsection 3.1.18 for compliance.

Criterion 23 - Protection System Failure Modes: Refer to subsection 3.1.19 for compliance.

Criterion 24 - Separation of Protection and Control Systems: Refer to subsection 3.1.20 for compliance.

Criterion 25 - Protection System Requirements for Reactivity Control Malfunctions: Refer to subsection 3.1.21 for compliance.

Criterion 29 - Protection Against Anticipated Operational Occurrences: Refer to subsection 3.1.25 for compliance.

7.2.2.3.2 Equipment Design Criteria

IEEE 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," establishes minimum requirements for safety-related functional performance and reliability of the RPS. This section describes how the requirements of Section 4 of IEEE 279-1971 are satisfied. As an exception, the PVNGS design provides a mono-directional data link from the core protection calculator (CPC) system to the plant monitoring system by means of fiber-optic communication. These data links are identical to the hardware utilized at each CEA calculator output (see paragraph 7.2.1.1.2.2). The non-conducting fiber-optic cable used ensures that no electrical failure at the plant monitoring system will affect the core protection calculators or the CEA calculators. The following heading numbers correspond to the section numbers of IEEE 279-1971.

7.2.2.3.2.1 Section 4.1, General Functional Requirement. The RPS is designed to limit reactor fuel, fuel cladding, and coolant conditions to levels within plant and fuel design limits. Instrument performance characteristics, response times, and accuracy are selected for compatibility with and adequacy for the particular function. Trip setpoints are established by analysis of the system parameters. Factors such as instrument inaccuracies, bistable trip times, CEA travel times, and circuit breaker trip times are considered in the design of the system.

7.2.2.3.2.2 Section 4.2, Single Failure Criterion. The RPS is designed so that any single failure within the system shall not prevent proper protective action at the system level. No single failure will defeat more than one of the four protective channels associated with any one trip function. The wiring in the system is grouped so that no single fault or failure, including either an open or shorted circuit, will negate protective system operation. Signal conductors and power leads coming into or going out of each cabinet are protected and routed separately for each channel of each system to minimize possible interaction. Single failures considered in the design of the RPS are described in the failure modes and effects analysis (FMEA) shown on table 7.2-4A. Also see reference 24 for the FMEA of the upgraded Core Protection Calculator System (CPCS).

7.2.2.3.2.3 Section 4.3, Quality Control of Components and Modules. The systems which function to provide protective action are designed in accordance with Topical Report CENPD-210A, "Description of the C-E Nuclear Steam Supply System Quality Assurance Program".[5]

7.2.2.3.2.4 Section 4.4, Equipment Qualification. The RPS meets the equipment requirements described in section 3.10 and CENPD-182, "Seismic Qualification of Instrumentation and Electrical Equipment",[4] and section 3.11 and CENPD-255, "Qualification of Combustion Engineering Class 1E Instrumentation".[3]

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 1 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
1) Excore Flux Monitor (68)	a) Low Output.	Loss of H.V. Power Supply Breakdown in insulation Resistance	Loss of data, erroneous data. Failure to detect HI flux levels.	Not annunciating. Automatic sensor. validity test. 3-channel comparison. Periodic manual test	3-channel redundancy. (4th channel in bypass)	Makes reactor Trip Logic for variable overpower HI LOG PWR, LO DNBR and HI PWR DENS 1-out-of-2 coincidence	Loss of H.V. Power Supply will fail all three subchannel detectors. To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
	b) High Output	Detector shorts, continuous ionization	Erroneous data. Possible channel Trip for Trip for HI LINEAR PWR, LO DNBR, HI LOG PWR, or HI PWR DENSITY	Annunciating Pre-Trip and Trip HI LIN PWR alarm. Nuclear Instrument Inoperative Alarm	3-channel redundancy. (4th channel bypass)	Makes reactor Trip Logic for HI LIN PWR, LO DNBR, and HI PWR DENS 1 out-of-2 coincidence Power Reduction Signals (PRS) Logic 1-out-of-2 coincidence	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
2) Core Out-Let Temp. $T_{hot(80)}$	a) Low Output.	Power supply failure. RTD bridge network failure	Reduces ΔT power indication. Channel will not trip on a valid hi temp. condition.	Annunciating. Automatic sensor validity test. 3-channel comparison Plant Computer monitor and alarm Periodic test.	3-channel redundancy. (4th channel bypass)	Reactor Trip Logic for LO DNBR and HI PWR DENS is converted to 2-out-of-2 coincidence.	Calculated values of DNBR calibrated nuclear power and local power density (LPD) will change. To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 2 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	b) High Output	RTD opens or Network failure.	Increases ΔT power indication. Possible channel trips (DNBR, LPD).	Annunciating	3-channel redundancy. (4th channel bypass)	Reactor Trip Logic for LO DNBR and HI PWR DENS is converted to 1-out-of-2 coincidence	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
3) Core Inlet Temperature T_{hot} (82)	a) One spurious low.	Power Supply failure. RTD bridge network failure.	Increases ΔT power indication. Possible channel trips (DNBR, LPD).	Annunciating. Automatic sensor. validity test . 3-channel comparison plant computer monitor and alarm. Periodic test	3-channel redundancy. (4th channel bypass)	Reactor Trip Logic for LO DNBR and HI PWR DENS is converted to 1-out-of -2 coincidence	To restor the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
	b) One spurious high	RTD opens network failure.	Decrease in ΔT power indication. Channel not trip if T_{cold} goes low.	Annunciating.	3-channel redundancy. (4th channel bypass)	Reactor trip logic for LO DNBR and HI PWR DENS is converted to 2-out-of-2 coincidence	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
4) Reactor Coolant Pump speed sensor (84)	a) One spurious loss of transmission	Power supply or pulse amplifier failure, mech. damage to sensor.	Loss of data. Low DNBR channel trip possible.	Annunciating. Plant Computer monitor and alarm, trip status indication.	3-channel redundancy trip bypass.	Reactor trip logic for LO DNBR is converted to 1-out-of-2 coincidence.	Sensor transmits pulses. Pulse rate related to flow. To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 3 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	b) High signal rate.	Electronic noise.	HI RCP speed input to CPC indicating hi RCS flow, or normal flow when flow actually low. Calculated DNBR will be high channel will not trip on valid low RCS flow.	3-channel comparison, periodic test.	3-channel redundancy. (4th channel in bypass)	RCP trip logic for lo DNBR becomes 2-out-of-2 coincident.	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
	c) Low signal rate.	High resistance in lines, loss of signal strength, intermittent failure.	Low RCP speed input to CPC indicating lo RCS flow. Possible lo DNBR trip in channel.	Pre-trip/trip alarms, 3-channel comparison, periodic test.	3-channel redundancy. (4th channel in bypass)	RPS trip logic for lo DNBR would become 1-out-of-2 coincident.	To restor the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
5) Non-Target CEA Position (149)	a) Low or High	Shorted resistor, power supply malfunction.	Erroneous data input to CEA calculator.	Annunciation. Automatic sensor validity test, CEA deviation.	A penalty factor.	A penalty factor is initiated in the core protection calculators (operating temperature margins reduced).	One CEA calculator in each channel will show CEA deviation to all CPC calculators. Possible reactor trip will occur.

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 4 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	b) Other than actual position.	Shorted resistors, shorted reed switches, power supply malfuction.	Erroneous data input to two CEA calculator.	Annunciation, automatic sensor validity test, CEA deviation.	A penalty factor.	A penalty factor is initiated in the core protection calculators (operating temperature margins reduced).	One CEA calculator will show CEA deviation to all CPC calculation. Possible reactor trip will occur.
	c) Off scale	Broken wire, open resistor, electrical short, power supply malfunction.	Loss of data.	Annunciation, automatic sensor validity test, CEA deviation.	A penalty factor.	A penalty factor is initiated in the core protection calculators (operating temperature margins reduced).	One CEA calculator will show CEA deviations to all CPC calculation. Possible reactor trip will occur.
	d) Single CPP failure	Module failure. CEA position data link failure	Loss of one of two redundant CEA position inputs to 1 CEAC in 1 or more channels	Annunciation and alarm	Reduadant CPP in each channel provides CEA position input to CEAC	None	There are two redundant CPPs and associated CEA position data links each CPC channel
	e) Failure of both CPPs in one channel	Power supply failure	Loss of both redundant CEA position inputs to 1 CEAC in all four channels. Loss of CEA position display if that channel is selected for display	CEAC Fail alarm and annunciation	Two channel redundancy (two CEACs per channel) CPC uses other CEAC.	None	CPC uses data from the other CEAC and annunciates failure CPP failure will also cause loss of target CEA position input in the failed channel
6) Target CEA Position (87)	a) Low	Shorted resistor, power supply malfunction	Erroneous data input affects DNBR and LPD calculation	Annunciation, automatic sensor validity test, 3-channel comparison	3-channel redundancy. (4th channel in bypass)	Makes reactor trip logic for LO DNBR and HI power density 1-out-of-2 coincidence	Possible trip in one safety channel. Trip effected will show CEA deviation.
	b) High	Shorted resistor, power supply malfunction	Erroneous data input to CPC Calculator and (two) CEA Calculators	Annunciation, automatic sensor validity test, CEA deviation.	3-channel redundancy. (4th channel in bypass)	Makes reactor trip logic for LO DNBR and HI power density 1-out-of-2 coincidence.	Possible trip in one safety channel. Trip effected will show CEA deviation.
	c) Other than actual position.	Shorted resistor, shorted reed switches,power supply malfunction.	Erroneous data input to Core Protection Calculators and (two) CEA Calculators.	Annunciation, automatic sensor validity test. CEA deviation.	3-channel redundancy. (4th channel in bypass)	Makes reactor trip logic for LO DNBR and HI POWER DENS 1-out-of-2 coincidence.	Possible trip in one safety channel. Trip effected will show CEA deviation.

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 5 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	d) Off scale	Broken wire, open resistor, electrical short, power supply mal-function	Loss of data	Annunciation; automatic sensor validity test. CEA deviation.	3-channel redun-dancy. (4th channel in bypass)	Makes reactor trip logic for LO DNBR and HI PWER DENS 1-out-of 2 coinci-dence.	Possible trip in one safety channel. Trip effected will show CEA deviation.
	e) Single CPP failure	Module failure. CEAC to CPC data link failure	Loss on one of two redundant CEA position inputs to CPC in the same channels	Annunciation and alarm	Redundant Target CEA position input from other CEAC to CPC data link provides CEA position input to CPC	None	There are two redundant CPPs and CEAC to CPC data links in each CPC channel. Target CEA position is redundantly transmitted.
	f) Failure of both CPPs in one channel	Power supply failure	Loss of both redundant Target CEA position inputs to one CPC channel	CPC Fail. Low DNBR and High power density channel trips, alarm and annunciation	Three channel redundancy (4th channel in bypass)	Makes reactor trip logic for Low DNBR and High Power Density 1 out of 2 coincidence	Diagnostic message identify cause of trip
7) Wide Range PZR pressure (press) signal (61)	a) One fails on. (High pressure signal level)	Sensor failure, component failure.	High PZR press signal to: LP PZR Press P/S. LO PZR pressure B/S does not trip for a bona fide condition	Periodic test; 3 channel comparison	3-channel redun-dancy. (4th channel in bypass)	Reactor Trip logic for LP PZR Press is coverted to 2-out-of-2 concidence and CSAS, SIAS logic LO PZR Press 2-out-of-2 coincidence	Back-up for SIAS is the containment pressure measurement channel. To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
	b) One fails off. (Low pressure signal level).	Sensor failure; dc power supply fall; open circuit	Low PZR Press signal to LO PZR. Press B/S. Bistable changes logic state and initiates channel trip	Annunciating; pre-trip and trip alarm in channel	3-channel redun-dancy Trip Channel Bypass	Reactor trip logic for LO PZR Press is converted to 1-out-of-2 coincidence and CSAS, SIAS logic 1-out-of-2 coincidence	To restore the sys-tem logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 6 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
8) PZR Narrow Range Pressure (PRESS) Signal (91)	a)On (High pressure signal level)	Sensor failure, component failure	High PZR press signal to HI PZR Press B/S and calculator HI PZR PRESS B/S will change logic state and initiate channel trip	Annunciating, Pre-trip and trip alarms in HI PZR channel.	3-channel redundancy (4th channel in bypass)	Reactor TRIP logic for LO DNBR is converted to 2-out-of-2 coincidence for HI PZR PRESS. CWP becomes 1-out-of-2 coincidence for HI PZR PRESS	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
	b)Off (Low Pressure signal level)	Sensor failure, dc power supply fail open circuit	LO PZR PRESS B/S will decrease DNBR Margin and initiate LO DNBR channel trip. HI PZR PRESS B/S will not trip for bona fide condition	Annunciating; pre-trip and trip alarms in LO DNBR channel	3-channel redundancy (4th channel in bypass)	Reactor TRIP logic for LO DNBR is coverted to 1-out-of-2 coincidence. CWP logic becomes 2-out of-2 coincidence for this parameter.	To restore the sys tem logic to 2-out of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
9) SG No.2 Level Signal (51) SG NO.1 Level siganl (55) (Wide Range)	a)Off (Low signal level)	Sensor failure, dc power supply fail; open circuit	Low steam generator water level signal to channel bi-stables. Low level bistables (B/S) change logic state and trip channel for affected steam generator	Annunciation; Pre-trip and trip alarms on low steam generator water level	3-channel redundancy. (4th channel in bypass)	Reactor TRIP and AFAS logic for affected steam generator low water level is converted to 1-out-of-2coincidence	One channel inopera tive for affected steam generator To restore the sys tem logic to 2-out of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the fialed channel.

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 7 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	b) On (High Signal level)	Sensor failure, component failure	High steam generator water level signal to channel bistables. Lo level bistables for affected steam generator will not trip on LO level	Annunciation on high S/G level. Periodic test, 3-channel comparision	3-channel redundancy. (4th channel in bypass)	Reactor TRIP and AFAS logic for low steam generator water level is converted to 2-out-of-2 coincidence for affected steam generator. System will still operate on non-failed SG level	One channel inoperative for affected steam generator. To restore the system logic to 2-out of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
10) Narrow Range level Sensor, Steam Generator No. 1 (20); Narrow Range Level Sensor, Steam Generator No. 2 (19)	a) Off (Low Signal Level)	Sensor failure, dc power supply fail open circuit	Lo Level Signal to one High SG level bistable for the affected steam generator. Bistable will not trip on actual HI level in steam generator	Periodic test, 3-channel comparison	3-channel redundancy (4th channel in bypass)	Reactor Trip Logic for HI steam generator level and the MSIS actuation Logic for HI steam Generator Level will be changed to 2-out-of-2	To restore the system logic to 2-out of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
	b) On (High Level Signal)	Sensor failure component failure	False HI Level Signal sent to one steam generator HI Level Bistable for affected steam generator. Bistable will change logic state and trip the channel	Channel pre-trip and trip alarms	3-channel redundancy (4th channel in bypass)	Reactor Trip Logic and MSIS actuation logic for HI steam generator logic on the affected steam generator will be changed to 1-out of-2	Same as above

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 8 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
11) S/G Pressure Signal No. 2 (27) S/G Pres-sure signal No. 1 (42)	a) One spurious off, (Low signal level)	Sensor failure, dc power fail; open circuit	Low steam generator pressure signal to SG Low Pressure (LO PRESS) bistable (B/S) in RPS and ESFS channels, SG Low Pressure, SG1.SG2, and SG2.SG1 B/S's. B/S's change their logic state and initiates channel trip in SG LO PRESS for reactor TRIP, and MSIS actuation. Also, differential 8 SG pressure signal input to one AFAS train actuation logic.	Annunciating; pre-trip and trip alarm on low steam generator pressure	3-channel redundancy (4th channel in bypass)	Reactor TRIP logic for steam generator steam pressure is converted to 1-out-of-2 coincidence	To restore the sys tem logic to 2-out of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
	b) One spurious on, (High signal level)	Sensor fails component failure	High steam generator pressure signal to SG LO PRESS and SG1.SG2 Press or SG2.SG1 Press Bistables. One SG LO Press Channel for affected SG will not trip for valid LO Press condition. The SG1.SG2 Press (or SG2.SG1) Bistables will change state	Annunciating; periodic rest. 3-channel comparison	3-channel redundancy (4th channel in bypass)	AFAS Reactor Trip and MSIS actuation Logic for LO SG Press changes to 2-out-of-2. AFAS actuation logic for opposite SG changes to 2-out-of-2	To restore the sys tem logic to 2-out of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 9 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
12) SG1 Diff.Pres. Signal, (13) SG2 Diff. Pres. Signal (12)	a) One fails on (High signal level)	Sensor failure, other component failure	HI or normal differential pres. Signal received by one SG LO FLOW bistable for affected steam generator. One channel will not trip on valid LO flow condition in affected steam generator	Periodic test, 3-channel comparison	3-channel redundancy (4th channel in bypass)	Reactor Trip Logic for LO flow in affected SG changes to 2-out-of-2	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
	b) One fails off (LO signal level)	Sensor fails dc power failure, open circuit	LO Differential pres. signal received by one SG LO Flow bistable for affected steam generator. Bistable will change state, initiating a channel trip	Annunciating	3-channel redundancy (4th channel in bypass)	Reactor Trip Logic for LO flow in affected SG changes to 1-out-of-2	Same as above
13) Containment Pressure Signal (6)	a) ON (goes high)	Component failure	High CONT PRESS signal to: HI CONT PRESS bistable in RPS channel and in ESFS channel. B/S change logic state, and initiates channel trip for high containment pressure for RPS TRIP, SIAS, CIAS, and MSIS actuation	Annunciating; pre-trip, and alarm on high containment pressure ESF channel indication	3-channel redundancy (4th channel in bypass)	Reactor Trip Logic redundacy pressure is converted to 1-out-of-2 coincidence and CIAS, SIAS and MSIS logic for HI containment pressure 1-out-of-2 coincidence	Same as above

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 10 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	b) Off goes low)	Component failure, dc power supply failure open circuit.	Low CONT PRESS signal to: HI CONT PRESS B/S in RPS channel, and ESFS channel. B/S in channel do not change their logic state and trip for bona fide high contan-ment condition	Periodic test 3-channel com-parison	3-channel redundancy (4th channel in bypass)	Reactor Trip logic for HI containment pressure is con-verted to 2-out-of-2 coincidence, and CIAS, SIAS, and SMIS logic for HI containment pres-sure 2-out-of-2 coincidence	To restore the sys-tem logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
14) Con-tainment Pressure Signal (10)	a) ON (HI Signal Level)	Sensor failure other component failure	HI Cont. Pres. Signal received by one HI-HI cont. pres. bi-stable changes state, initiating channel trip for CSAS actuation	Annunciating	3-channel redundancy (4th channel in bypass)	Actuation logic for CSAS becomes 1-out-of-2	Same as above
	b) Off (LO signal level)	Sensor dc power supply failure, open circuit	One HI-HI Cont. Pres. bistable constantly receives a LO or normal containment pres. signal. Bistable will not change logic state for a valid HI-HI cont. pres. condition	Periodic test 3-channel comparison	3-channel redundancy (4th channel in bypass)	Actuation logic for CSAS changes to 2-out-of-2	Same as above
15) RWT Level Signal (1)	a) Off (goes low)	Failed Sensor dc power supply fails	Low RWT level signal to REFUEL TANK LO LEVEL Bistable in ESFS channel. Bistable changes logic state and initiates channel trip for RAS actuation in ESFS	Annunciating; pre-trip and trip PPS alarms	3-channel redundancy (4th channel in bypass)	Makes RAS logic for low refueling water tank level 1 out of 2 coincidence	Same as above
	b) On (goes high)	Sensor fails; component failure	High RWT level signal to REFUEL TANK LO LEVEL Bistable in ESFS channel. Bistable will not change logic state in RAS channel when bona fide low RWT level condition exists	Periodic test 3-channel comparison	3-channel redundancy (4th channel in bypass)	Makes RAS logic for low refueling water tank level 2 out of 2 coincidence	Same as above

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 11 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
16) Refueling Water Tank LO Level Bistable (2), Channel A typical)	a) Setpoint power fails off	Component failure, open circuit.	Refueling Water Tank (RWT) level setpoint drops to zero Bistable will not change state on valid LO level signal	Periodic test	3-channel redundancy (4th channel in bypass)	RAS Actuation Logic changes to 2-out-of-2	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
	b) Trip Setpoint fails low	Component failure	Same as 16 a)	Same as 16 a)	Same as 16 a)	Same as 16 a)	Same as 16 a)
	c) Trip setpoint set fails high	Component failure	Bistable will trip at a greater than desired RWT level	Periodic test	3-channel redundancy (4th channel in bypass)	No impact on RAS actuation logic unless bistable trips at normal RWT level, then actuation logic will become 1-out-of-2	Same as above
	d) Trip voltage comparator fails off	Open circuit, component failure	Bistable relays will be deenergized resulting in half trips in the AB, AC and AD RAS Actuation Logic matrices	Annunciating	3-channel redundancy (4th channel in bypass)	RAS actuation logic becomes 1 out-of-2	Same as above
	e) Trip voltage comparator fails on	Component failure	Bistable relays will not be deenergized for a valid LO RWT Level Signal	Periodic test	3-channel redundancy (4th channel in bypass)	RAS actuation logic becomes 2-out-of-2	Same as above
	f) Pre-trip setpoint set fails low or off	Component failure, open circuit	Pre-trip setpoint decreases, pre-trip relay will not de-energize when RWT level reaches desired pre-trip level	Periodic test	3-channel redundancy (4th channel in bypass)	RAS Pre-trip indication logic will change to 1-out-of-2. No impact on RAS actuation logic	Same as above

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 12 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	g) Pre-Trip setpoint set fails HI	Component failure	Pre-trip relay will be de-energized at a higher than desired RWT level	Pre-trip alarm and test	None	Spurious RAS Pre-trip alarms. No impact on RAS actuation logic	Same as 16 c)
	h) Pre-trip voltage comparator fails off	Open circuit component failure	Same as 16 g)	Same as 16 g)	Same as 16 g)	Same as 16 g)	Same as 16 g)
	i) Pre-trip voltage comparator fails on	Component failure	Pre-trip relay will not be deenergized when RWT level reached pre-trip setpoint level	Periodic test	3-channel redundancy (4th channel in bypass)	RAS Pre-trip indication logic changes to 1-out-of-2	Same as above
	j) Pre-trip Opto-isolator fails off	Open circuit, component	Pre-trip relay will be deenergized	Annunciating	None	Spurious Pre-trip alarms. RAS actuation logic not affected	Same as above
	k) Pre-trip relay driver fails off	Open circuit transistor failure	Same as 16 j)	Same as 16 j)	Same as 16 j)	Same as 16 j)	Same as 16 j)
	l) Pre-trip relay driver fails on	Emittor to collector short circuit	Same as 16 i)	Same as 16 i)	Same as 16 i)	Same as 16 i)	Same as 16 i)
	m) Pre-trip relay coil fails open	Mechanical failure	Same as 16 j)	Same as 16 j)	Same as 16 j)	Same as 16 j)	Same as 16 j)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 13 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	n) Pre-trip relay NC contact in annun-ciator circuit fails open	Corrosion mechanical damage	RAS pre-trip for channel A will not be annunciated	Periodic test	Visual indication not affected, 3-channel redundancy (4th channel in bypass)	RAS actuation logic unaffected, Pre-trip annun-ciation logic becomes 1-out-of-2	Same as 16 j)
	o) Pre-trip relay NC contact in annun-ciator circuit fails closed	Contact arcing	Spurious pre-trip alarm for RAS	Annunciating	None	RAS Actuation logic unaffected	Same as above
	p) Pre-trip relay NC contact in indi-cator circuit fails open	Mechanical damage corrosion	No visual indication of channel A pre-trip	Periodic test	Audible annun-ciation not affected, 3-channel redundacy (4th channel in bypass)	RAS Actuation logic unaffected pre-trip indica-tion log becomes 1-out-of-2	Same as above
	q) Pre-trip relay NC contact in indi-cator circuit fails closed	Contact arcing	Spurious RAS pre-trip indication	Visual pre-trip indication	None	RAS Actuation logic unaffected	Same as above
	r) Trip Opto-isolator fails off	Open circuit, component failure	Same as 16 d)	Same as 16 d)	Same as 16 d)	Same as 16 d)	Same as 16 d)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 14 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	s) Trip Relay Driver (TR1, TR2 TR3 or R4) fails off	Open circuit, transistor failure	One bistable relay coil de-energized resulting in a spurious half trip in one logic matrix (i.e. AB, AC, or AD) or a spurious trip indication.	Trouble annunciator for TR-1, 2 and 3 and trip indication for R4	3-channel redundancy for TR-1, 2, and 3 (4th channel in bypass)	RAS Actuation logic becomes 1-out-of-2 selective or any 2-out-of-3	Same as 16 j)
	t) Trip Relay Driver fails on	Emittor to collector short on transistor	Affected trip relay will not deenergize for valid RWT LO level signal, one RAS actuation logic matrix, (i.e., AB, AC or AD) will not deenergize	Periodic test	3-channel redundancy (4th channel in bypass)	RAS Actuation logic becomes 2-out-of-2	Same as above
	u) Trip Relay Coil (TR-1 TR-2, TR-3, or R-4) fails open	Mechanical failure	Same as 16 s)	Same as 16 s)	Same as 16 s)	Same as 16 s)	Same as 16 s)
	v) Trip Relay Form C contacts in logic matrix fail to the NC Pole	Contacts welded by arcing, fuse failure	Affected RAS actuation logic matrix becomes half tripped, and Channel A trip indicator in affected matrix illuminated	Visual indication	3-channel redundancy (4th channel in bypass)	RAS Actuation logic remains 2-out-of-3 with one logic matrix half tripped	Same as above
	w) Trip Relay form C contacts in logic matrix fail to the NO Pole	Contacts welded	The affected RAS Actuation logic matrix (AB, AC or AD) will not deenergize for valid RWT LO Level signal, and channel A trip indicator in affected matrix will not illuminate	Periodic test	3-channel redundancy (4th channel in bypass)	RAS actuation logic becomes 2-out-of-2	Same as above

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 15 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	x) Trip Relay Form C contacts in trouble annun. circuit fail to the NO Pole	Contacts welded	Relay coil or relay driver failure will not be annunciated by trouble annunciator	Periodic test	Channel trip indictors in logic matrixes will indicate possible relay coil or relay driver failures	RAS Actuation logic not affected	Same as 16 j)
	y) Trip Relay Form C Contacts in trouble annun. circuit fail to the NC Pole	Fuse failure contacts	Spurious relay coil/relay driver failure indications	Annunciating	None	RAS Actuation logic not affected	Same as above
17) SG1 LO Level Bi-stable (59) SG2 LO level Bistable (52) (Channel A typical)			Failure modes and the effects on RPS Trip Logic for LO steam generator level trips are equivalent to the failure modes and effects on RAS Actuation Logic provided in line item 16, Failure modes a) through y).				
18) HI-HI Cont. Pres. Bistable (7) (Channel A typical)	a) Trip setpoint power supply fails off	Open circuit, component failure	HI-HI cont pres. setpoint goes to zero, and all Channel A bistable relays are de-energized by trip voltage comparator	Annunciating	3-channel redundancy (4th channel in bypass)	CSAS Actuation logic is converted to 1-out-of-2	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
	Failure Modes b) through y), and the effects on CSAS Actuation Logic are equivalent to the Failure Modes and effects on RAS Actuation Logic provided in Line item 16, Failure Modes b) through y).						

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 16 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
19) SG1 HI Level Bistable (135), SG2 HI Level Bistable (134) (Channel A Typical)	a) Trip setpoint power supply fails off	Open circuit, component failure	HI SG Level setpoint goes to zero. All channel A bistable relays for RPS Trip Logic and ESF Actuation Logic for HI SG level are deenergized	Annunciating	3-channel redundancy (4th channel in bypass)	RPS Trip Logic and ESF Actuation Logic for HI SG Level is converted to 1-out-of-2.	To restore the system logic to 2-out-of-3 coincidence the operator must restore the bypassed channel to operation and then bypass the failed channel.
	b) Trip setpoint set fails low	Component failure	Same as 19 a)	Same as 19 a)	Same as 19 a)	Same as 19 a)	Same as 19 a)
	c) Trip setpoint set fails high	Component failure	Bistable will not change states for valid SG HI Level	Periodic test	3-channel redundancy (4th channel in bypass)	RPS Trip and ESF Actuation Logic for HI SG Level changes to 2-out-of-2	Same as 19 a)
	d) Trip Voltage Comparator fails off	Open circuit component failure	All Channel A bistable relays for RPS Trip and ESF Actuation Logic for HI SG Level will be deenergized. AB, AC and AD Logic matrixes will be half tripped	Annunciating	3-channel redundancy (4th channel in bypass)	RPS Trip and ESF Actuation Logic for HI SG Level changes to 1-out-of-2	Same as 19 a)
	e) Trip Voltage Comparator fails on	Component failure	Same as 19 c)	Same as 19 c)	Same as 19 c)	Same as 19 c)	Same as 19 a)
	f) Pre-trip setpoint set fails off or low	Open circuit, component fialure	Pre-trip relay for HI SG Level deenergized. Spurious HI SG Level Pre-trip indication	Annunciating	None	No impact on RPS Trip or ESF Actuation Logic. Spurious pre-trip indication	Same as 19 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 17 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	g) Pre-Trip setpoint set fails HI	Component failure	Pre-trip relay will not be de-energized when SG Level reaches pre-trip level. No pre-trip indic. From Channel A	Periodic test	3-channel redundancy (4th channel in bypass)	No impact on RPS Trip or ESF Actuation Logic, Pre-trip Logic changes to 1-out-of-2	Same as 19 a)
	h) Pre-Trip Voltage Comparator fails off	Open circuit, component failure	Same as 19 f)	Same as 19 f)	Same as 19 f)	Same as 19 f)	Same as 19 a)
	i) Pre-Trip Voltage Comparator fails on	Component failure	Same as 19 g)	Same as 19 g)	Same as 19 g)	Same as 19 g)	Same as 19 a)
	j) Pre-Trip Opto-Isolator fails off	Component failure	Same as 19 f)	Same as 19 f)	Same as 19 f)	Same as 19 f)	Same as 19 a)
	k) Pre-Trip Relay driver fails off	Open circuit, transistor failure	Same as 19 f)	Same as 19 f)	Same as 19 f)	Same as 19 f)	Same as 19 a)
	l) Pre-Trip Relay driver fails on	Emitter-to-collector short	Same as 19 g)	Same as 19 g)	Same as 19 g	Same as 19 g)	Same as 19 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 18 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	m) Pre-Trip Relay Coil fails open	Mechanical failure	Same as 19 f)	Same as 19 f)	Same as 19 f)	Same as 19 f)	Same as 19 a)
	n) Pre-Trip Relay Form C Contact in Annunc. Circuit fails open	Corrosion, mechanical damage	Channel A pre-trip on HI SG Level will not be annunciated	Periodic test	3-channel redundancy, visual pre-trip indicator (4th channel in bypass)	No impact on RPS or ESF actuation Logic	Same as 19 a)
	o) Pre-Trip Relay Form C Contacts in Annunc. circuit fail closed	Contact weld	Spurious HI SG Level pre-trip alarm	Annunciating	None	RPS trip and ESF Actuation Logic not affected	Same as 19 a)
	p) Pre-Trip Relay Form C Contact in Indicator Circuit fails open	Mechanical damage corrosion	No visual indication of Channel A pre-trip	Periodic test	3-channel redundancy, pre-trip annunciator (4th channel in bypass)	Same as 19 o)	Same as 19 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 19 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	q) Pre-Trip Relay Form C Contacts in indicator circuit fails closed	Contact weld	Spurious visual pre-trip indication	Visual pre-trip indication	None	Same as 19 o)	Same as 19 a)
	r) Trip Opto-isolator fails off	Open circuit, transistor failure	Same as 19 d)	Same as 19 d)	Same as 19 d)	Same as 19 d)	Same as 19 a)
	s) Actuation Relay Driver (TR1, TR2 TR3, R4, R9, R10, or R11) fails off	Open circuit, transistor failure	One actuation relay coil is deenergized, resulting in spurious half trip in one RPS Trip Logic Matrix (i.e. AB, AC, or AD), a spurious trip indication, or a half trip in one ESF Actuation Logic Matrix	Annunciating	3-channel redundancy, for TR1, TR2, TR3 R9, R10, and R11. (4th channel in bypass)	RPS Trip and ESF Actuation Logic remains 2-out-of-3	Same as 19 a)
	t) Actuation Relay Driver fails on	Short circuit	One actuation relay coil will not be deenergized for valid HI SG Level. One RPS Trip, or one ESF actuation logic matrix (i.e., AB, AC, or AD) will not de-energize	Periodic test	3-channel redundancy (4th channel in bypass)	Either RPS trip or ESF actuation logic will change to 2-out-of-2	Same as 19 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 20 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	u) Actuation Relay Coil fails open	Mechanical failure	Same as 19 s)	Same as 19 s)	Same as 19 s)	Same as 19 s)	Same as 19 a)
	v) Actuation Relay (TR1, TR2 TR3, R9, R10, or R11) Form C contacts in Logic Matrix fail to NC Pole	Contact weld, fuse failure	Affected logic matrix (AB, AC, or AD for RPS Trip or ESF Actuation) becomes half tripped, Channel A trip indicator in affected matrix is illuminated	Visual indication	3-channel redundancy (4th channel in bypass)	RPS Trip or ESF Actuation Logic for HI SG Level remains 2-out-of-3 with one logic matrix half tripped	Same as 19 a)
	w) Actuation Relay Form C Contacts in Logic Matrix fail to NC Pole	Contact weld	Affected Logic Matrix (AB, AC, or AD for RPS Trip or ESF Actuation) will not be de-energized for a valid HI SG Level signal	Periodic test	3-channel redundancy (4th channel in bypass)	RPS trip or ESF Actuation Logic for HI SG Level becomes 2-out-of-2	Same as 19 a)
	x) Actuation Relay Form C Contacts in trouble annunc. Circuit fail to NC Pole	Contacts welded	Relay coil or relay driver failure will not be annunciated by trouble annunciator	Periodic test	Channel trip indicators in logic matrices will indicate possible relay coil or driver failures	RPS Trip and ESF Actuation Logic not affected	Same as 19 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 21 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
20) HI Containment Pressure Bistable(24) (Channel A typical) 21) HI Pressure Bistable (65) (Channel A Typical)	y) Actuation Relay Form C contacts in trouble annunc. circuit fail to NC Pole	Fuse failure contact weld	Spurious relay coil/driver failure indication	Annunciating	None	Same as 19 x)	Same as 19 a)
			The Failure Modes and the Effects on RPS Trip and ESF Actuation (SIAS, MSIS, and CIAS) Logic for HI containment pressure are equivalent to the failure modes and the effects on RPS Trip and ESF Actuation (MSIS Logic for HI SG LVL) provided in line Item 19, failure modes a) through y).				
			The failure modes and the effects on RPS Trip Logic for HI Pressurizer Pressure are equivalent to the failure modes and the effects on RPS Trip Logic for HI SG Level provided in line Item 19, failure modes a) through e) and n) through y). Failure modes f) through m), and z) through aa) are provided below.				
	f) Pre-Trip setpoint set fails off	Component failure	Pre-trip relay and CWP relay for HI PZR PRES. and de-energized spurious pre-trip alarm and CWP Logic Matrix half trip	Annunciating	None	No impact on RPS Trip Logic	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 22 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	g) Pre-Trip setpoint Set fails HI	Component fialure	Pre-trip and CWP Relays for Channel A will not be de-energized at the proper PZR pres. no pre-trip alarm or CWP from Channel A	Periodic test	3-channel redundancy (4th channel in bypass)	HI PZR Pres. Pre-trip logic converts to 1-out-of-2, and CWP on PZR Pres. coverts to 2-out-of 2	Same as 21 f)
	h) Pre-trip Voltage Comparator fails off	Open circuit, component failure	Same as 21 f)	Same as 21 f)	Same as 21 f)	Same as 21 f)	Same as 21 f)
	i) Pre-Trip Voltage Comparator fails on	Component failure	Same as 21 g)	Same as 21 g)	Same as 21 g)	Same as 21 g)	Same as 21 f)
	j) Pre-Trip Opto-isolator fails off	Component failure	Same as 21 f)	Same as 21 f)	Same as 21 f)	Same as 21 f)	Same as 21 f)
	k) Relay Driver (Pre-trip or CWP) fails off	Open circuit transistor failure	Affected relay coil de-energized resulting in either a spurious HI PZR Pres. pre-trip alarm or half trip of the CWP Logic Matrix	Annunciating for pre-trip relay, periodic test for CWP	3-channel redundancy (4th channel in bypass)	Spurious pre-trip alarm, or CWP on HI PZR Pres. con-verts to 1-out-of-2	Same as 21 f)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 23 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	l) Relay Driver (Pre-trip of CWP) fails on	Emitter-to-collector short	Affected relay coil will not deenergize for valid HI PZR Pres. Pre-trip signal	Periodic test	3-channel redundancy (4th channel in bypass)	CWP Logic goes to 2-out-of-2, or pre-trip alarm goes to 1-out-of-2	Same as 21 f)
	m) Relay Coil (Pre-trip of CWP) Fails open	Mechanical failure	Same as 21 k)	Same as 21 k)	Same as 21 k)	Same as 21 k)	Same as 21 k)
	• • •						
	z) CWP Relay Form C Contacts (one of two) fails open	Mechanical failure, corrosion	Part of CWP Logic Matrix is half tripped	Annunciating	3-channel redundancy (4th channel in bypass)	CWP Actuation logic remains 2-out-of-3 with a half trip in one logic matrix	Same as 21 f)
	AA) CWP Relay Form C Contacts (one of two) fails closed	Contact weld	One A Channel contact in CWP logic matrix remains closed on valid HI PZR Pres. pre-trip signal	Periodic test	3-channel reduncancy (4th channel in bypass)	CWP Actuation logic becomes 2-out-of-2	Same as 21 f)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 24 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
22) Hi Log PWR Level Bistable(75)			Failure modes for this bistable, and the effects on the RPS Trip Logic for HI Log PWR are equivalent to the failure modes and the effects on RPS Trip Logic for HI SG Level as provided in Line Item 19, failure modes a) through y).				
23) HI Local Power Density Bistable (96) (Channel A typical)	a) Trip input contact from CPC fails closed	Contacts welded	Bistable trip relays not de-energized for valid HI local PWR density signal	Periodic test	3-channel redundancy, (4th channel in bypass)	RPS Trip Logic for HI local power density changes to 2-out-of-2	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
	b) Trip input contacts from CPC fails open	Open circuit, mechanical failure corrosion	Bistable trip relays for Channel A will be de-energized	Annunciating	3-channel redundancy, (4th channel in bypass)	RPS Trip Logic for HI local power density becomes 1-out-of-2	Same as 23 a)
	c) Pre-trip Input contacts from CPC fails closed	Contacts welded	Pre-trip relay will not deenergize for valid HI local power density pre-trip signal	Periodic test	3-channel redundancy, (4th channel in bypass)	Pre-trip alarm logic for HI local power density becomes 1-out-of-2	Same as 23 a)
	d) Pre-trip input contacts form CPC fails open	Open circuit, Mechanical failure	HI local power density pre-trip relay is deenergized, spurious pre-trip alarm	Annunciating	None	Spurious pre-trip alarm, no impact on RPS trip logic	
	Failure modes e through r for this "bistable", and their effects on RPS Trip Logic for HI Local Power Density are equivalent to Failure Modes k) through q), and s) through y) of line Item 19.						

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 25 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
24) LO DNBR Bistable Relay Cards (92) (Channel A typical)		The Failure Modes for these bistable relay cards, and their effect on RPS Trip Logic are equivalent to the failure modes and effect on RPS Trip Logic Power Density as presented in Line Item 23.					
25) SG1 Low Level Bistable (104), SG2 Low Level Bistable (103) (Channel A typrical)	a) Trip setpoint power supply fails off	Open circuit, component fialure	LO SG LVL Pre-trip and trip setpoints go to zero LO SG LVL bistable relays will not deenergize for valid LO SG LVL	Periodic test	3-channel (4th channel in bypass)	AFAS-1 actuation logic goes to 2-out-of-2	To restore the sys tem logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
	b) Trip setpoint set fails low	Component failure	If LO SG LVL Trip setpoint goes to zero, pullup resistor changes effective setpoint to +10V, deenergizing bistable relays Otherwise B/S will trip at a lower level than desired.	Annunciating, Periodic Test.	3-channel redundancy (4th channel in bypass)	If setpoint goes to zero, AFAS-1 actuation for Channel A changes to "SG2.SG1 pres. and not (SG1.SG2 pres. and SG2 LO LVL)" Actuation logic remains 2-out-of-3, otherwise, none.	Same as 25 a)
	c) Trip setpoint set fails HI	Component failure	Bistable relays will be deenergized at a higher than desired SG LVL	Annunciating	3-channel redundancy (4th channel in bypass)	Same as above	Same as 25 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 26 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	d) Trip Voltage comparator fails off	Component failure, open circuit	SG LO LVL bistable relays will be deenergized. Spurious LO SG Level input to AFAS actuation logic	Annunciating	3-channel redundancy (4th channel in bypass)	Same as 25 b)	Same as 25 a)
	e) Trip Voltage comparator fails on	Component failure	Same as 25 a)	Same as 25 a)	Same as 25 a)	Same as 25 a)	Same as 25 a)
	f) Pre-trip setpoint set fails off	Open circuit, component fail	LO SG LVL Pre-trip setpoint goes to zero. Pullup resistor changes effective pre-trip set point, relays are deenergized. Spurious pre-trip alarm.	Annunciating	None	No impact on AFAS actuation logic	Same as 25 a)
	g) Pre-trip setpoint set fails HI	Component failure	SG Low Level Pre-trip bistable relays deenergized at higher than desired SG Level. Spurious pre-trip alarms	Annunciating	None	Same as above	Same as 25 a)
	h) Pre-trip voltage comparator fails off	Open circuit, component failure	Same as 25 f)	Same as 25 f)	Same as 25 f)	Same as 25 f)	Same as 25 f)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 27 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	i) Pre-trip voltage comparator fails on	Component failure	Channel A pre-trip relay will not be deenergized when SG Level reaches pre-trip level	Periodic test	3-channel redundancy (4th channel in bypass)	No impact on AFAS act. logic. Pre-trip logic for LO SG LVL changes to 1-out-of-2	Same as 25 a)
	j) Pre-trip Opto-Isolator fails off	Component failure, open circuit	Same as 25 f)	Same as 25 f)	Same as 25 f)	Same as 25 f)	Same as 25 f)
	k) Pre-trip relay driver fails off	Open circuit, transistor failure	Same as 25 f)	Same as 25 f)	Same as 25 f)	Same as 25 f)	Same as 25 f)
	l) Pre-trip relay driver fails on	Emittor- to collector short	Same as 25 i)	Same as 25 i)	Same as 25 i)	Same as 25 i)	Same as 25 i)
	m) Pre-trip relay coil fails open	Corrosion, mechanical damage	Same as 25 f)	Same as 25 f)	Same as 25 f)	Same as 25 f)	Same as 25 f)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 28 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	n) Pre-trip relay Form C contact in annunc. circuit fails open	Corrosion, mechanical damage	Channel A pre-trip on LO SG Level will not be annunciated	Periodic test	3-channel redundancy visual pre-trip indication (4th channel in bypass)	No impact on AFAS Act. Logic	Same as 25 a)
	o) Pre-trip relay Form C contact in annunc. circuit fails closed	Contact arcing	Spurious LO SG LVL pre-trip alarm	Annunciating	None	Same as above	Same as 25 a)
	p) Pre-trip relay Form C contact in indic. circuit fails open	Mechanical damage, corrosion	No visual indic. of Channel A pre-trip on LO SG LVL	Periodic test	3-channel redundancy audible pre trip alarm (4th channel in bypass)	Same as above	Same as 25 a)
	q) Pre-trip relay Form C. contacts in indic. circuit fail closed	Contact arc and weld	Spurious LO SG LVL pre-trip indic.	Visual indication	None	Same as above	Same as 25 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 29 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	r) Trip Opto-Isolator fails off	Open circuit, component failure	Same as 25 d)	Same as 25 d)	Same as 25 d)	Same as 25 d)	Same as 25 d)
	s) Trip Relay 1 Driver fails off	Open circuit, transistor failure	Trip relay 1 is deenergized, closing contacts in AFAS Logic circuit for Channel A	Annunciating	3-channel redundancy (4th channel in bypass)	AFAS Logic for Channel A remains the same with one set of contacts "actuated", Actua tion logic remains 2-out-of-3	Same as 25 a)
	t) Trip Relay 1 Driver fails on	Collector-to-emitter short	Trip relay 1 will not be de-energized on valid LO SG LVL signal	Periodic test	3-channel redundancy (4th channel in bypass)	Channel A AFAS logic becomes "LO SG LVL" logic for other channels unaffected. Actua tion Logic remains 2-out-of-3	Same as 25 a)
	u) Trip Relay 2 Driver fails off	Open circuit, transistor failure	Trip relay 2 is deenergized, opening contacts in AFAS logic circuit. AFAS Channel A actuation logic trip	Annunciating	3-channel redundancy (4th channel in bypass)	AFAS Act. Logic becomes 1-out-of-2	Same as 25 a)
	v) Trip Relay 2 Driver fails on	Emitter-to-collector short	Trip relay 2 will not be deenergized on valid LO SG LVL signal AFAS Act. Channel A will not trip	Periodic test	3-channel redundancy (4th channel in bypass)	AFAS actuation logic becomes 2 out-of-2	Same as 25 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 30 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	w) Trip Relay Form C Contacts in trouble annunc. circuit fails open	Mechanical damage, open circuit	Relay coil/relay driver failure will not be annunciated by trouble annunciator	Periodic test	None	No impact on AFAS actuation logic	Same as 25 a)
	x) Trip Relay Form C Contacts in trouble annunc. circuit fail closed	Contact arcing and weld	Spurious relay/relay driver trouble indication	Annunciating	None	Same as above	Same as above
26) SG1>SG2 Pres. bistable (48) SG2>SG1 Pres. bistable (102) (Channel A typical)	a) Set-point power supply fails off	Component failure, open circuit	Diff. voltage goes to zero, bistable relays 4 and 6 will deenergize. Trip alarm and SG diff. pres. input to Channel A AFAS logic	Annunciating	3-channel redundancy (4th channel in bypass)	AFAS logic for Channel A (AFAS 1 typical) becomes "LO SG 1 LVL and not AFAS 2)" AFAS actuation logic remains 2-out-of-3	To restore the system logic to 2-out of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 31 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	b) Set point PWR supply fails HI	Short circuit, component	Trip and pre-trip setpoint voltages go to +15V, pull-down resistors change effec-tive setpoints to 0V and bistable relays 4 and 6 are deenergized	Annunicating	3-channel redundancy (4th channel in bypass)	Same as 26 a)	Same as 26 a)
	c) Trip setpoint set fails low	Short circuit, component fail	Equiv. to 25 b)	Equiv. to 25 b)	Equiv. to 25 b)	Equiv. to 25 b)	Equiv. to 25 b)
	d) Trip setpoint set fails HI	Component failure	Trip setpoint voltage goes to +10V, pulldown resistor changes effective setpoint to 0V and bistable relays 4 and 6 are deenergized	Annunciating	3-channel redundancy (4th channel in bypass)	Same as 26 a)	Same as 26 a)
	e) Process "A: input buffer fails off	Open circuit, component failure	Ref. pres. signal goes to zero trip and pre-trip comparators deenergize bistable relays 4, 6, and 7.	Annunciating	3-channel redundancy (4th channel in bypass)	Same as 26 a)	Same as 26 a)
	f) Process "A" input buffer fails HI	Short circuit, component failure	Ref. pres. signal goes HI, bistable will not change state for valid HI diff. SG pres.	Periodic test	3-channel redundancy (4th channel in bypass)	Channel A AFAS logic becomes "LO SG LVL" AFAS actuation logic remains 2-out-of- 3	Same as 26 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 32 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	g) Process "B" input buffer fails off	Open circuit, component failure	Measured SG diff. pres. goes, negative. Bistable will not change state for valid HI diff. SG pres.	Periodic test	3-channel redundancy (4th channel in bypass)	Same as 26 f)	Same as 26 a)
	h) Process "B" input buffer fails HI	Short circuit, component failure	Measured SG pres. diff. goes Hi and bistable relays 4, 6 and 7 are deenergized	Annunciating	3-channel redundancy (4th channel in bypass)	Same as 26 a)	Same as 26 a)
	Failure modes i) through t) (for pre-trip portion of bistable) are equivalent to failure modes f) through q) of Line Item 25						
	u) Trip voltage comparator fails off	Component failure, open circuit	Same as 26 a)	Same as 26 a)	Same as 26 a)	Same as 26 a)	Same as 26 a)
	v) Trip voltage comparator fails on	Short circuit, component failure	Same as 26 f)	Same as 26 f)	Same as 26 f)	Same as 26 f)	Same as 26 f)
	w) Trip Opto-Isolator fails off	Open circuit, component failure	Same as 26 a)	Same as 26 a)	Same as 26 a)	Same as 26 a)	Same as 26 a)
	x) Trip Relay 4 Driver fails off	Transistor failure	Trip relay 4 deenergized spurious SG diff. pres. trip indication	Annunciating	None	No impact on AFAS logic or AFAS actuation logic	Same as 26 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 33 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	y) Trip Relay 4, Driver fails on	Emitter to collector short	Trip relay 4 will not de-energize for valid HI SG diff. pres. signal. Channel A trip not annunciated	Periodic test	3-channel redundancy (4th channel in bypass)	Same as 26 x)	Same as 26 a)
	z) Trip Relay 6, Driver fails off	Transistor failure	Trip relay 6 is deenergized False "SG diff. pres." input to Channel A AFAS logic	Trouble annunicator	3-channel redundancy (4th channel in bypass)	Same as 26 a)	Same as 26 a)
	AA) Trip Relay 6, Driver fails on	Emitter to collector short	Trip relay 6 will not de-energize for valid "SG Diff. Pres." signal	Periodic test	3-channel redundancy (4th channel in bypass)	Same as 26 f)	Same as 26 f)
	AB) Trip Relay 6, Coil fails open	Mechanical failure	Same as 26 z)	Same as 26 z)	Same as 26 z)	Same as 26 z)	Same as 26 z)
	AC) AFAS Logic Relay (AK40, or AK41), Coil fails open	Mechanical failure	Relay will not energize for valid SG LVL, SG diff. pres. and opposite AFAS Act. False AFAS sig. to opposite AFAS logic	Periodic test	3-channel redundancy (4th channel in bypass)	AFAS (AFAS2) Channel A logic becomes "LO SG LVL", and AFAS2 (AFAS1) logic becomes "LO SG LVL and not SG Diff. Pres" AFAS actuation remains 2-out of-3	Same as 26 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 34 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	AD) AFAS Logic Relay (AK40 or AK41) Contacts in same AFAS Train Logic fails open	Open circuit, mechanical failure	Contact will not be closed for valid SG LVL, SG diff. and opposite AFAS Act. Inputs	Periodic test	3-channel redundancy (4th channel in bypass) affected	Channel A logic for affect AFAS train becomes "LO SG LVL" Channel A logic for other AFAS train and AFAS act. logic not	Same as 26 a)
	AE) AFAS Logic Relay (AK40 or AK41) Contacts in same AFAS Train Logic fail closed	Contact arcing and weld	Contact will be closed regardless of input for affected AFAS train. Unable to deenergize Channel A AFAS bistable trip relays for affected AFAS train	Periodic test	3-channel redundancy (4th channel in bypass)	AFAS actuation logic for affected AFAS train becomes 2-out-of-2	Same as 26 a)
	AF) Bistable Trip Relay Driver (TR1, TR2, or TR3) fails off	Transistor failure, open circuit	One bistable trip relay de-energized, including half trip of one logic matrix (AB, AC, or AD) for one AFAS train	Annunciating	3-channel redundancy (4th channel in bypass)	AFAS actuation logic remains 2 out-of-3 with one matrix half-tripped for one AFAS train	Same as 26 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 35 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	AG) Bi-stable Trip Relay Driver (TR1, TR2 TR3) fails on	Emitter to collector short	One Channel A bistable trip for one AFAS train will not deenergize for valid input. One AFAS Logic Matrix (AB, AC, or AD) for one AFAS train will not trip	Periodic test	3-channel redundancy (4th channel in bypass)	Actuation logic for one AFAS train becomes 2-out-of-2	Same as 26 a)
	AH) Bi-stable Trip Relay Coil (TR1 TR2 or TR3) fails open	.Mechanical failure	Same as 26 AF)	Same as 26 AF)	Same as 26 AF)	Same as 26 AF)	Same as 26 AF)
	AI) Bi-stable Trip Relay Contact in Logic Matrix fails open	Open circuit, Mechanical failure	Same as 26 AF)	Same as 26 AF)	Same as 26 AF)	Same as 26 AF)	Same as 26 AF)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 36 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	AJ) Bi-stable Trip Relay Contacts in Logic Matrix fails closed	Contact arcing and weld	Same as 26 AG)	Same as 26 AG)	Same as 26 AG)	Same as 26 AG)	Same as 26 AG)
	AK) Bi-stable Trip Relay Contacts in Trouble Annunc. Circuit fail open	Mechanical damage open circuit	Trip Relay/Relay Driver failure (off) not annunciated by trouble annunciator.	Periodic test	Logic matrix indicator lights	No impact on AFAS actuation logic	Same as 26 a)
	AL) Bi-stable Trip Relay Contact in Trouble Annunc. Circuit fail closed	Contact arcing and weld	Spurious TRIP Relay/Relay Driver Trouble Annunciator	Annunciating	None	Same as above	Same as 26 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 37 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
27) SG1 LO Pres. Bi-stable (45) SG LO Pres. Bistable (30) (Channel A typical)	a) Bi-stable setpoint power supply fails off	Component failure open circuit	Step adjust, min. adjust and max. adjust for trip and pre-trip setpoints go to zero Trip and pre-trip setpoints equiv. to last process input. Bistable trip will occur on any momentary process input decrease.	Annunciating	3-channel redundancy (4th channel in bypass)	RPS trip and MSIS logic becomes 1-out-of-2	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
	b) Bi-stable setpoint Power Supply fails HI	Component failure, short circuit	Step adjust, min. adjust and max. adjust for trip and pre-trip setpoints go high. Setpoints go high, and comparators initiate bistable trip.	Annunciating	3-channel redundancy (4th channel in bypass)	Same as 27 a)	Same as 27 a)
	c) 15V Power Supply fails off	Component failure open circuit	Loss of bistable setpoint power supply. See 27 a)	Annunciating	3-channel redundancy (4th channel in bypass)	Same as 27 a)	Same as 27 a)
	d) 15V Power Supply fails HI	Component failure	HI volt input to clock circuit digital representation circuit limiter circuit, and setpoint power supply. Probable overstress and loss of setpoint power supply. See 27 a)	Annunciating	3-channel redundancy (4th channel in bypass)	Same as 27 a)	Same as 27 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 38 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	e) Set-point step adjust fails open	Mechanical damage component failure	Setpoint step goes to zero, and setpoint equals last process input. Decrease in process input will cause bistable trip.	Annunciating	3-channel redundancy (4th channel in bypass)	Same as 27 a)	Same as 27 a)
	f) Set-point step adjust fails high	Short circuit	Setpoint step goes to +10V and setpoint goes LO. Pullup circuit in comparator initiates bistable trip	Annunciating	3-channel redundancy (4th channel in bypass)	Same as 27 a)	Same as 27 a)
	g) Set-point max. adjust fails open	Component failure open circuit	Max. setpoint goes ot 0Vs and stays there. Pullup circuit in comparator initiates bistable trip	Annunciating	3-channel redundancy (4th channel in bypass)	Same as 27 a)	Same as 27 a)
	h) Set-point max. adjust shorted	Component failure	Max. setpoint goes HI, Set-point will continue to track process input above desired max. Possible bistable trip in SG press. operating range.	Periodic test, annunciating for trip	3-channel redundancy (4th channel in bypass)	No effect unless channel trip occurs, then trip logic becomes 1-out-of-2	Same as 27 a)
	i) Set-point min. adjust fails open	Component failure open circuit	Setpoint min. goes to zero, setpoint can drop below desired minimum during power decreases. Possible failure to initiate channel trip on loss of SG pres. at LO PWR LVLs	Periodic test	3-channel redundancy (4th channel in bypass)	RPS trip and MSIS logic for LO SG Pres. becomes 2-out-of 2 at LO PWR LVLs	Same as 27 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 39 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	j) Set-point min. adjust shorted.	Comp. failure.	Setpoint minimum goes hi. Unable to reset setpoint during power decreases. Possible channel trip during power decrease.	Periodic test, annunciating during power decreases.	3-channel redundancy. (4th channel in bypass)	RPS trip and MSIS logic for LO SG press. becomes 1-out-of-2 during power decreases.	Same as 27 a)
	k) Pre-trip set-point adjust fails open	Comp. failure, open circuit.	Pre-trip bias voltage goes to zero. Pre-trip and trip set-points become identical. Loss of pre-trip indication for channel.	Periodic test.	3-channel redundancy. (4th channel in bypass)	RPS trip and MSIS logic unaffected. Pre-trip logic becomes 1-out-of-2.	Same as 27 a)
	l) Pre-trip set-point adjust shorted.	Comp. failure.	Pre-trip bias voltage goes hi, driving pre-trip setpoint hi. Spurious pre-trip alarm.	Annunciating.	None.	No impact on RPS trip and MSIS logic.	Same as 27 a)
	m) Reset button (1 of 3) fails open.	Mech. damage, corrosion.	Unable to reset trip and pre-trip setpoints from 1 location during power decrease. Probable ch. trip during power decrease.	Periodic test, annunc. ch. trip during power decrease.	3-channel redundancy, reset buttons at other locations. (4th channel in bypass)	RPS trip and MSIS logic for LO SG press. becomes 1-out-of-2 during power decrease.	Same as 27 a)
	n) Reset button (1 of 3) shorted.	Contact weld.	Contacts remain closed after reset, and reset logic becomes disabled for all locations. Ch. trip on power decrease.	Periodic test, ch. trip alarm during power decrease.	Same as above.	Same as above.	Same as 27 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 40 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	o) Clock circuit fails HI	Comp. failure.	Faster generation of digital representation of process input. No other impact.	Periodic test.	None required.	No impact on RPS trip or MSIS logic.	Same as 27 a)
	p) Clock circuit fails Low	Comp. failure.	Slower generation of digital representation of process input. Setpoint lags input during power increase. No adverse effect.	Periodic test.	None required.	No impact on RPS trip or MSIS logic.	Same as 27 a)
	P1) 15VDC variable setpoint power supply fails low or off	Component failure in power supply	15 VCD power to clock and other circuits on variable setpoint card lost. Setpoint output from card goes to 0 VDC. Trip set-point goes to zero. Bistable will not trip on valid low pressure condition.	Periodic test	3-channel redun-dancy (4th channel in bypass)	RPS trip logic for LO-SG-Press. becomes 2-out-of-2 coincident	Same as 27 a)
	P2) 15VDC variable setpoint power supply output goes high	Component tolerance buildup, component failure.	Voltage to clock and other circuits on variable setpoint exceeds 15V. Clock frequency may increase and setpoint output voltage may increase. If setpoint increases, bistable will trip at a higher pressure.	Periodic test, annunciating if bistable trips.	3-channel redun-dancy (4th channel in bypass)	If bistable trips, RPS trip logic for LO-SG-Press will becomes 1-out-of-2 coincident	Same as 27 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 41 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
27) SG1 Lo Press. Bi-stable (45), SG2 Lo Pres. Bistable (30) (Ch. A Typ.) (Cont.)	q) Digital represent. circuit fails off.	Comp. failure.	Bias voltage to setpoint generators goes to zero. Set-points track process input up and down. Unable to trip ch.	Periodic test.	3-channel redundancy. (4th channel in bypass)	RPS trip and MSIS logic goes to 2-out-of-2.	Same as 27 a)
	r) Digital represent. Circuit fails hi.	Comp. failure.	Bias voltage to setpoint generators goes hi, driving setpoints up. Possible ch. trip if setpoints exceed process input.	Periodic test, annunciating for ch. trip.	3-channel redundancy. (4th channel in bypass)	RPS trip and MSIS logic for LO SG press. becomes 1-out-of-2.	Same as 27 a)
	s) Set-point limiter fails off.	Open circuit, comp. failure.	Trip and/or pre-trip setpoint goes to zero. Pullup circuit in comparator initiates ch. trip.	Annunciating.	3-channel redundancy. (4th channel in bypass)	Same as 27 a)	Same as 27 a)
	t) Set-point limiter fails low	Comp. failure.	Trip and/or pre-trip setpoints are limited at too low a value Bistable will not trip at proper SG press.	Periodic test.	3-channel redundancy. (4th channel in bypass)	RPS trip and MSIS logic changes to 2-out-of-2.	Same as 27 a)
	u) Set-point limiter fails HI.	Comp. failure, short circuit.	Trip and/or pre-trip setpoint limit values go hi. Trip set-point can follow process input into normal operating range. Possible spurious ch. trip under normal SG pressure fluctuations.	Periodic test, annunc. for ch. trip.	3-channel redundancy. (4th channel in bypass)	Same as 27 a)	Same as 27 a)
	Failure modes v) through an) and their effects on RPS trip and MSIS logic for LO SG Press. are equivalent to Line Item 19s Failure modes d), e), and h) through y) and their effects on RPS trip and MSIS logic for HI SG Level.						

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 42 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
28) LO PZR Pres. Bi-stable (62) (Ch. A Typ.)	The Failure Modes for this bistable and their effects on RPS trip logic for LO PZR Press. are equivalent to the failure modes and their effects on RPS trip logic for Lo SG Press. as presented in Line Item 27.						
29) Variable Overpower Bistable (72) (Ch. A. Typ.)	a) Bi-stable setpoint power supply fails off	Comp. failure, open circuit.	Step adjust, max. adjust, and min. adjust voltages for trip and pre-trip setpoints go to zero. Trip and pre-trip set-points go to zero and bi-stable trips.	Annunciating.	3-channel redundancy. (4th channel in bypass)	RPS trip logic for overpwr. Goes to 1-out-of-2.	To restore the sys-tem logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
	b) Bi-stable setpoint power supply fails HI	Comp. failure, short circuit.	Step adjust, max. adjust, and min. adjust voltages for trip and pre-trip setpoints go high. Trip and pre-trip set-point values increase, as do the limit values. Ch. bistable not respond properly to increasing power level or to HI power level.	Periodic trip.	3-channel redundancy. (4th channel in bypass)	RPS trip logic for variable power goes to 2-out-of-2.	Same as 29 a)
	c) 15 V power supply fails off.	Open circuit, comp. failure.	Loss of bistable setpoint power supply. See 29 a).	Same as 29 a)	Same as 29 a)	Same as 29 a)	Same as 29 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 43 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
29) (Cont.)	d) 15 V power supply fails HI	Comp. failure.	HI voltage input to clock circuit, digital representa-tion circuit, limiter circuit and bistable setpoint power supply. Possible overstress of clock circuit or setpoint power supply. Probable Ch. trip.	Annunciating	3-channel reduncancy. (4th channel in bypass)	RPS trip logic for overpower goes to 1-out-of-2.	Same as 29 a)
	e) Set-point step adjust fails open	Mech. damage, comp. failure.	Offset between process input and trip setpoint goes to zero and bistable trips.	Annunciating	3-channel redundancy. (4th channel in bypass)	Same as 29 a)	Same as 29 a)
	f) Set-point step adjust fails HI	Short circuit, comp. failure.	Offset between process input and trip setpoint goes hi. Time to reach setpoint during power increase transient slightly longer than it should be. No effect during steady state operation as setpoint is limited by max. adjust.	Periodic test.	3-channel redundancy. (4th channel in bypass)	Same as 29 b)	Same as 29 a)
	g) Set-point max. adjust fails open	Mechanical damage component failure	Max. setpoint value for power goes to zero. Bistable trips	Annunciating	3-channel redundancy (4th channel in bypass)	Same as 29 a)	Same as 29 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 44 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
29) (Cont.)	h) Set-point max adjust fails HI	Component failure	Max. setpoint value for over-power goes HI, setpoint will continue to track power into safety limit range. Bistable may not trip for valid over-power condit.	Periodic test	3-channel reduncancy (4th channel in bypass)	Same as 29 b)	Same as 20 a)
	i) Set-point min. adjust fails open	Mechanical damage component failure	Overpower setpoint minimum goes to zero, setpoint will continue to track linear power at LO Power Levels. Possible spurious channel trips at LO power	Periodic test Annunc. for channel trip at Low PWR	3-channel redundancy (4th channel in bypass)	No impact on RPS trip logic except at LO PWR LVLs where it becomes 1-out-of-2	Same as 29 a)
	j) Set-point min. adjust fails HI	Component failure short circuit	Overpower setpoint minimum goes HI therby driving set-point HI bistable may not trip for valid power excursion	Periodic test	3-channel redundancy (4th channel in bypass)	Same as 29 b)	Same as 29 a)
	k) Pre-trip Setpoint adjust fails open	Mechanical damage component failure	Pre-trip setpoint bias voltage goes to zero, pre-trip and trip setpoint becomes identical loss of pre-trip indic. for channel	Periodic test	3-channel redundancy (4th channel in bypass)	RPS trip logic not affected. Pre-trip logic becomes 1-out-of-2	Same as 29 a)
	l) Pre-trip Setpoint adjust shorted	Component failure	Pre-trip bias volt. goes low driving pre-trip setpoing low. Spurious pre-trip alarms	Annunciating	None	No impact on RPS trip logic	Same as 29 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 45 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
29) (Cont.)	m) Clcok Circuit Freq. goes HI	Component failure	Setpoint generation time is decreased, and setpoint tracks process input quicker. Bistable will not trip on power excursion.	Periodic test	3-channel reduncancy (4th channel in bypass)	Same as 29 b)	Same as 20 a)
	n) Clock Circuit freq. goes Low	Component failure	Setpoint generation time increases and setpoint tracks process input slower. Possible spurious channel trips during PWR increase	Annunc. For channel trip, otherwise periodic test	3-channel redundancy (4th channel in bypass)	Same as 29 a)	Same as 29 a)
	o) Digi-tal repre-sentation Circuit fails off	Component failure	Loss of process input ref. for setpoint generation. Setpoint drops to offset (step) value. Spurious channel trip	Annunciating	3-channel redundancy (4th channel in bypass)	Same as 29 a)	Same as 29 a)
	p) Digi-tal repre. Circuit fails HI	Component failure	Erroneous HI valves for process input used for setpoint generation	Same as 29 f)	Same as 29 f)	Same as 29 f)	Same as 29 f)
	q) Set-point limiter fails low	Component failure open circuit	Setpoint limited below max. setpoint, spurious channel trip during power increase	Annunciating	3-channel redundancy (4th channel in bypass)	Same as 29 a)	Same as 29 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 46 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	r) Set-point Limiter fails HI	Component failure	Same as 29 h)	Same as 29 h)	Same as 29 h)	Same as 29 h)	Same as 29 h)
	Failure Modes s) through AK) and their effect on RPS Trip Logic for variable overpower are equivalent to Line Item 19, Failure Modes d), e), and h) through y) and their effects on RPS Trip Logic on HI SG LVL.						
30) SG1 LO Flow Bistable (101) SG2 LO Flow Bistable (100)	a) Bi-stable setpoint PWR supply fails off	Component failure open circuit	Step adjust, max. adjust and min. adjust voltages for trip and pre-trip go to zero. Digital representation goes to zero. Trip setpoint goes to zero. Bistable not respond to SG flow decrease	Annunc. for P/S fail	3-channel redundancy (4th channel in bypass)	RPS Trip Logic for LO flow becomes 2-out-of-2	To restore the sys-tem logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
	b) Bi-stable Setpoint PWR supply fails HI	Component failure short circuit	Step adjust, max. adjust, and min. adjust voltages go more negative. Trip and pre-trip setpoints decrease bistable not trip on decreasing SG flow	Periodic test	3-channel redundancy (4th channel in bypass)	RPS Trip Logic for LO flow becomes 2-out-of-2	Same as 30 a)
	c) 15V Power fails off	Open circuit, Component circuit	Loss of bistable setpoint power supply.	See 30 a)	See 30 a)	See 30 a)	See 30 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 47 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
30) (Cont.)	d) 15V Power Supply fails high	Component failure	HI voltage input to variable setpoint card and bistable setpoint power supply. Probable overstress of setpoint power supply or clock circuit. See 30 a)	Annunciating	3-channel reduncancy (4th channel in bypass)	RPS trip logic for LO flow becomes 2-out-of-2	Same as 30 a)
	e) Set-point step adjust fails open	Mechanical failure component failure	Setpoint offset voltage goes to zero and setpoint rises to the process input value, bistable trips	Annunciating	3-channel redundancy (4th channel in bypass)	RPS Trip Logic for LO flow becomes 1-out-of-2	Same as 30 a)
	e1) Set-point step adjust fails low	Component failure, component out-of-tolerance.	Setpoint offset voltage goes low, offset between process input and setpoint decreases. No impact during normal operation, but bistable will trip earlier than expected on decreasing flow.	Periodic Test	3-channel redun- (4th channel in in bypass)	RPS trip logic for SG-LO-Flow unaffected, but one bistable will trip earlier than others.	See 30 a)
	f) Set-point adjust fails high	Component failure short circuit	Setpoint offset voltage goes more negative. Difference between process input and setpoint increases. See 30 b)	See 30 b)	See 30 b)	See 30 b)	See 30 b)
	g) Set-point max. adjust fails open	Mechanical failure component	Max. setpoint offset voltage goes to zero, setpoint held at 0v. See 30 a)	Periodic test	3-channel redundancy (4th channel in bypass)	Same as 30 a)	Same as 30 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 48 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
30) (Cont.)	h) Set-point max. adjust fails HI	Component failure	Max. adjust bias voltage goes more negative setpoint max. limit increases. Setpoint can track process input into operating range. Possible spur. channel trip under normal flow fluctuations	Periodic tests annunc. for channel trip	3-channel reduncancy (4th channel in bypass)	Same as 30 e)	Same as 30 a)
	i) Set-point min. adjust fails open	Mechanical damage component failure	Min. setpoint ref. voltage goes to zero. Min. setpoint limit goes to zero bistable not respond to loss of flow at LO power	Periodic test	3-channel redundancy (4th channel in bypass)	Same as 30 a)	Same as 30 a)
	j) Set-point min. adjust fails high	Component failure	Min. setpoint ref. voltage goes more negative and min. setpoint limit increases. Possible spurious channel trips at LO power and LO flow	Periodic test, annunciating for channel trip	3-channel redundancy (4th channel in bypass)	Same as 30 e)	Same as 30 a)
	k) Pre-trip setpoint adjust fails open	Mechanical damage open circuit	Pre-trip setpoint bias voltage goes to zero, and pre-trip and trip setpoints become identical. Loss of channel pre-trip capability	Periodic test	3-channel redundancy (4th channel in bypass	No impact on RPS Trip Logic. Pre-trip logic becomes 1-out-of- 2	Same as 30 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 49 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
30) (Cont.)	l) Pre-trip setpoint adjust fails high	Component failure	Pre-trip setpoint bias voltage goes high and pre-trip setpoint increases possible spurious pre-trip alarm	Annunciating	None	No impact on RPS Trip Logic	Same as 30 a)
	m) Clock circuit freq. goes high	Component failure	Setpoint generation time decreases and setpoint can track process input quicker Bistable may not trip on flow decrease	Periodic test	3-channel redundancy (4th channel in bypass)	Same as 30 a)	Same as 30 a)
	n) Clock circuit freq. goes low	Component failure	Setpoint generation time increases and setpoint does not track process input as fast as it should. Possible channel trip during power/flow decrease	Periodic test, annunc. for channel trip	3-channel redundancy (4th channel in bypass)	Same as 30 e)	Same as 30 a)
	o) Digi-tal repre-sentation circuit fails off	Component failure	Loss of process input reference for setpoint generation. Setpoint drops to step value. Bistable not respond to flow decrease	Periodic test	3-channel redundancy (4th channel in bypass	Same as 30 a)	Same as 30 a)
	p) Digi-tal repre-sentation circuit fails high	Component failure	Erroneous, high ref. values used for setpoint generation Possible spurious channel trip	Annunciating for channel trip	3-channel reduncancy (4th channel in bypass)	Same as 30 e)	Same as 30 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 50 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
30) (Cont.)	q) Set-point limiter fails low	Component failure	Setpoint limited to artifi-cially LO value. Bistable not respond properly to decrease in RCS flow	Periodic test	3-channel redundancy (4th channel in bypass)	Same as 30 a)	Same as 30 a)
	r) Set-point limiter fails hi	Component failure	Same as 30 h)	Same as 30 h)	Same as 30 h)	Same as 30 h)	Same as 30 h)
	Failure Modes s) through AK) and their effect on RPS Trip Logic for Low Flow are equivalent to Line Item 19, Failure Modes d), e), and h) through y) and their effect on RPS Trip Logic for HI SG LVL.						
31) Control Element Assembly Calculator (88)	a) No data output	Loss of AC power. Input/ output failure Data link failure. Arithmetic, logic or memory failure	Loss of CEA position display	Annunciating alarm on CPC operator's module.	Two-channel redundancy	None	CPC uses data from the other CEAC and annun-ciates failure
	b) Errone-ous data output	CEA position sensor failure input/output failure. Data link failure Arithmetic, logic or memory failure	Erroneous calculated values. Possible DNBR or LPD trip	Annunciating alarm on CPC operator's module. Comparison of CEA position dis-plays, comparison of like parameters on operator's modules	CPC uses worst case data from the two CEAC's	Possible DNBR or LPD trip	CPC compares data from the two CEACs and annunciates

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 51 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
32) Core Protection Calculator (89)	a) Tripped	Loss of AC power input/ output failure arithmetic, logic or memory failure sensor failure	Loss of control board displays Erroneous calculated results	Annunciating PPS alarm on channel trip. 3-channel comparisons annunciating watchdog timer	3-channel redundancy. (4th channel in bypass)	Reactor trip logic for DNBR, LPD and CWP is converted to 1-out-of-2 coincidence	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
	b) Stays in un-tripped state	Input/output failure Arithmetic, logic or memory failure sensor failure	Erroneous calculated results	3-channel comparisons Annunciating watchdog timer	3-channel redundancy (4th channel in bypass)	Reactor trip logic for DNBR, LPD and CWP is on coincidence of 2-out-of-2 remaining channels	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 52 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
33) LO PZR Pressure Operating Bypass (33, 36, 60, 34) Channel A typical	a) Bi-stable PWR supply fails off	Component failure open circuit	Trip setpoint goes to zero. Operator unable to bypass LO PZR Pres. Bistable at LO pres. or operating bypass automatically removed, Possible channel trip on LO PZR Pres.	Annunc., Periodic test, operator when initiate operating bypass	3-channel redundancy (4th channel in bypass)	RPS Trip Logic for LO PZR Pres. goes to 1-out-of-2 at LO PWR/ Pres. operator	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel
	b) Bi-stable setpoint PWR supply fails HI	Component failure	Trip setpoint voltage goes HI, The pre-set point at which the LO PZR Pres. operating bypass is automatically removed increases LO PZR Pres. bistable will remain bypassed.	Periodic test. bypass indicator lit at power	3-channel redundancy (4th channel in bypass)	RPS Trip Logic for LO PZR Pres. becomes 2-out-of-2	Same as 33 a)
	c) 15V PWR supply fails off	Component failure open circuit	Loss of bistable setpoint PWR supply. See 33 a)	See 33 a)	See 33 a)	See 33 a)	See 33 a)
	d) 15V PWR supply fails HI	Component failure short circuit	Overstress of bistable setpoint PWR supply. Setpoint power supply output may go hi (see 33 b) for effects) or setpoint power supply may burn out and its output go to 0 VDC (see 33 a) for effects)	See 33 a) and 33 b)	See 33 a) and 33 b)	See 33 a) and 33 b)	See 33 a) and 33 b)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 53 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
33) (Cont.)	e) Set-point set fails open	Component failure	See 33 a)	See 33 a)	See 33 a)	See 33 a)	See 33 a)
	f) Set-point set fails HI	Component failure	See 33 b)	See 33 b)	See 33 b)	See 33 b)	See 33 b)
	g) Trip voltage comparator fails off	Component failure,	Bistable Relay, AK21, is de-energized and PZR Pres. operating bypass is removed. Probable channel trip on LO PZR Pres.	Annunc. for channel trip, periodic test	3-channel redundancy (4th channel in bypass)	Same as 33 a)	Same as 33 a)
	h) Trip voltage comparator fails on	Short circuit component failure	Bistable Relay AK21 will not be de-energized when PZR Pres. reaches setpoint. Operating bypass will remain engaged. LO PZR Pres. bistable remains bypassed	Periodic test, by-pass indicator on when it should not be	3-channel redundancy (4th channel in bypass)	Same as 33 b)	Same as 33 b)
	i) Opto-isolator fails off	Open circuit component failure	Same as 33 g)	Same as 33 g)	Same as 33 g)	Same as 33 g)	Same as 33 g)
	j) Relay Driver, (Relay AK21) fails off	Open circuit, transistor failure	Same as 33 g)	Same as 33 g)	Same as 33 g)	Same as 33 g)	Same as 33 g)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 54 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
33) (Cont.)	k) Relay Driver (Relay AK21) fails on	Emitter-to-collector short	Same as 33 h)	Same as 33 h)	Same as 33 h)	Same as 33 h)	Same as 33 h)
	l) AK21 Coil open	Sustained Overvoltage	The low pressurizer pressure trip cannot be bypassed in Channel A	Periodic PPS testing or when attempting to initiate bypass	None required. Failure will not cause trip and will not prevent trip	During a condition of low pressurizer pressure, the bistable will be tripped in that channel regardless of the position of the bypass switch	
	m) AK21 Coil short	Deterioration of Insulation	Attempting to bypass low pressurizer pressure under conditions of low pressure will place a severe load on the relay driver. Under this abnormal load the relay driver may fail. If the driver fails short the results will be the same as those listed for item 33 k)	Same as 33 k)	Same as 33 k)	Same as 33 k)	
			If the driver fails open the results will be the same as those listed for an open relay coil.	Same as 33 l)	Same as 33 l)	Same as 33 l)	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 55 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
33) (Cont.)	n) AK21 Contact in Relay Latching Circuit open	Deterioration of contact	Low Pressurizer Pressure cannot be bypassed in Channel A	Periodic PPS testing or when attempting to initiate a bypass on this function	Same as 33 l)	During a condition of low pressurizer pressure the bistable will be tripped	
	o) AK21 Contact in Relay Latching Circuit short	Welded Contact	Bypass will not lock out automatically	Periodic PPS testing	3-channel redundancy (4th channel in bypass	Unless the bypass is removed manually, bypass will be in effect whenever there is low pressurizer pressure	
	p) AK21 Contacts in permissive indic. circuit fail open	Mechanical damage open circuit	Permissive indicator will not be lit when PZR Pres. goes below operator bypass setpoint LO PZR Pres.	Periodic test visual at LO PZR Pres.	3-channel redundancy (4th channel in bypass	Same as 33 a)	Same as 33 a)
	q) AK21 Contacts in permissive indic. circuit fail closed	Corrosion contact weld	Permissive indicator will remain on even when permissive not available. No impact on bypass capability	Visual indication, test	None required	No impact on RPS Trip Logic for LO PZR Pres.	Same as 33 a)
	r) Permissive indicator fails off	Light burn out	Same as 33 p)	Same as 33 p)	Same as 33 p)	Same as 33 p)	Same as 33 p)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 56 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	s) AK22 Driver fails off	Transistor failure	AK22 cannot be energized even when permissive available. Unable to place operating bypass on LO PZR Pres. bistable (Ch. A) possible channel trip	Periodic test, bypass indicator will not come on. Annunc. for channel trip	3-channel redundancy for LO PZR Pres. bistable (4th channel in bypass)	Same as 33 a)	Same as 33 a)
	t) AK22 Driver fails on	Emitter-to-collector short	AK22 will be energized whenever AK21 is energized. Lo PZR Pres. Bistable will be automatically bypassed below operating bypass setpoint	Periodic test. Oper. bypass light comes on when no bypass placed by operator	3-channel redundancy (4th channel in bypass	Same as 33 b)	Same as 33 a)
	u) AK22 Coil open	Sustained overvoltage	Low pressurizer pressure trip bypass for the affected channel will not be actuated when demanded.	Periodic PPS testing status light not lit	3-channel redundancy (4th channel in bypass	Same as 33 a)	Same as 33 a)
	v) AK22 Coil short	Deterioration or Insulation	Attempting to bypass log pressurizer pressure under conditions of low pressure will place a severe load on the relay driver. With this abnormal load the relay driver may fail. If the driver fails short the results will be the same as those listed for an open relay coil.	Same as 33 u)	Same as 33 u)	Same as 33 u)	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 57 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
33) (Cont.)	w) Contact in Latch Circuit shorts	Mechanical failure	Bypass transistor will remain latched "on" after bypass switched is turned to "normal" Low PZR Press. trip will be bypassed.	Unable to unlatch transistor manually status light lit	Redundant channel	Bypass	Same as 33 a)
	x) Contact in Latch Circuit opens	Mechanical failure	Unable to latch bypass transistor "on"; Low PZR Press. trip will not bypass	Status light not lit	Redundant channel	None	Same as 33 a)
	y) Contact in Annun-ciated Circuit short	Mechanical failure	Annunciator and status light actuated	Alarm	None required	Nuisance Alarms and indications	Same as 33 a)
	z) Contact in Annun-ciated Circuit open		No annunciation	No status indication		Redundant channel	None
	aa) Low PZR Pres-sure Trip Bypass Switch Contact Bypass Circuit short	Mechanical failure	Low pressurizer pressure trip automatically bypassed in the affected channel when PZR Pres. aux. B/S permits bypass condition	Periodic PPS test-ing. Bypass condi-tion before manual action	3-channel redundancy (4th channel in bypass	During a condition of low pressurizer pressure the bi-stable will be bypassed	If a bypass is required the other 2 channels may be bypassed as they are un-affected by the fault

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 58 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
33) (Cont.)	ab) Low PZR Pressure Trip Bypass Switch Contact Bypass Circuit Open	Mechanical failure	Bypass transistor will not switch "ON". Low PZR Pres. trip will not be bypassed when desired	Unable to bypass. Status light not lit	One bistable alone cannot cause trip. Other two channels can be bypassed (4th channel already in bypass)	None	The low pressurizer pressure bypass circuits in the other 2 channels are unaffected and will respond properly.
	ac) Contact Normal Circuit shorts	Mechanical failure	Bypass transistor remains "OFF" and bypass condition will not latch on	Status light not lit	Same as 33 ab)	None	Operator would have to hold bypass switch in bypass position to maintain bypass in this channel
	ad) Contact Normal Circuit open	Mechanical failure	Bypass transistor will not switch "OFF" manually	Unable to manually remove bypass status light status	Same as 33 ab)	None	Function of circuit is not impaired, nuisance

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 59 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
34) Safety Channel Nuclear Instument (83) (Ch. A Typical)	a) Trouble annunc. bistable fails off.	Failure causes equiv. to trip ch. bistable fail modes.	Trouble annunc. relays de-energized. Spurious N.I. trouble indication and spurious LPS and DNBR ch. trips.	Annunciating.	3-channel redundancy for LPD and DNBR. None for trouble annunc. (4th channel in bypass)	RPS trip logic for LPD and DNBR goes to 1-out-of-2.	To restore the system logic ot 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
	b) Trouble annunc. bistable fails on.	Failure causes equiv. to trip ch. bistable fail. modes.	Trouble annunc. relays not de-energize during NI test or when there is trouble in the NI Drawer. Loss of trouble annunc. LPD and DNBR bistables not tripped. LPD and DNBR bistables may not trip during NI test due to erroneous data.	Periodic test, lack of annunc. during NI test.	3-channel redundancy. (4th channel in bypass)	RPS trip logic for LPD and DNBR may go to 2-out-of-2.	Same as 34 a)
	c) Trouble bistable relay contacts in annunc. circuit fail closed	Contact arc and weld.	NI test or trouble in NI not annunciated.	Periodic test, lack of annunc. during NI test.	None.	RPS trip logic not affected.	Same as 34 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 60 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
34) (Cont.)	d) Trouble bistable relay contacts in annunc. fail open.	Open circuit, mech. failure.	Spurious NI trouble alarms.	Annunciating.	None.	RPS trip logic not affected.	Same as 34 a)
	e) Trouble bistable relay contacts in power trip test interlock fail closed.	Contact arc and weld.	LPD and DNBR bistables in affected ch. will not be tripped during NI ch. test or when there is trouble in the NI drawer. LPD and DNBR bistables may not trip due to erroneous data.	Periodic test, lack of LPD/DNBR trip indic. during NI test.	3-channel redundancy. (4th channel in bypass)	RPS trip logic may go to 2-out-of-2.	Same as 34 a)
	f) Trouble bistable relay contacts in power trip test interlock fail open.	Open circuit, mech. failure.	Spurious ch. trips for LPD and DNBR if bypass relays are not engaged.	Annunciating.	3-channel redundancy. (4th channel in bypass)	RPS trip logic for LPD and DNBR goes to 1-out-of-2.	Same as 34 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 61 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
34) (Cont.)	g) 10^{-4} % log power bistable fails off.	Failure causes equiv. to trip ch. bistable fail modes.	Bistable will not energize when power exceeds 10^{-4}%. One HI log power trip ch. cannot be bypassed. Probable ch. trip for high log power.	Periodic test, annunc. ch. trip HI log power bypass permissive light not come on at power.	3-channel redundancy. (4th channel in bypass)	One ch. of HI log power tripped at power. Other 2 channels can still be bypassed for operation.	Same as 34 a)
	h) 10^{-4} % log power bistable fails on.	Fail. causes equiv. to trip ch. bistable failure modes.	Bistable will be energized at all power levels. Operator can bypass HI log power bistable at less than 10^{-4} % power.	3-channel comparison, periodic test.	3-channel redundancy. (4th channel in bypass)	RPS trip logic for high log power becomes 2-out-of-2 if ch. is bypassed.	Same as 34 a)
	i) 10^{-4} % log power bistable fails off.	Fail. causes equiv. to trip ch. bistable failure modes.	Bistable relay will not be energized below 10^{-4} % power. CWP will not be bypassed and CPC cannot be bypassed. Spurious LPD and DNBR ch. trips at Lo power plus spurious CWP's at Lo power.	Periodic test, 3-channel comparison.	3-channel redundancy. (4th channel in bypass)	One ch. for LPD, DNBR and CWP tripped at Lo power. Other 2 channels can still be bypassed.	Same as 34 a)
	j) 10^{-4} % log power bistable fails on.	Fail. causes equiv. to trip ch. bistable failure modes.	Bistable relay will remain energized above 10^{-4} % power. One CPC will remain bypassed and one ch. for CWP will remain bypassed.	CPC bypass permissive indication, test	3-channel redundancy. (4th channel in bypass)	RPS trip logic and CWP logic for LPD or DNBR beomes 2-out-of-2.	Same as 34 a)
	k) 10^{-4} % log power bistable contacts in CWP fail open.	Mech. failure, open circuit.	CWP will not be bypassed for LPD and DNBR below 10^{-4} % power. Possible spurious CWP ch. trip at Lo power if CPS is not bypassed.	Periodic test, annunc. for CWP ch. trip.	3-channel redundancy. (4th channel in bypass)	No impact on RPS trip logic or CWP as other chs. Are bypassed.	Same as 34 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 62 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
34) (Cont.)	l) 10^{-4} % log power bistable contacts in CWP fail closed.	Contact arc and weld.	CWP for LPD and DNBR will remain bypassed all power levels.	Periodic test.	3-channel redundancy. (4th channel in bypass)	CWP on LPD or DNBR pre-trip goes to 2-out-of-2.	Same as 34 a)
	m) 10^{-4} % log power bistable contacts in CPC fail open.	Mech. failure, open circuit.	CPC bypass permissive for one channel not enabled below 10^{-4} % power. Unable to bypass one CPC. Possible LPD and DNBR ch. trips at low power.	Periodic test, annunc. for ch. trip.	3-channel redundancy. (4th channel in bypass)	No impact on RPS trip logic as other CPC's can still be bypassed.	Same as 34 a)
	n) 10^{-4} % log power bistable contacts in CPC fail closed.	Contact arc and weld.	CPC bypass will not be automatically removed at 10^{-4} % power. CPC will be bypassed.	CPC bypass indic. test	3-channel redundancy. (4th channel in bypass)	RPS trip logic for LPD and DNBR becomes 2-out-of-2.	Same as 34 a)
	o) Rate of change of power bistable fails on.	Fail. causes equiv. to trip ch. bistable fail. modes.	Loss of annunc. at HI rate of change of power for on channel.	Periodic test.	3-channel redundancy. (4th channel in bypass)	HI rate of change of power annunc. logic goes to 1-out-of-2.	Same as 34 a)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 63 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
34) (Cont.)	d) Rate of change of power bistable fails off.	Fail. causes equiv. to trip ch. bistable fail. modes.	Spurious HI rate of change of power alarms.	Annunciating.	None.	No impact on RPS trip logic.	Same as 34 a)
	q) Log power level summers fail HI.	Comp. failure.	Erroneous log power level indic. at main control board or remote shutdown area.	3-channel comparison, periodic test.	3-channel redundancy. (4th channel in bypass)	No impact on RPS trip logic.	
	r) Log power level summers fail off.	Comp. failure, open circuit.	Loss of log power level indic. at main control board or remote shutdown area.	Operator.	3-channel redundancy. (4th channel in bypass)	No impact on RPS trip logic.	
	s) Calibrated linear power level summer fails HI.	Comp. failure.	HI linear power indic. at main control board.	3-channel comparison, periodic test.	3-channel redundancy. (4th channel in bypass)	No impact on RPS trip logic.	
	t) Calibrated linear power level summer fails off.	Comp. failure, open circuit.	Loss of one channel of linear power indic. on main control board.	Operator.	3-channel redundancy. (4th channel in bypass)	No impact on RPS trip logic.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 64 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
34) (Cont.)	u) Rate of change of power summer fails HI.	Comp. failure.	Erroneous power change rate indic. at main control board.	3-channel comparison, periodic test.	3-channel redundancy. (4th channel in bypass)	No impact on RPS trip logic.	
	v) Rate of change of power summer fails off.	Comp. failure, open circuit.	Loss of rate of change of power indic. for one channel.	Operator.	3-channel redundancy. (4th channel in bypass)	No impact on RPS trip logic.	
35) High Log Power Operating Bypass (70, 71, 79) (Ch. A Typ.)	a) Bypass relay AK27 coil open.	Sustained overvoltage.	High log power trip bypass cannot be obtained in Ch. A.	Whenever a bypass of high log power is attempted in the affected channel. Periodic PPS testing.	3-channel redundancy. (4th channel already in bypass)	Bistable will be tripped when the power level exceeds 1 to 2% full power.	The other 2 channels are unaffected and can be bypassed. Bypassing the other 2 channels precludes a trip caused by high LOG power as a coincidence of at least two channels is required to produce a trip.
	b) Bypass relay AK27 coil short		Shorted coil will cause auxiliary logic power supply voltage to be reduced to approximately zero when the power level exceeds 10^{-4} % full power.	Periodic test annunciation of power supply failure	3-channel redundancy (4th channel in bypass)	High log power bistable cannot be bypassed above 10^{-4}% power, channel will trip	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 65 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
35) (Cont.)	c) Bypass relay AK27 N.O. contact in bistable bypass circuit short.	Welded contact	High LOG power trip can be bypassed in the affected channel regardless of power level. Bypass not auto. removed.	Periodci PPS testing.	3-channel redundancy (4th channel in bypass)	Bistableis continually bypassed. Logic becomes 2-out-of-2 for Hi Log Power	System becomes 2-out-of-2 for that parameter at low power.
	d) Bypass relay AK27 N.O. contact in bistable bypass circuit open.	Deterioration of contact.	High LOG power trip cannot be bypassed in the affected channel.	Whenever a bypass of high LOG power is attempted in the affected channel. Periodic PPS testing.	3-channel redundancy (4th channel in bypass)	Bistable will be tripped when the power level exceeds 1 to 2% full power.	
	e) Relay AK27 N.O. contacts in permissive indic. circuit fail open.	Corrosion, mech. damage, open circuit.	Loss of bypass permissive indic. for ch. Operator not bypass HI log power bistable above 10^{-4}% power. Probable channel trip.	3-channel comparison, annunc. for ch. trip, periodic test.	Bypasses not affected for other 2 channels (4th channel in bypass)	Trip logic for HI log power not affected as other 2 chs. will be bypassed.	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 66 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
35) (Cont.)	f) Relay AK27 N.O. contacts in permis-sive indic. cir-cuit fail closed.	Contact weld.	Spurious operating bypass per-missive indication. Bypass cannot be initiated.	Visual indication, 4-channel compari-son.	Bypass capability not affected.	RPS trip logic not affected. Bypass cannot be initiated at less than 10^{-4}% power	Same as 35 e)
	g) Relay AK27 N.C. contacts in bypass annunc. circuit fail closed.	Contact weld, open circuit	Operating bypass permissive will not be annunciated when it is initiated.	Visual bypass per-missive indic. with no annunc., period-ic test.	Visual indication of ch. bypass per-missive, bypass capability not affected.	RPS trip logic not affected as bypass can still be init-ated.	
	h) Bypass relay driver fails off.	Open circuit, transistor failure.	Operating bypass for channel cannot be initiated. Probable HI log power channel trip above 10^{-4}% power.	Operator when initiating bypass.	Bypasses in other 2 channels not affected. (4th channel already bypassed)	Trip logic for HI log power will not be affected as other 2 channels can be bypassed.	Same as 35 e)
	i) Bypass relay driver fails on.	Emitter-to-collector short.	One channel operating bypass for HI log power will be auto-matically generated whenever power exceeds 10^{-4}% power.	Bypass annunc. before Operator initiates bypass.	Other 2 channels still must be manually bypassed. (4th channel already bypassed)	RPS trip logic for HI log power not affected. This trip normally bypassed above 10^{-4}% power. Bypasses automatic-ally removed below 10^{-4}% power.	Same as 35 e)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 67 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
35) (Cont.)	j) Bypass relay AK20 fails open.	Mech. damage, overstress.	Same as 35 h)	Same as 35 h)	Same as 35 h)	Same as 35 h)	Same as 35 e)
	k) Relay AK20 contacts in bypass circuit fail open.	Mech. damage, corrosion, open circuit.	Same as 35 h)	Same as 35 h)	Same as 35 h)	Same as 35 h)	Same as 35 e)
	l) Relay AK20 contacts in bypass circuit fail closed.	Contact weld.	Hi log power operating bypass for Ch. A will be engaged at all times. HI log power bistable will be bypassed at all power levels.	Visual bypass indic. at low power.	3-channel redundancy for HI log power trip. (4th channel in bypass)	RPS trip logic for HI log power goes to 2-out-or-2.	Same as 35 e)
	m) Relay AK20 N.C. contacts in "Bypass OFF" circuit fail closed.	Open circuit, contact weld.	Spurious and erroneous "Bypass OFF" indic. when bypass is in effect.	Concurrent "Bypass" and "Bypass OFF" indications.	Bypass not affected.	No impact on RPS trip logic.	Same as 35 e)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 68 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
35) (Cont.)	n) Relay AK20 N.C. contacts in "Bypass OFF" circuit fail open.	Corrosion, mech damage.	Loss of "Bypass OFF" indic. for one channel. Bypass not affected.	"Bypass OFF" and "Bypass" lamps off at same time.	Bypass not affected.	No impact on RPS trip logic.	
	o) Relay AK20 N.O. contacts in annunc. circuit fail open.	Open circuit, contact weld, corrosion.	Operating bypass permissive annunciator will not be turned off when the HI log power bypass is initiated.	Operator when initiating bypass.	None required.	No impact on RPS trip logic or bypass capability	
	p) Relay AK20 N.O. contacts in annunc. circuit fail closed.	Contact weld.	Same as 35 g)	Same as 35 g)	Same as 35 g)	Same as 35 g)	
	q) Manual bypass init. Switch (2 locations) open.	Comp. failure, contact corrosion.	Unable to manually initiate or remove HI log power operating bypass. (Bypass automatically removed below 10^{-4}% power.)	Operator when attempting to initiate or remove bypass.	Redundant bypass switches.	No impact on RPS trip logic. Bypass can be initiated from alternate locations.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 69 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
35) (Cont.)	r) Manual bypass switch (2 locations) fails to "bypass) position.	Contact weld.	Same as 35 i)	Same as 35 i)	Same as 35 i)	Same as 35 i)	Same as 35 i)
	s) Manual bypass switch (2 locations) fails to "OFF" position.	Contact weld.	Unable to manually initiate operating bypass using either switch. HI log power bistable in ch. will not be bypassed above 10^{-4}% power. Probable ch. trip at power.	Operator when attempting to initiate bypass, annunc. for channel trip.	3-channel redundancy for HI log power and operating bypass. (4th channel in bypass)	No impact on RPS trip logic. Other 2 channels can still be bypassed so reactor trip will not be initiated.	
	t) Aux. logic power supply fails off.	Open circuit, comp. failure.	Unable to bypass HI log power bistable. Probable ch. trip for HI log power above 10^{-4}% power.	Power supply trouble alarm, loss of all bypass indic. lamps in channel.	Separate power supplies used for bypasses in other channels.	No impact on RPS trip logic as other 2 channels can still by bypassed. (4th channel already in bypass)	
36) Power Trip Test Interlock (90, 95) (Ch. A Typ.)	a) 12 V aux. logic power supply fails off.	Open circuit, comp. failure.	Relay AK28 will be deenergized and its contacts will open, deenergizing (tripping) the Ch. A bistables for DNBR and LPD, if they are not bypassed.	Power supply trouble annunc. channel trip annunciation.	3-channel redundancy for LPD and DNBR. (4th channel in bypass)	RPS trip logic for LPD and DNBR goes to 1-out-of-2.	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 70 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
36) (Cont.)	b) Relay AK38 fails open.	Mech. damage, overstress.	Same as 36 a)	Same as 36 a)	Same as 36 a)	Same as 36 a)	Same as 36 a)
	c) Relay AK28 N.O. contacts in LPD circuit fail open.	Contact corrosion, open circuit.	Power to Ch. A LPD bistable will be interrupted, resulting in spurious Ch. A LPD trip.	Annunciating.	3-channel redundancy for LPD. (4th channel in bypass)	RPS trip logic for LPD goes to 1-out-of-2.	Same as 36 a)
	d) Relay AK28 N.O. contacts in LPD circuit fail closed.	Contact weld.	Ch. A LPD bistable will not be tripped when there is trouble in the NI drawer. Ch. A LPD bistable may not trip due to erroneous input if there is trouble in NI drawer.	Periodic test, no LPD ch. trip when NI trouble occurs.	3-channel redundancy for LPD. (4th channel in bypass)	RPS trip logic for LPD goes to 2-out-of-2.	Same as 36 a)
	e) Relay AK28 N.O. contacts in DNBR circuit fail open.	Contact corrosion, open circuit.	Equivalent to 36 c) for DNBR trip.	Equiv. to 36 c) for DNBR trip.	Equiv. to 36 c) for DNBR trip.	Equiv. to 36 c) for DNBR trip.	Equiv. to 36 a) for DNBR trip.
	f) Relay AK28 N.O. contacts in DNBR circuit fail closed.	Contact weld.	Equivalent to 36 d) for DNBR trip.	Equiv. to 36 d) for DNBR trip.	Equiv. to 36 d) for DNBR trip.	Equiv. to 36 d) for DNBR trip.	Equiv. to 36 a) for DNBR trip.

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 71 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
36) (Cont.)	g) Trip channel bypass relay AXCK4-6 N.O. contacts in LPD circuit fail open.	Open circuit, contact corrosion.	Power trip test interlock for LPD will not be overridden when Ch. A LPD bistable is bypassed. Probable spurious LPD bistable trips during CPC tests or NI tests. Ch. trip will not occur because bistable is bypassed.	Periodic test, LPD bistable trip indic. on NI test while bistable bypassed.	3-channel redundancy (4th channel also bypassed)	RPS trip logic is 2-out-of-2 with bistable bypassed.	
	h) Trip channel bypass relay AXK4-6 N.O. contacts in DNBR circuit fail closed.	Contact weld.	Same as 36 d)	Same as 36 d)	Same as 36 d)	Same as 36 d)	Same as 36 a)
	i) Trip channel bypass relay AXK3-6 N.O. contacts in DNBR circuit fail open.	Open circuit, contact corrosion.	Equivalent to 36 g) for DNBR.	Equivalent to 36 g) for DNBR.	Equiv. to 36 g) for DNBR.	Equiv. to 36 g) for DNBR.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 72 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
36) (Cont.)	j) Trip channel bypass relay AXCK3-6 N.O. contacts in DNBR circuit fail closed.	Contact weld.	Same as 36 f)	Same as 36 f)	Same as 36 f)	Same as 36 f)	
37) CWP Logic (69, 99, 121) (Ch. A Typ.)	a) CWP contact from CPC fails open.	Open circuit, mech. damage, contact corrosion.	Relay AK11 is deenergized and contacts in the CWP logic matrix are opened. Spurious CWP ch. trip.	Visual indication.	3-channel redundancy. (4th channel in bypass)	No impact on RPS trip logic, CWP logic goes to 1-out-of-2.	To restore the system logic to 2-out-of-3 coincidence, the operator must restore the bypassed channel to operation and then bypass the failed channel.
	b) CWP contact from CPC fails closed.	Contact weld.	Relay AK11 will not be de-energized on LPD and DNBR pre-trip signals.	Periodic test, LPD or DNBR pre-trip indic. with no ch. A CWP indication.	3-channel redundancy. (4th channel in bypass)	No impact on RPS trip logic. CWP logic goes to 2-out-of-2.	
	c) CWP indic. lamp burn out	Overstress, end natural life.	No visual indication of Ch. A CWP trip.	Periodic test.	None required.	No impact on CWP logic or RPS trip logic.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 73 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
37) (Cont.)	d) Relay AK11 fails open.	Mech. damage, overstress.	Same as 37 a)	Same as 37 a)	Same as 37 a)	Same as 37 a)	Same as 37 a)
	e) Relay AK11 contacts in CWP logic, one set fails open.	Contact corrosion, open circuit.	CWP 2-of-4 logic matrix partially enabled (for CWP on low DNBR or HI LPD).	Periodic test.	3-channel redundancy. (4th channel in bypass)	CWP logic remains 2-out-of-3 with one contact set open.	
	f) Relay AK11 contacts in CWP logic, one set fails closed.	Contact weld.	One set of contacts in CWP logic matrix (for CWP on LO DNBR or HI LPD) will not open for valid signal. One "2-out-of-4" combination no longer valid.	Periodic test.	3-channel redundancy. (4th channel in bypass)	CWP logic for DNBR or LPD becomes 2-out-of-2.	
	g) 12 V aux. logic power supply fails off.	Comp failure, open circuit.	Relay AK11 will be deenergized and contacts in CWP 2-of-4 ladder will open. Spurious CWP "Ch." trip.	Power supply fail annunc., visual CWP ch. trip indication.	3-channel redundancy. (4th channel in bypass)	CWP logic goes to 1-out-of-2.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 74 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
38) CPC Test Enable (Ch. A Typ.)	a) Bypass relay AXK2-6, N.O. contacts in enable circuit fail open.	Contact corrosion, open circuit.	Relay AK56 will not be energized when Ch. A DNBR bistable bypassed. Unable to test CPC.	Operator when attempting to test CPC.	None.	No impact on RPS trip logic.	
	b) Bypass relay AXK3-6 N.O. contacts in CPC test enable circuit fail closed.	Contact weld.	Relay AK56 will be energized, and the CPC test enable circuit will be partially enabled.	Annunciating.	HI LPD bistable must still be bypassed to enable the CPC test.	No direct impact on RPS trip logic.	
	c) Bypass relay AXK4-6 N.O. contacts in CPC test enable circuit fail open.	Contact corrosion, open circuit.	Equivalent to 38 a)	Equiv. to 38 a)	Equiv. to 38 a)	Equiv. to 38 a)	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 75 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
38) (Cont.)	d) Bypass relay AXK4-6, N.O. contacts in CPC test enable circuit fail closed.	Contact weld.	Equivalent to 38 b)	Equiv. to 38 b)	Equiv. to 38 b)	Equiv. to 38 b)	
	e) Relay AK56 fails open.	Mech. damage, overstress.	Equivalent to 38 a)	Equiv. to 38 a)	Equiv. to 38 a)	Equiv. to 38 a)	
	f) Relay AK57 fails open.	Mech. damage, overstress.	Equivalent to 38 a)	Equiv. to 38 a)	Equiv. to 38 a)	Equiv. to 38 a)	
	g) Relay AK56 N.O. contacts fail open.	Contact corrosion, open circuit.	Equivalent to 38 a)	Equiv. to 38 a)	Equiv. to 38 a)	Equiv. to 38 a)	
	h) Relay AK56 N.O. contacts fail closed.	Contact weld.	Equivalent to 38 b)	Equiv. to 38 b)	Equiv. to 38 b)	Equiv. to 38 b)	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 76 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
38) (Cont.)	i) Relay AK57 N.O. contacts fail open.	Contact corrosion, open circuit.	Equivalent to 38 a)	Equiv. to 38 a)	Equiv. to 38 a)	Equiv. to 38a)	
	j) Relay AK57 N.O. contacts fail closed.	Contact weld.	Equivalent to 38 b)	Equiv. to 38 b)	Equiv. to 38 b)	Equiv. to 38 b)	
	k) Aux logic power supply (Ch. A) fails off.	Comp. failure, open circuit.	Equivalent to 38 a)	Power supply trouble annunication.	None.	No impact on RPS logic	
39) Trip Input By-pass Switch AXS-1 (BXS-1, CXS-1 DXS-1)	a) Switch fails in normally off posi-tion	Mechanical binding of switch	Switch cannot be turned to the "trip input bypass" position for testing of the channel A (B, C, or D) bistable for trip parameter 1	Operator when pre-paring to test bistable, visual indication	None for bypass. 3 channel redun-dancy for PPS trip logic (4th channel in bypass)	No direct effect on PPS trip logic. However, will not be able to test the bistable in channel A.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 77 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
39) (Cont.)	b) Switch fails in the on "bypass" position	Mechanical binding or other mechanical failure of switch	Switch cannot be returned to the off position. The trip inputs to the AB, AC and AD logic matrices will be bypassed for Trip Parameter 1. Also, trip input bypass capability for trip parameter 1, channels B, C and D will be lost.	Operator when attempting to remove trip input bypass after test, visual indication	None for trip input bypass switch. 3 channel redun-dancy for PPS (4th channel is bypassed at the bistable)	PPS trip logic for trip parameter 1 becomes 2-out-of -2 coincident.	To restore PPS trip logic to 2-out-of-3 coincident, the channel that is bypassed at the bistable must be restored to service and channel A by-passed at the bistable until the trip input bypass switch is repaired.
40)	This item left blank intentionally.						
41)	This item left blank intentionally.						

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 78 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
42) Bypass Relay Coil AXK-1	a) Open	Sustained overvoltage.	Bistable "1" in Ch. A cannot be bypassed.	Periodic PPS testing or when attempting to bypass the bistable.	Noise for bypass, 3 channel redundancy for PPS Trip Logic (4th channel bypassed at bistable)	If the bistable is tripped, the system becomes any 1-out-of-2 logic for the affected function.	
	b) Short.	Deterioration of insulation.	No symptoms until an attempt is made to bypass bistable "1" in Ch. A. Inserting the bypass will force the supply voltage down and cause all bypasses in channel A to be removed.	Periodic PPS testing or when attempting to bypass the bistable.	Same as 42 a)	If the bypass is attempted it will result in the loss of all bypass capability for that channel.	If that particular bypass is not attempted there will be no effect upon the other bypass circuits in that channel.
43) Bypass relay (AXK1 Typcial) N.O. Contacts Set 1, Set 2 or Set 3	a) Contacts fail open.	Contact corrosion, open circuit.	Bistable trip relay contacts in one logic matrix will not be bypassed. Affected logic matrix will be half-tripped during bistable test.	Periodic test.	3-channel redundancy. (4th channel bypassed at bistable)	RPS trip logic for affected parameter is essentially 2-out-of-2 or 1-out-of-2 selective.	
	b) Contacts shorted.	Contact weld.	Bistable trip relay contacts in one logic matrix will be permanently bypassed. Affected logic matrix will not trip for valid signal coincidence.	Periodic test.	3-channel redundancy. (4th channel bypassed at bistable)	RPS trip logic for affected parameter becomes 2-out-of-2.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 79 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
44) Bypass Relay (AXK1 Typical) N.O. Contacts in Indicator Circuit	a) Contacts fail open.	Contact corrosion.	No visual indication of channel bypass.	Operator when bypassing channel.	Audible bypass annunciation.	RPS trip logic not affected.	
	b) Contacts shorted.	Contact weld. Open circuit.	Spurious visual indication of channel bypass.	Visual indication.	None.	No impact on RPS trip logic.	
45) Bypass Relay (AXK1 Typical) N.O. Contact in Annunc. Circuit	a) Contacts fail open.	Contact corrosion, open circuit.	No annunciation when channel is bypassed.	Operator when bypassing channel.	Visible bypass indication.	No impact on RPS trip logic.	
	b) Contacts shorted.	Contact weld.	Spurious channel bypass alarms.	Annunciating.	None.	No impact on RPS trip logic.	
46) Bypass Relay Cotnact Set 6A, 6B	These contact sets (1 N.O. and 1 N.C.) are spares for all parameters except HI LPD and LO DNBR. For these two parameters, these contact sets are used in the Power Trip Test Interlock and the CPC Test enable. See Line Items 36 and 38.						
47) Auxiliary Bypass Relay AXKB6, AXKB9, AXKB10, AXKB11, AXKB12 or AXKB13.	a) Coil fails open.	Mech. damage, overstress.	The ESFS actuation relays associated with the affected parameter (LO PZR press. for AXKB6, etc.) will not be bypassed when the trip bistable is tested. Three ESFS actuation logic mtrices (i.e., AB, AC and AD for Ch. A bistable) for a specific ESFS function (i.e., SIAS for LO PZR press, AXKB6) will be half-tripped.	Periodic test.	3-channel redundancy. (4th channel bypassed at bistable)	Actuation logic for a given ESF function goes to 1-out-of-2.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 80 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
48) Auxiliary Bypass Relay Contact Sets 1, 2 or 3	a) Contact set fails open.	Corrosion, mech. damage, open circuit.	Bistable trip relay contacts in one ESF actuation logic matrix will not be bypassed when the bistable is tested. Affected logic matrix is half-tripped during bistable test.	Periodic test, visual indication	3-channel redundancy. (4th channel bypassed at bistable)	Actuation logic for one ESF function becomes 1-out-of-2 selective or any 2-out-of-2.	
	b) Contacts shorted.	Contact weld.	Bistable trip relay contacts in one ESF actuation logic matrix will be permanently bypassed. ESF logic matrix will not trip for valid signal coincidence.	Periodic test.	3-channel redundancy. (4th channel bypassed at bistable)	Actuation logic for one ESF function becomes 2-out-of-2.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 81 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
49) Trip Channel Bypass Power Supplies (PS-49, PS-52, Ch. A Typ.)	One Fails off	Comp. failure, open circuit.	Loss of one of two redundant power supplies for the trip channel bypass relays.	Visual indication	Redundant power supply.	No impact RPS Trip or ESFS Actuation logic.	
50) Trip Channel By-pass Power Supply Indi-cator Lamp	Fails off	Broken Fila-ment, end of natural life, open circuit.	Spurious trip channel bypass power supply failure indica-tion.	Visual indication.	None required.	No impact on trip logic.	
51) RPS 2-of-4 Trip Logic Matrix (AB Typical)	a) One of two matrix power sup-plies (PS9 or PS-4 Typ.) fails off	Comp. failure, open circuit.	Loss of one of two logic matrix power supplies. Two of the four matrix relays will be de-energized.	Power supply trouble alarm, visual indication.	Second power supply provides power to both sides of "Logic Ladder", and to the two remaining logic matrix relays.	RPS trip logic remains 2-out-of-3. Two "Series" trip paths are tripped. (4th channel bypaased at bistables)	RPS trip path logic is 2-out-of-3 selective.
	b) One of two matrix power sup-lies fail HI.	Component failure.	Possible overstress of 2-of-4 logic matrix relays. Relays may fail open and logic matrix will become half tripped.	Visual indication if matrix relays fail open.	Same as above.	Same as above.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 82 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
51) RPS 2-of-4 Trip Logic Matrix (AB Typical) (Cont.)	c) Logic Matrix Power Supply Indicator Lamp Fails off	Open filament, natural end of life.	Spurious visual indication of failure of one logic matrix power supply.	Visual indication of power supply failure without alarm.	None required. trip logic.	No impact on RPS	
	d) Logic Matrix Power Supply Trouble Annunc. Relay Fails Open.	Overstress, mech. damage coil spool cracked, open coil winding	Spurious logic matrix power supply trouble alarms.	Annunciating.	None required.	No impact on RPS trip logic.	
	e) Logic matrix power supply trouble annunc. relay con-tacts fail open.	Mech. damage, corrosion, open circuit.	Same as 51 d)	Same as 51 d)	Same as 51 d)	Same as 51 d)	Same as 51 d)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 83 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
51) RPS 2-of-4 Trip Logic Matrix (AB Typical) (Cont.)	f) Logic matrix power supply trouble annunc. relay contacts fail closed.	Contact weld.	P/S trouble alarm will not sound if power supply fails.	None unless power supply fails, then lamp goes out but alarm doesn't sound.	Visual power supply operability indication.	No impact on RPS trip logic.	
	g) Logic Matrix Power supply diode fails open.	Overstress, mech. damage.	Equivalent to 51 a)	Equivalent to 51 a)	Equivalent to 51 a)	Equivalent to 51 a)	
	h) Logic matrix power supply diode shorted.	Overstress	No impact during normal operation, loss of isolation for power supplies.	None.	Redundant power supplies.	None.	
	i) Logic matrix power supply fuses fail open.	Overstress, mech. damage.	Equivalent to 51 a)	Equiv. to 51 a)	Equiv. to 51 a)	Equiv. to 51 a)	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 84 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
51) RPS 2-of-4 Trip Logic Matrix (AB Typical) (Cont.)	j) Bistable relay trip indicator lamp (A1 Typ.) fails off.	Broken filament.	Loss of visual indication for bistable relay trip in affected matrix.	Periodic test.	Bistable relay trip annunicator.	No impact on RPS trip logic.	
	k) Bistable Relay trip indicator lamp transistor driver fails off.	Comp. failure, open circuit.	Same as 51 j)	Same as 51 j)	Same as 51 j)	Same as 51 j)	
	l) Bistable trip indicator lamp transistor driver fails on.	Emitter to collector short.	Spurious indication of bistable relay trip in affected matrix.	Visual indication.	None required.	No impact on RPS trip logic.	
	m) Logic matrix relay driver fails open (AB-1 Typ.)	Transistor failure, open circuit.	One matrix relay will be de-energized, inducing a trip in one of the four RPS trip paths. One set of trip breakers open.	Visual indication.	A minimum of two RPS trip paths must be de-energized to produce a trip.	RPS trip still requires a 2-of-3 signal coincidence. (4th channel bypassed at bistable)	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 85 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
51) RPS 2-of-4 Trip Logic Matrix (AB Typical) (Cont.)	n) Logic matrix relay driver fails on.	Emitter ot collector short.	One logic matrix relay will not deenergize on a valid signal coincidence.	Periodic test.	Four redundant logic matrix relays.	RPS trip remains 2-out-of-3. Affected logic matrix can still generate a trip. (4th channel bypassed at bistable)	Other two active logic matrices are unaffected, and can also generate a trip on a valid signal coincidence. (Three logic matrices associated with the bypassed channel are not active.)
	o) Logic matrix relay fails open.	Open circuit, overstress.	Equiv. to 51 m)	Equiv. to 51 m)	Equiv. to 51 m)	Equiv. to 51 m)	Equiv. to 51 m)
	p) "Logic Ladder" diode (1-of-4) shorted.	Open circuit, overstress.	Same as 51 m)	Same as 51 m)	Same as 51 m)	Same as 51 m)	Same as 51 m)
	q) "Logic Ladder) diode (1-of-4) shorted.	Comp. failure.	No impact on logic matrix.	None.	None required.	No impact on RPS trip logic.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 86 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
51) RPS 2-of-4 Logic Matrix (AB Typical) (Cont.)	r) Logic matrix relay indicator lamp fails off.	Broken fila-ment.	Spurious indication that one logic matrix relay has been de-energized.	Visual indication.	None required.	No impact on RPS trip logic.	
	s) Logic matrix relay (1AB-1 Typ.) con-tacts in trip path fail open.	Open circuit, mech. damage, contact corrosion.	Same as 51 m)	Same as 51 m)	Same as 51 m)	Same as 51 m)	
	t) Logic matrix relay (1AB-1 Typ.) con-tacts in RPS trip path fail closed.	Contact weld.	Same as 51 n)	Same as 51 n)	Same as 51 n)	Same as 51 n)	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 87 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
52) EFSAS Actuation Logic Matrix (AB Typical)	Failure Modes a through i and their effects on the ESFAS Actuation Logic for all ESF functions are equivalent to failure modes a) through i) of Line item 51, and their effects on RPS trip logic.						
	j) Bistable relay trip indicator lamp fails off.	Broken filament, burnt out.	Loss of visual indication for a bistable relay trip for one ESF function (i.e., CSAS) in the AB matrix.	Periodic test.	Bistable relay trouble annunciator.	No impact on ESFAS actuation logic for any ESF function.	
	k) Bistable relay trip indicator lamp transistor driver fails off.	Transistor failure, open circuit.	Same as 52 j)	Same as 52 j)	Same as 52 j)	Same as 52 j)	
	l) Bistable relay trip indicator lamp transistor driver fails on.	Emitter-to-collector short.	Spurious visual indication of the trip of one bistable relay for one ESF function in the AB matrix.	Visual indication.	None required.	No impact on ESFAS actuation logic for any ESF function.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 88 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
	m) One logic matrix relay driver for one ESF function fails off.	Open circuit, transistor failure.	One logic matrix relay for the affected ESF function is de-energized, tripping 1 of 4 actuation paths.	Visual indication.	ESF actuation path logic is 2-of-3 selective. The other 2 actuation paths are not affected. (4th channel bypassed)	ESF actuation still requires a 2-of-3 signal coincidence.	
	n) One logic matrix relay driver for one ESF function fails on.	Emitter-to-collector short.	One logic matrix relay for the affected ESF function will not be deenergized for a valid signal coincidence, and the associated trip path will not trip.	Periodic test.	The remaining 2 logic matrix relays for the ESF function (in matrix AB) are not affected and can still generate a ESF trip on a valid signal coincidence.	ESFAS actuation logic remains 2-of-3, but the trip path logic for the AB matrix for the affected ESF becomes 2-out-of-2 selective. (4th channel in bypass)	
	o) One logic matrix relay for one ESF function fails open.	Overstress, mech. damage, coil open, coil shorted	Same as 52 m)	Same as 52 m)	Same as 52 m)	Same as 52 m)	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 89 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
52) ESFAS Actuation Logic Matrix (AB Typical) (Cont.)	p) One logic matrix relay's contacts in ESF actuation path fail open.	Mech. damage, corrosion, open circuit.	Same as 52 m)	Same as 52 m)	Same as 52 m)	Same as 52 m)	Same as 52 m)
	q) One logic matrix relay's contacts in ESF actuation path fail closed.	Contact weld.	Same as 52 n)	Same as 52 n)	Same as 52 n)	Same as 52 n)	Same as 52 m)
	r) One "Logic Ladder" diode for one ESF function fails open.	Open circuit, overstress.	Same as 52 m)	Same as 52 m)	Same as 52 m)	Same as 52 m)	Same as 52 m)
	s) One logic matrix relay indicator lamp fails off.	Burnt out, broken fila-ment.	Spurious indication that one logic matrix relay for one ESF function has de-energized.	Visual indication.	None required.	No impact on ESFAS actuation logic.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 90 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
53) RPS Trip Path (Path A Typ.)	a) Trip path power supply (PS-34 Typ.) fails off.	Comp. failure.	RPS trip A Relay and all ESF actuation path A Relays are deenergized. One trip path for RPS trip and ESF actuation is tripped.	Multiple visual and audible alarms.	The remaining 3 trip paths for RPS trip and ESF actu-ation are not affected.	Trip path logic for all functions changes from 2-of-4 selective to 1-of-3 selective.	
	b) Trip path power suuply (PS-34 Typ.) fails HI.	Failure internal to power supply.	Possible overstress of trip relays in one of the Ch. A trip paths (RPS trip or ESF actuation).	None.	P/S output Zener will maintain 12 VDC to trip paths.	None.	
	c) Trip path power supply indicator lamp fails off.	Burnt out, broken fila-ment.	Spurious visual indication of power supply failure.	Visual indication.	None required.	No impact on trip path.	
	d) Trip path power supply output Zener fails open.	Comp. failure.	Loss of overpower protection for Ch. A trip paths. If power supply fails high, trip path fuses will blow. Effect equivalent to 53 a).	None, unless P/S fails high, then trip path trip indications.	Same as 53 a)	Same as 53 a)	
	e). Trip path power supply output Zener shorted.	Overstress, comp. failure.	The trip path power supply will be shorted. See 53 a)	See 53 a)	See 53 a)	See 53 a)	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 91 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
53) RPS Trip Path (Ch. A Typ.) (Cont.)	f) RPS trip path fuse fails open.	Overstress, mech. damage.	Loss of power to RPS trip relay K1, one set of trip breakers open.	Annunciting.	The 3 remaining trip breakers are not affected.	Trip path logic becomes 1-of-3 selective, but a 2-out-of-3 signal coincidence is still required for RPS trip.	
	g) Ground detection circuit shorted.	Mech, failure, comp. failure.	Spurious indication of grounded trip path.	Annunciating.	None required.	No impact on RPS trip logic or RPS trip path.	
	h) Ground detection, circuit fails open.	Comp. failure, open circuit.	Loss of ground detection capa-bility for one trip path. If ground occurs, power supply will be loaded down. Fuse will probably blow. See 53 f)	None.	See 53 f)	See 53 f)	
	i) Trip relay (K-1 Typ.) fails open.	Mech. damage, overstress, open circuit, coil shorted.	K-1 relay contacts in trip breaker actuation circuits will change state and one set of trip circuit breakers (TCBs) will open.	Breaker status indication.	Other three TCBs are not affected.	Trip path logic becomes 1-of-3 selective, but 2-out-of-3 signal coincidence still required for trip.	
	j). Trip relay con-tacts in undervolt-age trip circuit fail open.	Mech. damage, open circuit.	Undervoltage trip circuit will deenergize, causing the trip circuit breaker to open.	Same as 53 i)	Same as 53 i)	Same as 53 i)	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 92 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
53) RPS Trip Path (Ch. A Typ.) (Cont.)	k) Trip relay contacts in undervoltage trip circuit fail closed.	Contact weld.	Undervoltage trip circuit for one TCB will not deenergize for valid trip signal. One TCB will not open.	Periodic test.	Other 3 TCBs are not affected and are sufficient to produce trip.	Trip path logic becomes 2-of-3 selectives, but 2-out-of-3 signal coincidence still required for trip.	
	l) Trip Relay contacts in shunt trip circuit fail closed.	Open circuit, contact weld, contamination.	Shunt trip circuit will be energized and one TCB will open.	Same as 53 i)	Same as 53 i)	Same as 53 i)	
	m) Trip relay contacts in shunt trip circuit fail open.	Contact corrosion.	Shunt trip circuit for one TCB will not be energized for valid trip signal.	Same as 53 k)	Same as 53 k)	Same as 53 k)	
	n) Remote indicator SSR fails open.	LED failure, SS transistor failure.	Spurious remote indicator of trip path A trip.	Visual indication.	None required.	No impact on RPS trip path or RPS trip logic.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 93 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
53) RPS Trip Path (Path A Typ.) (Cont.)	o) Remote indicator SSR fails on.	Emitter-to-collector short.	Loss of remote visual indication of trip path A trip.	Periodic test.	Local indication and plant annunc.	Same as above.	
	p) Local indicator SSR fails off.	LED failure, SS transistor failure.	Spurious local indication of trip path A trip.	Visual indication.	None required.	Same as above.	
	q) Local indicator SSR fails on.	Emitter-to-collector short.	Loss of local indication of trip path A trip.	Periodic test.	Remote indication and plant annunc.	Same as above.	
	r) Plant Annunc. SSR fails off.	LED failure, SS transistor failure.	Spurious annunciation of trip path A trip.	Annunciation	None required.	Same as above.	
	s) Plant annunc. SSR fails on.	Emitter-to-collector short.	Loss of annunciation for trip path A trip.	Periodic test.	Remote and local indication.	Same as above.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 94 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
53) RPS Trip Path (Path A Typ.) (Cont.)	t) One dropping resistor for one SSR fails open.	Mech. damage, overstress, open lead.	The affected SSR will be de-energized. See 53 n), p), or r) for affects.	See 53 n),p), or r)	See 53 n),p), or r)	See 53 n),p),or r)	
	u) One dropping resistor for one SSR shorted.	Comp. failure.	The affected SSR will see a higher control signal voltage SSR will probably fail open due to overstress.	See 53 n),p) or r)	See 53 n),p) or r)	See 53 n),p) or r)	
54) Trip Circuit Breaker Actuation (TCB-1 Typ.)	a) Bus 1, 125 VDC, fails off.	Mech. damage, ground.	TCB-1 undervoltage trip circuit will be deenergized, and TCB-1 will open.	Breaker status indication.	Other 3 TCBs are not affected.	One TCB open RPS trip still requires 2-out-of-3 signal coincidence.	
	b) Bus 1, fuse fails open.	Mech. damage, overstress.	Same as 54 a)	Same as 54 a)	Same as 54 a)	Same as 54 a)	
	c) Manual trip push-button contacts in undervoltage trip circuit fail closed.	Mech binding, contact weld.	Undervoltage trip circuit for one TCB will not be deenergized by its manual trip button. Shunt trip circuit can still open TCB.	Periodic test.	Auto trip function not affected, shunt grip circuit not affected. Other 3 TCBs not affected.	No impact on trip function.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 95 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
54) Trip Circuit Breaker Actuation (TCB-1 Typ.) (Cont.)	d) Manual Trip button contacts in under-voltage circuit fail open.	Open circuit	Undervoltage trip circuit will be deenergized and the TCB will open.	Breaker status indication.	Other 3 TCBs are not affected.	Same as 54 a)	
	e) Manual trip but-ton con-tacts in shunt trip circuit fail open.	Open circuit, mech. damage. contact corrosion.	Shunt trip circuit for the TCB will not be energized by manual trip button. Shunt trip circuit will not trip TCB.	Periodic test.	Underfreq. trip circuit will still open TCB. Other 3 TCBs not affected. Auto trip function not affected.	Same as 54 b)	
	f) Manual trip but-ton cont-tacts in shunt trip circuit fail closed.	Short circuit.	Shunt trip circuit will be energized and one TCB will open.	Breaker status indication.	Same as 54 a)	Same as 54 a)	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 96 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
54) Trip Circuit Breaker Actuation (TCB-1 Typ.) (Cont.)	g) Supplementary protection system (SPS) contacts in undervoltage trip circuit fail open.	Open circuit, mech. damage, SPS failure.	Undervoltage trip circuit for the TCB will be deenergized and the TCB will open.	Same as 54 a)	Same as 54 a)	Same as 54 a)	
	h) SPS contacts in undervoltage trip circuit fail closed.	Contact weld, SPS failure.	SPS will not deenergize the undervoltage trip circuit for one TCB on a valid trip signal.	Periodic test.	SPS still energizes shunt trip circuit to trip TCB auto and manual trip functions not affected. Other 3 TCB s not affected.	Same as 54 c)	
	i) SPS contacts in shunt trip circuit fail closed.	Short circuit, contact weld.	Shunt trip circuit for the TCB will energize and the TCB will open.	Same as 54 a)	Same as 54 a)	Same as 54 a)	
	j) SPS contacts in shunt trip circuit fail open.	Open circuit, mech. damage.	SPS will not energize shunt trip circuit for one TCB on valid trip signal.	Periodic test.	SPS will deenergize undervoltage trip circuit to trip TCB auto and manual trip funct. not affected.	Same as 54 c)	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 97 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
54) Trip Circuit Breaker Actuation (TCB-1) (Cont.)	k) Under-voltage trip cir-cuit fails open.	Open circuit, comp. failure.	Same as 54 d)	Same as 54 d)	Same as 54 d)	Same as 54 d)	
	l) Shunt trip circuit fails open.	Open circuit, comp. failure.	Unable to energize shunt trip circuit on valid trip signal, shunt trip circuit will not open TCB.	Periodic test.	Undervoltage trip circuit will open TCB. Other 3 TCBs unaffected.	Same as 54 c)	
	m) Closing circuit pushbutton fails closed.	Contact cor-rosion, mech. damage, open circuit.	Unable to energize TCB closing circuit to close TCB after test or trip.	Operator, TCB status indicator.	Other 3 TCBs are not affected.	Same as 54 a)	
	n) Closing circuit pushbutton fails closed.	Short cir-cuit, mech. damage, contact weld.	Closing circuit will remain energized, and oppose the shunt trip circuit. TCB opening will rely on spring for trip signal.	Periodic test.	TCB will still open on trip signal. Other 3 TCBs are not affected, circuit breaker spring loaded to open.	Trip actuation logic remains 2-of-4 selective. Trip still requires a 2-out-of-3 signal coincidence.	No impact on RPS Trip Logic or trip actua-tion.
	o) Closing circuit fails off.	Open circuit, comp. failure.	Same as 54 m)	Same as 54 m)	Same as 54 m)	Same as 54 m)	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 98 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
54) Trip Circuit Breaker Actuation (TCB-1 Typ.) (Cont.)	p) TCB fails closed.	Mech. binding, contact weld, short circuit.	TCB will not open in response to trip actuation signal.	Periodic test.	Other 3 TCBs not affected.	Same as 54 n)	
	q) TCB fails open.	Open circuit, mech. damage.	TCB will be open.	Breaker status indication.	Other 3 TCBs not affected.	Same as 54 a)	
	r) TCB N.O. contacts in status circuit fails open.	Mech. damage, contact corrosion, open circuit.	Loss of visual indication for closed TCB.	Visual indication.	"TCB Open" lamp will come on when breaker opens. TCB function not affected.	No impact on RPS trip function.	
	s) TCB N.O. contacts in status circuit fail closed.	Short circuit, contact weld.	"TCB Closed" lamp remains on when TCB opens.	Periodic test, "TCB Open" and "TCB Closed" lamps on at same time.	None required.	Same as above.	
	t) TCB NC contacts in status circuit fail closed.	Open circuit, contact weld.	"TCB Open" lamp stays on when breaker is closed.	Visual indication.	None required, TCB funct. not affected.	Same as 54 r)	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 99 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
54) Trip Circuit Breaker Actuation (TCB-1 Typ.) (Cont.)	u) TCB NC contacts in status circuit fail open.	Contact corrosion, mech. damage.	"TCB Open" lamp will not come on when breaker opens.	Periodic test.	"TCB Closed" lamp goes off when breaker opens, TCB not affected.	Same as 54 r)	
	v) "TCB Open" lamp fails off.	Burnt out, mech. damage.	Same as 54 u)	Same as 54 u)	Same as 54 u)	Same as 54 u)	
	x) "TCB Closed" lamp fails off.	Burnt out, mech. damage.	Same as 54 r)	Same as 54 r)	Same as 54 r)	Same as 54 r)	
55) 480 V ac Bus (Bus 1 Typ.)	Fails off.	Short mech. damage.	Loss of one of two redundant 480 V ac supplies to the CEDMs	Bus current indic.	Redundant bus.	None.	
56) MG Set Input Breaker (MG-1 Typ.)	a) Fails Open.	Open circuit, mech. damage	Loss of 480 V ac input to 1 MG set. Loss of 1 of 2 redund. Supplies to CEDMs.	Input breaker status indication.	Redundant MG set and bus.	None.	
	b) Fails Closed.	Contact weld, Mech. binding.	No impact on normal operation. Loss of overcurrent protect, for MG set. Possible damage to MG set if overcurrent occurs.	None.	MB output breaker, redundant MG set and bus.	None.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 100 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
57) Motor-Generator Set (MG-1 Typ.)	Fails off	Motor fails, generator fails, fly-wheel failure.	Loss of 1 of 2 480 V ac inputs to the CEDMs.	MG Set status indic.	Redundant MG set.	None.	
58) MG Set Output Breaker	a) fails Open.	Open circuit, mech damage.	Same as 57 a)	Same as 57 a)	Same as 57 a)	Same as 57 a)	
	b) Fails Closed.	Contact weld, mech. binding.	No impact on normal operation, loss of overload protect for MG output. Possible damage to generator on overcurrent.	None.	Redundant MG set.	None.	
59) MG Set Load Con-tactors	a) Fails Open.	Open circuit, mech. damage, contact cor-rosion	Same as 57 a)	Same as 57 a)	Same as 57 a)	Same as 57 a)	
	b) Fails Closed.	Contact weld, short circuit.	No impact on normal operation. Possible damage to generator due to motoring when MG set is unloaded.	None.	MG set breakers, redundant MG set.	None.	
60) CEDM Ring Bus Current Status Indicator (1 of 2)	Fails off	Open circuit, comp.failure.	Spurious indication of loss of current in one side of ring bus.	Indicating.	None required.	None.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 101 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
61) Synchronizing Circuit (SIAS, Ch. A Typ.)	Fails HI or LOW	Comp. failure.	Unable to synchronize one MG set to the CEDM bus possible MG set.	Operator, when trying to synch. MG set.	Redundant MG set.	None.	
62) ESFAS Initiation Circuit (SIAS, Ch. A Typ.)	Failure Modes a) through e) and their effects on the ESFAS Initiation Circuit are equivalent to Line Item 53, Failure Modes a) through e) and their effect on RPS trip initiation circuit.						
	f) ESFAS initiation circuit (SIAS, Ch. A Typ) fuse fails open.	Overstress, mech. damage, degradation.	Loss of power to Ch. A initiation relays, one leg of the actuation circuit open for Train A and Train B.	Annunciating, visual indication.	The other 3 ESFAS init. channels are not affected.	ESFAS Init. path logic becomes 1-of-3 selective, but a 2-out-of-3 signal coincidence still required for ESFAS actuation.	
	g) Remote manual pushbutton fails open.	Mech. damage, contact corrosion, open circuit.	Same as 62 e)	Same as 62 e)	Same as 62 e)	Same as 62 e)	
	h) Remote manaul pushbutton fails closed.	Contact weld, short circuit, mech damage.	Unable to deenergize the Ch. A init. relays for one ESFAS function using the remote manual pushbutton.	Periodic test.	Auto init. Capability not affected. Other 3 init. circuits can init. desired ESFAS function manually.	Auto ESFAS init. unaffected. Manual ESFAS init. for one function becomes 2-of-3 selective.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 102 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
62) ESFAS Initiation Circuit (SIAS, Ch. A Typ.) (Cont.)	i) SSR lockout relay fails off.	LED failure, SS transistor failure.	No impact on normal operation. Unable to reset ESFAS init. relays for one ESFAS function after chan. Has been tripped.	Operator, when re-setting channel.	Same as 62 e)	Init. path logic for one ESFAS funct. becomes 1-of-3 selective, actuation requires 2-out-of-3 signal coincidence.	
	j) SSR Lockout relay fails on.	Emitter-to-collector short.	No impact on normal operation. After trip, initiation circuit for one ch. of one ESFAS function can reset itself if trip clears on all foru initiating bistables.	Periodic test.	Other 3 init. circuit ch. not affected and will remain locked out.	None.	
	k) Lockout reset pushbutton fails open	Contact corrosion, mech. damage, open circuit.	Same as 62 h)	Same as 62 h)	Same as 62 h)	Same as 62 h)	
	l) Lockout reset pushbutton fails closed.	Contact weld, short circuit, mech. damage.	No impact on normal operation. The affected init. circuit will automatically reset when the reset key switch is engaged.	Operator, when resetting ch.	Other 3 init. circuit chans. for affected funct. are not affected.	None.	
	m) Lockout key switch fails open	Mech. binding. open circuit, contact corrosion.	Same as 62 h)	Same as 62 h)	Same as 62 h).	Same as 62 h)	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 103 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
62) ESFAS Initiation Circuit (SIAS, Ch. A Typ.) (Cont.)	n) Lockout key switch fails closed.	Contact weld, mech. binding or damage, short circuit.	No impact on normal operation. Operator will be able to reset the affected init. circuit after trip without using the reset key.	None.	Other 3 init. circuits are not affected.	None.	Operator will not know that the init. circuit can be reset without the reset key.
	o) Lockout keyswitch relay (K1201) fails open.	Open circuit, mech. damage, overstress.	Same as 62 h)	Same as 62 h)	Same as 62 h)	Same as 62 h)	
	p) Lockout keyswitch relay contacts in reset circuit fail open.	Contact corrosion, open circuit, mech. damage.	Same as 62 h)	Same as 62 h)	Same as 62 h)	Same as 62 h)	
	q) Lockout keyswictch relay contacts in reset circuit fail closed.	Contact weld, short circuit.	Same as 62 m)	Same as 62 m)	Same as 62 m)	Same as 62 m)	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 104 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
62) ESFAS Initiation Circuit (SIAS, Ch. A Typ.) (Cont.)	r) Train A or B initiation relay coil (SIAS, CIAS, or MSIS only) fails open.	Mech. damage, overstress, open circuit.	One set of relay contacts in the actuation circuit for one train of one ESF function will open.	Annunciating	Remaining 3 init. relays for the affected ESF func. train are still energized	ESFAS actuation still requires 2-out-of-3 signal coincidence. Initiation relay logic changed to 1-of-3 selective.	
	s) Train A or B initiation relay N.O. contact in actuation circuit fails open (SIAS, CIAS, or MSIS only).	Open circuit, contact corrosion, mech. damage.	Same as 62 q)	Same as 62 q)	Same as 62 q)	Same as 62 q)	
	t) Train A or b init. relay N.O. contacts in actuation circuit fail closed (SIAS, CIAS, or MSIS only).	Contact weld, short circuit.	One set of relay contacts in the actuation circuit for one train of one ESF function will not open on a valid 2-out-of-4 siganl coincidence.	Periodic test.	Remaining 3 init. relays for the affected ESF func. train are capable of actuating the train.	Actuatuion for one ESF function train becomes 2-of-3 selective. ESFAS actuation still requries a 2-out-of-3 signal coincidence.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 105 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
62) ESFAS Initiation Circuit (SIAS, Ch. A Typ.) (Cont.)	u) Train A or B solid init. relay fails off. (CSAS, RAS, AFAS-1 or AFAS-2).	LED failure, SS trans. failure, open circuit, drop ping resistor failure.	Equivalent to 62 q)	Equiv. to 62 q)	Equiv. to 62 q)	Equiv. to 62 q)	
	v) Train A or B solid state initiation relay fails on. (CSAS, RAS, AFAS-1, or AFAS-2).	Emitter-to-collector short.	Equivalent to 62 s)	Equiv. to 62 s)	Equiv. to 62 s)	Equiv. to 62 s)	
	w) Remote Indication SSR fails off.	LED failure, SS transistor failure, dropping resistor fail.	Spurious indication of initi-ation Ch. trip on remote PPS module.	Visual indication.	None required.	None.	
	x) Remote indication SSR fails on.	Emitter-to-collector short.	Loss of remote visual indica-tion for initiation circuit trip.	Periodic test.	Local visual indicator.	None.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 106 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
62) ESFAS Initiation Circuit (SIAS, Ch. A Typ.) (Cont.)	y) Local indication SSR fails off.	LED failure, SS transistor failure, resistor failure.	Spurious local indication of initiating circuit trip.	Visual indication.	None required.	None.	
	z) Local indication SSR fails on.	Emitter-to-collector short.	Loss of local visual indication of initiation circuit trip.	Periodic test.	Remote visual trip indicator.	None.	
	aa) Initiation reset flasher SSR fails off.	LED failure, SS transistor failure, dropping resistor failure.	Initiation reset flasher in test circuit will flash, indicating a spurious channel initiation.	Visible indication.	None required.	None.	
	ab) Initiation reset flasher SSR fails on.	Emitter-to-collector short.	Initation reset flasher in test circuit will not provide indication that a channel initiation has occurred during test. Operator may test another channel - leading to actuation.	Local and remote initiation indication without initiation reset indic. during test.	Local and remote initiation indication.	Possible ESF function actuation during test. Possible reactor trip if MSIVs are closed.	Operator error needed to produce ESF actuation during test. No adverse safety impact on plant. Failure not affect normal PPS operation.

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 107 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
63) ESFAS Actuation Circuit (SIAS, CSAS, RAS, MSIS, or CIAS).	a) One 36 V dc power supply fails off.	Component failure.	Loss of one of two redundant power supplies for one set of component actuation relays.	Annunciating.	Redundant power supply.	None.	
	b) One 120 V ac vital bus circuit breaker fails open.	Mech. damage, high current.	Equivalent to 63 a)	Equiv. to 63 a)	Equiv. to 63 a)	Equiv. to 63 a)	
	c) One 120 V ac vital bus circuit breaker fails closed.	Contact weld, mech. damage.	No impact on normal operation. Power supply is supplied with a 30 A input fuse. Fuse will open if input current exceeds 30A and the power supply will lose input power.	Periodic test, power supply failure is annunciated.	Redundant power supply.	None.	
	d) 36 V dc power supply indicator lamp fails off.	End of life, burnt out, mech. damage.	Spurious visual indication of power supply failure.	Visual indication.	None required.	None.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 108 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
63) ESFAS Actuation Circuit (SIAS, CSAS, RAS, MSIS, or CIAS). (Cont.)	e) 36 V dc power supply trouble annunci-ator relay fails open.	Overstress, mech. damage, open coil winding.	Spurious power supply failure alarm.	Annunciating.	None required.	None.	
	d) 36 V dc power supply trouble annunc. relay shorted.	Insulation failure.	Output of one 36 V dc P/S will be shorted. Automatic elec-tronic current limiting circuit limits output current to a preset value.	Annunciating for power supply failure.	Redundant power supply.	None.	
	g) One auction-eering diode fails open.	Overstress, open circuit, mech. damage.	Equivalent to 63 a)	Equiv. to 63 a)	Equiv. to 63 a)	Equiv. to 63 a)	
	h) Auc-tioneering diode shorted.	Overstress, internal failure.	Loss of isolation between two 36 V dc power supplies.	Periodic test.		None.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 109 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
63) ESFAS Actuation Circuit (SIAS, CSAS, RAS, MSIS, or CIAS). (Cont.)	i) One manual actuation pushbutton fails open.	Mech. damage, open circuit, contcat deteriora-tion.	One leg of the actuation cir-cuit for one ESFAS function will open up. Power for actu-ation relays will be supplied via opposite leg of circuit.	Annunciating.	Opposite leg of actuation circuit will supply power to actuation relays.	Manual ESFAS actu-ation becomes 1-of-1, auto initiation becomes 1-of-4 selective.	Auto ESFAS actuation still requires a 2-out-of-3 signal coincidence.
	j) One manual actuation pushbutton fails closed.	Contact weld, mech. damage.	The manual actuation button will not open one leg of actuation circuit.	Periodic test.	Automatic ESFAS actuation not affected.	Unable to manually actuate one ESFAS function.	
	k) Annunc-iation diodes fail open.	Overstress, open lead, mech. damage.	Equivalent to 63 i)	Equiv. to 63 i)	Equiv. to 63 i)	Equiv. to 63 i)	
	l) Annunc. diodes short.	Overstress, internal failure.	Voltage drop across diodes goes to zero, annunc. "sees" open circuit, spurious annunc. of one actuation circuit leg opening up.	Annunciating.	None required.	None.	
	m) Actu-ator cir-cuit indi-cator lamp fails off.	Filament burnt out, mech. damage.	Spurious visual indication that one leg of the actuator circuit has opened up.	Visual indication.	None required.	None.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 110 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
63) ESFAS Actuation Circuit (SIAS, CSAS, RAS, MSIS, or CIAS). (Cont.)	n) Lockout reset button fails open.	Contact deterioration, mech. damage, open circuit.	Unable to reset one leg of the actuation circuit after test or an actuation. Other leg can still be reset, which will reenergize lockout relay in affected leg.	Visual indication.	Reset pushbutton in other leg of actuation circuit.	None.	
	o) Lockout reset pushbutton fails closed.	Contact weld, mech. damage.	No imapct during normal operation, after auto. actuation. If actuation is caused by using manual actuation button, actuation relays will automatically reset.	Periodic test.	Automatic actuation and manual ESFAS initiation capabilities not affected.	One ESFAS function cannot be manually actuated from the actuation relay level.	Auto ESFAS actuation and manual ESFAS actuation from the initiation circuit not affected.
	p) Lockout relay N.O. contacts fail open.	Open circuit, contact deterioration.	Equivalent to 63 i)	Equiv. to 63 i)	Equiv. to 63 i)	Equiv. to 63 i)	Equiv. to 63 i)
	q) Lockout relay N.O. contacts fail closed.	Contact weld.	Same as 63 o)	Same as 63 o)	Same as 63 o)	Same as 63 o)	Same as 63 o)
	r) Lockout relay coil fails open.	Mech. damage, open winding.	Equivalent to 63 i)	Equiv. to 63 i)	Equiv. to 63 i)	Equiv. to 63 i)	Equiv. to 63 i)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 111 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
63) ESFAS Actuation Circuit (SIAS, CSAS, RAS, MSIS, or CIAS). (Cont.)	s) Lockout relay coil shorted.	Insulation failure, mech. short.	One group of actuation relays (either pumps or valves) will be shorted out, and will de-energized. Circuit breaker for affected group will probably open on high current.	Annunciating.	Only pumps or only valves will be actuated, so the full safety system will not be spur-iously actuated.	Either the pumps or the valves (but not both) in one train of one ESFAS function will be actuated.	
	t) Lockout relay surge protection diode fails open.	Overstress, mech damage.	Loss of surge protection for lockout relay. Possible damage to relay due to inductive kick when relay deenergizes. Relay may fail open.	Periodic test.	None required.	None.	
	u) Lockout relay surge protection diode shorted.	Overstress, internal failure.	Same as 63 s)	Same as 63 s)	Same as 63 s)	Same as 63 s)	Same as 63 s)
	v) One actuation relay coil fails open.	Mech. damage, open winding, open lead.	One valve or one pump will be actuated in one train of one ESFAS function.	Status indicator for affected valve or pump.	Only one com-ponent actuated, the full train for the affected ESFAS fucntion will not be spur-iously actuated by failure of one actuation relay.	Full ESFAS actua-tion still requires a 2-out-of-3 signal coincidence. Only a single comp. affec-ted by this failure. (4th input signal bypassed at bi-stable).	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 112 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
63) ESFAS Actuation Circuit (SIAS, CSAS, RAS, MSIS, or CIAS). (Cont.)	w) One actuation relay coil shorted.	Insulation failure, mech. short.	Actuation relay will not hold contacts, one pump or one valve actuated in one train of one ESFAS function.	Same as 63 v)	Only one component actuated, the full train for the affected ESFAS function will not be spuriously actuated by failure of one actuation relay.	Same as 63 v)	
	x) Actuation relay surge protection diode fails open.	Overstress, mech damage.	Equivalent to 63 t)	Equiv. to 63 t)	Equiv. to 63 t)	Equiv. to 63 t)	
	y) Actuation relay surge protection diode shorted.	Overstress, internal failure.	Same as 63 s)	Same as 63 s)	Same as 63 s)	Same as 63 s)	Same as 63 s)
	z) Actuation relay test relay fails open.	Open winding, mech. damage, overstress, open lead.	Unable to test the actuation of one pump or one valve in one Train of one ESF function.	Periodic test.	None required.	None.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 113 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
63) ESFAS Actuation Circuit (SIAS, CSAS, RAS, or CIAS). (Cont.)	aa) Actuation relay test relay N.C. contacts fail closed.	Contact weld, mech. damage.	Same as 63 z)	Same as 63 z)	Same as 63 z)	Same as 63 z)	
	ab) Actuation relay test relay N.C. contacts fail open.	Contact deterioration, mech. damage.	Same as 63 v)	Same as 63 v)	Same as 63 v)	Same as 63 v)	
	ac) Power return line circuit breaker fails open.	Contact deterioration, mech. damage.	Power return line for one group of actuation relays (pumps or valves) in one train of one ESF function opens up. Relays are de-energized.	Annunciating.	None.	All valves, or all pumps (but not both) in one train of one ESF function are actuated.	
	ad) Power return line circuit breaker fails closed.	Contact weld, mech. damage.	Loss of overcurrent protection for one leg of one actuation circuit.	Breaker test during shutdowns.	None.	None.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 114 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
64) ESFAS Actuation Circuit (AFAS-1, AFAS-2, or MSIS)	Failure Modes a) htrough h) and their effects are the same as for Line Item 63, Failure Modes a) through h).						
	i) Annunciator diodes fail open.	Overstress, mech. damage.	One actuation leg for AF pumps (or MSIVs) will open up. Corresponding aux. FW valve actuation leg not affected.	Annunciating	Opposite actuation leg for aux. FW pumps (or MSIVs) will provide power to act. relays.	AFW pump actuation becomes 1-of-2 selective. Valve act. not affected.	AFAS actuation still requires a 2-out of-3 signal coinci ence. (4th input signal bypassed at bistable)
	j) Annunc. diodes shorted.	Internal failure, overstress, mech short.	Voltage drop across annunc. diodes goesto zero. Annunc. "sees" an open circuit. Spuri ous AFAS (or MSIS actuation alarm.	Annunciating	None required.	None.	
	k) Actuation circuit indicator lamp fails off	Burnt out, mech. damage.	Spurious visual indication that one actuation leg has opened up.	Visual inciation.	None required.	None.	
	l) Lockout reset pushbutton fails open.	Contact deteriora-tion, mech. damage.	No imapct on normal operation. Unable to reset the AFW pump (or MSIV) portion of one actu-ation leg after test or actua tion. Reset button in opposite leg will provide power to reset relay and reset the affected leg.	Periodic test.	Reset pushbutton in opposite actu tion leg.	None.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 115 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
64) ESFAS Actuation Circuit (AFAS-1, AFAS-2, or MSIS) (Cont.)	m) Lockout reset pushbutton fails closed.	Contact weld, mech. damage.	No impact during normal operation or after automatic actuation. If actuation is via manual actuation button, actuation relays for AFW pump (or MSIV) will automatically reset when manual actuation button released.	Periodic test.	Automatic actuation and manual initiation not affected.	AFW pumps (MSIVs) cannot be manually actuated from the actuation circuit for either AFAS-1 or AFAS-2 (MSIS A, MSIS B).	Auto AFAS (MSIS) actuation and manual AFAS (MSIS) actuation from the initiation circuit not affected.
	n) Manual actuation button fails closed.	Contact weld, mech. damage.	Unable to manually actuate one AFAS Train (or MsiS Train).	Periodic test.	Same as above	Unable to manually actuate AFW pumps and one set of valves from the actuation circuit.	Same as above.
	o) Manual actuation button fails open.	Contact deterioration, mech damage.	One leg of one AFAS (MSIS) actuation circuit open. AFAS valve relay will de-energize and actuate valves. Pump relays will be powered by opposite leg.	Annunciating.		One set of AFAS valves will be actuated.	Full AFAS actuation still requires a 2-out-of-3 signal coincidence. (4th input signal by passed at bistable).
	p) Lockout relay fails open.	Open winding, overstress, mech. damage.	Equivalent to 64 i)	Equiv. to 64 i)	Equiv. to 64 i)	Equiv. to 64 i)	Equiv. to 64 i)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 116 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
64) ESFAS Actuation Circuit (ESFAS-1, AFAS-2, or MSIS) (Cont.)	q) Lockout relay shorted.	Insulation failure, mech. damage.	Shorted coil will draw high current, causing return line circuit breaker to open. One AFAS valve set and one pump (MSIV) set will be actuated.	Annunciating.	None.	One AFAS valve set and one pump set (MSIV) actuated. Possible reactor trip if one MSIV closes.	
	r) Lockout relay N.O. contacts fail open.	Contact de-terioration, mech. damage, open lead.	Equivalent to 64 i)	Equiv. to 64 i)	Equiv. to 64 i)	Equiv. to 64 i)	Equiv. to 64 i)
	s) Lockout relay N.O. contacts fail closed.	Contact weld, mech. damage.	Equivalent to 64 m)	Equiv. to 64 m)	Equiv. to 64 m)	Equiv. to 64 m)	Equiv. to 64 m)
	t) Lockout relay surge protection diode shorted.	Overstress, internal failure, mech. short.	Equivalent to 64 q)	Equiv. to 64 q)	Equiv. to 64 q)	Equiv. to 64 q)	Equiv. to 64 q)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 117 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
64) ESFAS Actuation Circuit (AFAS-1, AFAS-2, or MSIS) (Cont.)	u) Lockout relay surge protection diode shorted.	Mech. damage, overstress.	Loss of surge protection for lockout relay. Possible damage to relay due to inductive kick when relay deenergizes. Relay may fail open.	Periodic test.	None required.	None.	
	v) Pump actuation relay fails open.	Mech. damage, overstress, open winding.	One AFAS pump (MSIV) will be actuated.	Comp. status indic.	None.	For AFAS, one pump actuated. For MSIS, probable reactor trip due to MSIV closing.	
	w) Pump action relay shorted.	Insulation breakdown, mech. short.	Equivalent to 64 q)	Equiv. to 64 q)	Equiv. to 64 q)	Equiv. to 64 q)	Equiv. to 64 q)
	x) Pump actuation relay surge sup-presseion diode open.	Mech. damage, overstress.	Equivalent to 64 u)	Equiv. to 64 u)	Equiv. to 64 u)	Equiv. to 64 u)	Equiv. to 64 u)
	y) Pump actuation relay surge suppress. diode shorted.	Overstress, interanl failure, mech. short.	Equivalvent to 64 q)	Equiv. to 64 q)	Equiv. to 64 q)	Equiv. to 64 q)	Equiv. to 64 q)

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 118 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
64) ESFAS Actuation Circuit (AFAS-1, AFAS-2, or MSIS) (Cont.)	z) One test relay coil fails open.	Mech. damage, open winding, overstress, short circuit	Unable to test actuate one component.	Periodic test.	None.	None.	
	aa) Test relay N.C. contacts fail closed.	Contact weld, mech. damage.	Same as 64 z)	Same as 64 z)	Same as 64 z)	Same as 64 z)	
	bb) Test relay N.C. contacts fail open.	Contact deterioration, open lead, mech. damage.	Same as 64 v)	Same as 64 v)	Same as 64 v)	Same as 64 v)	
	cc) AFAS valve act. relay fails open.	Open winding, mech. damage, overstress.	One AFAS valve set will be actuated. One leg of pump actuation circuit will open, but opposite leg will provide power to pump act. relays.	Annunciating.	None.	One set of AFAS valves will be actu ated. Full AFAS (MSIS) actuation still requires a 2-out-of-3 signal coincidence. (4th input siganl bypassed at bistable)	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 119 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
64) ESFAS Actuation Circuit (AFAS-1, AFAS-2, or MSIS). (Cont.)	dd) AFAS valve act. relay shorted.	Insulation breakdown mech. short.	Equivalent to 64 q)	Equiv. to 64 q)	Equiv. to 64 q)	Equiv. to 64 q)	Equiv. to 64 q)
	ee) AFAS valve act. relay N.O. contacts in pump act. cir cuit fail open.	Open lead, mech. damage, contact deterioration.	Same as 64 i)	Same as 64 i)	Same as 64 i)	Same as 64 i)	Same as 64 i)
	ff) AFAS valve act. relay N.O. contacts in pump act. cir-cuit fail closed.	Contact weld, mech. damage.	SSR1A unable to actuate pump and valve group for one actuation leg.	Periodic test.	Manual actuation, SSR3A not affected.	Full actuation of AFAS (MSIS) requires 2-of-4 selective input from init. circuit.	AFAS actuation still requires 2-out-of-3 signal coincidence. (4th input signal bypassed at bis table).
	gg) Power return circuit breaker open.	Mech. damage, open circuit.	One entire actuation leg for one AFAS (MSIS) train is de-energized. One AFAS valve set and one pump set (MSIV) actuated.	Annunciating.	None.	For AFAS, one valve set and one pump set in one AFAS train are actuated. For MSIS, one MSIV closes, probable reactor trip.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 120 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
64) ESFAS Actuation Circuit (AFAS-1, AFAS-2, or MSIS). (Cont.)	hh) Power return line circuit breaker fails closed.	Contact weld, mech. damage.	Loss of overcurrent protection for one leg of the actuation circuit.	Periodic breaker tests.	None.	None.	
65) Test Power Supply	a) High output voltage.	Internal failure.	Depends upon ability of components to sustain overvoltage.	Possible power supply indicator light inoperative.	None required.	Unable to test PPS.	No effect upon operation of PPS. Overvoltage condition may cause failure of affected bistable test coils when matrix hold push button is depressed during test.
		Mechanical damage.	Possibilities: 1. Matrix pushbutton system channel trip select, and RPS channel trip select switch fail closed or open. 2. Bistable test coils fail open or short. 3. Bistable test coil surge suppression diodes fail open or short.	Inability to conduct bistaable relay test.	None required.		
	b) Low or no output voltage.	Internal failure, mech. damage, input under-voltage, input CRT breaker open.	No test capability.	Test power supply and matrix relay hold indicator lights in-operative.	None required.	Unable to test PPS.	No effect upon operation of PPS.

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS
(Sheet 121 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
66) Matrix Hold Switch e.g., “AB” Matrix)	a) Open – Matrix relay circuit contacts.	Mech. failure, contact deterioration.	Unable to energize matrix relay test coils which inhibits matrix response when selected pari of contacts in “AB” logic matrix is actuated. Matrix will pass test signal as bonafide actuation signal (e.g., CSAS).	Matrix relay hold and drop-out indicator lights inoperative. Annunciation.	None required	Matrix Relay Hold Switch has a detent in the “hold” position, which allows detection of open contacts before switch is rotated to the “trip” position.	Test procedure requires matrix and channel switch at off position. The failure of these contact pairs can be deteced before channel is tested.
	b) Closed – Matrix relay circuit contacts	Mech. damage, welded contacts.	Matrix relay test coils remain energized, preventing reactor trip initiated by same matrix.	Matrix relay hold and drop-out indicator lights remain on.	Removal of test power.	Affected logic matrix cannot initiate trip when required during test.	Reactor trip logic becomes 2-out-of-2 during test period only. (4th input signal bypassed at bistable.)
	c) Open – Bistable relay circuit contacts.	Mech. failure, contact deterioration.	Unable to energize any system channel trip select switch or RPS channel trip select switch, bistable test relay coils.	Unable to release bistable relay. No trip indicator lights.	None required	None. Unable to conduct matrix logic test for “AB” matrix.	No affect on operation of PPS. Operator cannot test bistables, pair associated with matrix logic (e.g., “AB”).
	d) Closed – Bistable relay circuit contacts	Mech. damage, welded contacts	Bistable relay test coils connected to system channel trip select switch remains energzied during test.	Bistable relay trip indicator light is on	Removal of test power supply or positioning CRT switches to off.	Actuation signal is initiated when test switch is turned on.	First position of system channel trip select switch is RPS trip, and when Operator starts test sequence the reactor may trip.

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 122 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
67) System Channel Trip Select Switch	Intermit-tent contact (Open)	Mech. damage, contact deterioration.	Unable to energize bistable relay test coils associated with system channel trip select switch.	No bistable test light indication.	None required	Unable to test logic matrices for affected system channel trip.	
68) RPS Channel Trip Select Switch	Intermit-tent contact (Open)	Mech. damage, contact deterioration.	Unable to energize bistable relay test coils associated with test switch position.	No bistable test light at test switch position location.	None required	Unable to test logic matricees for affected bistable pair.	No affect on opera-tion of PPS.
69) Bi-stable relay test coil (e.g., A1-1)	a) Open	Overvoltage, mech. damage.	Unable to energize affected bistable test coil to initiate relay trip for the particular parameter under test.	Bistable test light stays off.	None required	Unable to test that portion of logic matrices completely for the parameter under test.	No effect on opera-tion of PPS.
	b) Short	Mech. damage.	Test power supply will be reduced to approx. zero.	Power supply indi-cator light inoper-ative.	None required	Unable to test logic matrices completely.	
		Deterioration of Insulation	Bistable relay test coil cannot be energized.	Bistable test light stays off.	None required		
70) Matrix Relay Trip Select Switch	Intermit-tent contact (Open) (e.g., po-sition 1).	Mech. damage, contact deterioration.	Matrix relay test coils for the affected position (e.g., "1" remain de-energized during test period.	Matrix relay hold indicator light inoperative Annunciation.	None required	Reactor trip could occur during bist-able relay trip test.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 123 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
71) Matrix Relay Test coil (e.g., 1AB-1)	a) Open	Overvoltage, mech. damage.	Unable to energize affected test coil to inhibit matrix relay trip.	Matrix relay hold indicator lights do not illuminate.	None required	Unable to conduct test of trip path (e.g., #1) for affected matrix logic (e.g., "AB").	No affect on operat-tion of PPS.
	b) Short	Deterioration of Insulation	Test power supply will be reduced to approx. zero.	Power supply and matrix hold indi-cator lights do not illuminate.	None required	Unable to conduct test of trip path (e.g., #1) for affected matrix logic (e.g., "AB").	No affect on opera-tion of PPS.
72) Matrix Relay Hold Indicators	Open	Overvoltage, mech. damage.	Test coil state cannot be visually determined.	Visual, periodic test.	None.	None.	No affect on opera-tion of PPS.
73) Matrix Relay Drop-Out Indicators	Open	Overvoltage mech. damage.	Matrix relay state cannot be determined.	Visual, periodic test.	None.	None.	No affect on opera-tion of PPS.
74) Matrix Test dc/dc Converter	a) Fails off.	Comp. failure, open circuit, fuse fails open.	Unable to provide dc power to one matrix test circuit. Unable to test one matrx (i.e., "AB").	Operator, when attempting matrix test.	None.	No impact on PPS operation.	
	b) Fails hi.	Comp. failure.	Possible damage to components on matrix test circuits, bistable test coils may fail open. Test switches may fail open. Unable to properly test one matrix.	Operator, when attempting matrix test.	None.	No impact on PPS operation.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 124 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
75) Channel A Test Switch	a) Fails open.	Mech. binding, contact deterioration.	Unable to test channel A related logic matrices or other channel A functions.	Operator, when attempting test.	None.	No impact on PPS operation.	
	b) Fails closed.	Mech. binding.	Unable to test any channel but channel A.	Operator, when attempting test on another channel.	None.	No impact on PPS operation.	
	c) Contacts to ch. A test enable relay fail open.	Contact corrosion, mech. binding.	Same as 74 a)	Same as 74 a)	Same as 74 a)	Same as 74 a)	
	d) Contacts to ch. A test enable relay fail closed.	Contact weld, mech. binding.	Ch. A test enable relay remains energized. Possible to test two ch's. at same time.	Ch. A test lamp stays on when switch is turned off.	Procedures preclude testing more than one ch. at a time.	None.	
	e) Contacts to Ch. B test switch fail open.	Contact corrosion, open lead, mech. damage.	Unable to provide power to Ch. B test switch, unable to test Ch. B, C, or D.	Operator, when trying to test Ch. B.	None.	None.	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 125 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
75) Channel A Test Switch (cont.)	f) Contacts to Ch. B test switch fail closed.	Contact weld, mech. damage.	Power still provided to Ch. B test switch when ch. A is in test. Possible to test two ch's. at same time.	None.	Procedures preclude testing two ch's. at same time.	None.	
	g) Contacts to test annunc. fail open	Contact deterioration, mech. damage, open lead.	Spurious "Test in Progress" alarms.	Annunciation.	None.	None.	
	h) Contacts to test annunc. fail closed.	Contact weld, mech. binding.	"Test in Progress" alarm not sound when Ch. A switch engaged.	Operator, when starting test.	Ch. A "Test in Progress" lamp comes on.	None.	
76) Ch. A Test Lamp	Fails off.	Burnt out, mech. damage.	Loss of visual indication when Ch. A is in Test.	Operator, when starting test.	Test annunc. not affected	None.	
77) Ch. A Test Relay	a) Fails open.	Overstress, open winding, mech. damage.	Relay contacts in matrix hold switch power lines will not close. Unable to test Ch. A.	Operator, when starting test	None.	None.	
	b) N.O. contacts in power circuit fail open.	Open lead, contact corrosion.	Same as 77 a)	Same as 77 a)	Same as 77 a)	Same as 77 a)	

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 126 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
77) Ch. A Test Relay	c) One N.O. contact in power circuit fails closed.	Contact weld, mech. binding	None.	None.	None.	None.	
78) PPS Calibration and Test Panel Trip Test Pushbutton (PB -) (e.g., Channel "A")	a) Open	Mech. damage, contact deterioration.	Unable to energize bistable relay trip test circuit and supply test signal to bistable selected for test.	No bistable trip indication.	None.	None.	No effect on operation of PPS. May not be able to test bistables in affected channel (e.g., Channel "A").
	b) Closed	Mech. damage welded contacts.	Bistable relay trip test circuit energized when test signal power supply is turned on.	Bistable in test indicator.	Rotating matrix hold switch to the "Hold" position and/or reducing signal level below trip level.	Half logic matrix trip could occur during testing.	Operator will be aware of problem as soon as test power supply is turned on and before test sequence starts.
79) Trip Test Circuit Relay (K-1, e.g., Channel A")	a) Open coil.	Overvoltage, mech. damage.	Unable to energize trip test circuit. The contacts which connect the bistable selected for test to the test signal will not be energized.	No trip signal indication.	None.	Selected bistable relays cannot be tested in affected channel (e.g., "A")	No effect on operation of PPS.

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 127 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
79) Trip Test Circuit Relay (K-1, e.g., Channel "A") (Cont.)	b) Shorted coil.	Deterioration of insulation, mech. damage.	Test power supply could be reduced to approx. zero.	Test power supply indicator light will extinguish. No signal reading on DVM.	None.	Selected bistable relays cannot be tested in affected channel (e.g., "A")	No effect on operation of PPS.
	c) Contact open.	Deterioration of contact, mech. damage.	Unable to energize trip circuit. Bistable selected for test cannot be connected to the test signal.	No trip signal indication.	None.	Selected bistable relays cannot be tested in affected channel (e.g., "A")	No effect on operation of PPS.
	d) Contact short.	Weld contact.	Trip test circuit remains energized.	Possible signal reading on DVM. Bistable trip indication.	Bistable select and meter input switch in off position.	Should test signal be inputted half logic matrix trip can occur during test only.	
80) NI Drawer Log Level Trip Test Switch (S2) (e.g., Channel "A")	a) Open contacts: "A"	Mech. damage, contact deterioration.	Unable to transmit test signal to next channel (e.g., "B") when next channel is selected for test.	No response of next channel during test. No bistable trip indication.	None. channels B, C, D	Unable to test tion of PPS. Nuclear Drawer.	No effect on opera-
	"B"		Unable to test channel "A" when conducting channel test. Relay AK 60 will not energize when test is run.	No response from channel under test. No bistable trip indication.	None.	Unable to test ch. A Nuclear Drawer.	No effect on operation of PPS.
	"D"		Unable to transmit selected test signal to log level trip circuitry.	No bistable trip indication.	None.	Unable to test ch. A Nuclear Drawer.	No effect on operation of PPS.

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 128 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
80) NI Drawer Log Level Trip Test Switch (S2) (e.g., Channel "A") (Cont.)	b) Closed contacts: "A"	Mech. damage, welded contacts.	Unable to disconnect nest channel, when ch. "A" is in test. Interchannel interlock during test is overridden.	Multichannel bi-stable tirp indicaiton.	None	Possible reactor trip during test.	Operator must deliberately depress ch. "A" test switch coincidence with other channel to initiate inadvertent trip.
	"B"		Unable to discard channel "A" from test during test program.	Multichannel bi-stable trip indication.	None.	Possible reactor trip during test.	
81) HI Drawer Test Relay (AK60) (e.g., "A")	a) Open coil.	Overvoltage, mech. damage.	Unable to energize relay contacts which transmit test signal to log level trip circuitry when channel is under test.	No bistabel trip indication.	None.	Unable to test channel A Nuclear Drawer.	No effect on opera-tion of PPS.
	b) Short coil.	Deterioration of insulation.	Test power supply may reduce to approximately zero.	No bistable trip light. Power supply test light not lit.	None.	Unable to test ch. A Nuclear Drawer.	No effect on opera-tion of PPS.
	c) Open contacts.	Deterioration of contact, mech. damage.	Unable to transmit selected test signal to log level trip circuitry.	No bistable trip indication.	None.	Unable to test ch. A Nuclear Drawer.	No effect on opera-tion of PPS.
	d) Short contacts.	Deterioration of contact, welded contact.	Interlock feature of relay AK60 is inhibited, cannot cause multi-test condition with failure in "A" channel.	Bench test.	Design of inhibit circuit would not allow trip condi-tion if failure occurs in "A" channel.	Possible to have a reactor trip during test.	Operator must deliberately actuate two channel test switches to obtain trip effect.

Table 7.2-4A

PLANT PROTECTIVE SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

(Sheet 129 of 129)

Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
82) Log Trip Level Adjust (R8)	Open or Intermit-tent.	Failed resis-tive element.	Operator will be unable to trim test signal level.	DVTM	None.	Unable to test ch. A, Nuclear Drawer.	
83) Initia-tion Reset Flasher Circuti	a) Fails on	Flasher failure, data coupler failure, dis-crete comp. failure.	Reset lamp will flash, giving spurious indication of a chan-nel trip for ESFAS or a TCB trip.	Visual indication.	None.	None.	
	b) Fails off.	Comp. failure.	Reset lamp will not flash when a channel trip is induced by test.	During test, flasher not flash but trip indi-cators come on.	Trip indic. for each channel of each PPS function.	None.	

7.2.2.3.2.5 Section 4.5, Channel Integrity. Type testing of components, separation of sensors and channels, and qualification of the cabling are utilized to ensure that the channels will maintain their functional capability required under applicable extremes of environment, power supplied, malfunction, and fault conditions. Loss of or damage to any one channel will not prevent the protective action of the RPS. Sensors are connected so that blockage or failure of any one connection does not prevent protective system action. The process transducers located in the containment building are specified and rated for the intended service. Components which must operate during or after a limiting fault are qualified for the most limiting environment for the period of time for which they must maintain their functional capability. Results of type tests are used to verify this. Separation requirements for the components of the RPS are discussed in subsection 7.2.3.

7.2.2.3.2.6 Section 4.6, Channel Independence. Each redundant channel is independent of the other redundant channels. The sensors are separated, cabling is routed separately and, in cabinets, each redundant channel is located in a separate compartment which provides thermal and mechanical barriers. This minimizes the possibility of a single event causing more than one channel's failure. The outputs from these redundant channels are isolated from each other so that a single failure does not cause impairment of the system function. The RSPT signals are sent to separate CEA calculators. To provide the required input to the CEAC, the signals utilized as inputs are sent through isolation amplifiers (see figure 7.2-0D).

Outputs from the redundant channels to non-safety related areas are isolated so that failure in the non-safety related area does not cause loss of the safety system function. Outputs from the

components of the RPS to the control boards are isolated if they go to non-1E portions of the board. The signals originating in the RPS which feed the plant monitoring system (PMS) are isolated to maintain their channel independence.

7.2.2.3.2.7 Manual Initiation

A manual trip is effected by depressing either of the pushbuttons in both trip legs on the main control board for the RPS or the pushbuttons on the RTSS. No single failure will prevent a manual trip.

7.2.2.3.2.8 Control and Protection System Inspection

A. Classification of Equipment

No portion of the RPS is used for both protective and control functions with the following exception: The RPS' DNBR, LPD, and high pressurizer pressure provide a CEA Withdrawal Prohibit (CWP) which is treated as an associated circuit, and is isolated in the CEDMCS auxiliary cabinets before going to the CEDMCS. As an associated circuit it meets the requirements of IEEE 279-1971.

B. Isolation Devices

Signals from the RPS are isolated such that a failure will not affect the protective action of the RPS. The CWP is isolated in the CEDMCS Auxiliary Cabinets to prevent a failure in the CEDMCS from propagating back into the RPS.

C. Single Random Failure

This criterion is not applicable. The CWP which is sent to the CEDMCS is only a permissive signal and does not

cause a control action which could require a protective action.

D. Multiple Failures Resulting From a Credible Single Event

This cannot exist since the CWP cannot initiate a control action, only permit it.

7.2.2.3.2.9 Derivation of System Input. Insofar as is practicable, system inputs are derived from signals that are direct measures of the desired variables. Variables that are measured directly include neutron flux, temperatures, and pressures. Level information is derived from appropriate differential pressure measurements. Flow information is derived from reactor coolant pump speed measurement and coolant temperature.

7.2.2.3.2.10 Capability for Sensor Checks. RPS sensors are checked by cross-channel comparison. Each channel has a known relationship with the other channels of the same parameter.

7.2.2.3.2.11 Capability for Test and Calibration. The RPS design complies with IEEE 338-1971, "Trial Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems" and Regulatory Guide 1.22, "Periodic Testing of Protection System Actuator Functions", as discussed in section 7.2.2.3.3.

7.2.2.3.2.12 Channel Bypass or Removal From Operation. Any one of the four protection channels in the RPS may be tested, calibrated, or repaired without impairing the systems' protective action capability. In the RPS, individual trip channels may be bypassed to create a two-out-of-three logic on the remaining channels which maintains the coincidence of two

required for trip. The single failure criterion is met during this condition. Testing of each of the two CEA position indication channels can be accomplished in a very brief time. The probability of failure of the other position indication system is acceptably low during such testing periods.

7.2.2.3.2.13 Operating Bypasses. Operating bypasses are provided as shown on Table 7.2-2. The operating bypasses are automatically removed when the permissive conditions are not met. The circuitry and devices which function to remove these inhibits are designed in accordance with IEEE 279-1971.

7.2.2.3.2.14 Indication of Bypasses. Indication of test or bypass conditions, or removal of any channel from service is given by annunciators. Operating bypasses that are automatically removed at fixed setpoints are alarmed and indicated.

7.2.2.3.2.15 Access to Means for Bypassing. Trip channel bypasses have access controlled by means of key locked doors. When the first parameter is bypassed there is an audible and visible alarm to indicate which channel is being bypassed. The specific parameter or parameters which are being bypassed are indicated by lights at the PPS cabinet and its remote operator's module.

The operating bypasses have audible and visible alarms. The operating bypasses have automatic features which provide a permissive range at which they can be actuated. Should the permissive range be exceeded, the bypass will be automatically removed.

7.2.2.3.2.16 Multiple Setpoints. Manual reduction of the setpoints for low pressurizer pressure and low steam generator pressure trips are used for the controlled reduction of pressurizer pressure and steam generator pressure as discussed in sections 7.2.1.1.1.6 and 7.2.1.1.1.8. The setpoint reductions are initiated by main control board pushbuttons for each channel, one pushbutton for the pressurizer pressure and one pushbutton for both steam generator pressures within the one channel. This method of setpoint reduction provides positive assurance that the setpoint is never decreased below the existing pressure by more than a predetermined amount.

The variable overpower trip setpoint tracks the actual reactor power from a minimum value to a high value or vice versa, if the power changes slowly enough. The variable overpower trip setpoint is designed with a maximum rate of decrease or increase. Should the actual power increase at too rapid a rate, it will catch up with the more slowly increasing setpoint and cause a trip.

The low reactor coolant flow trip setpoint automatically tracks below the input variables by a fixed margin for all decreasing inputs with a rate less than the rate limit. The setpoint decreases at a fixed rate for all decreasing input variable changes greater than the rate limit, except that there is a fixed minimum limit on the setpoint. Should the input variable decrease at too rapid a rate, it will catch up with the more slowly decreasing or limited setpoint and cause a trip. The setpoint automatically increases as the input variable increases independent of rate.

7.2.2.3.2.17 Completion of Protective Action Once it is Initiated. The system is designed to ensure that protective action (reactor trip) will go to completion once initiated.

Operator action is required to clear the trip and return to operation. Protective action is initiated when the reactor trip circuit breakers open. Protective action is completed when the CEAs arrive at their full-in position.

7.2.2.3.2.18 Access to Setpoint Adjustments, Calibration and Test Points. Keys or built-in features are provided to control setpoints, calibration, and test point adjustments. Access is indicated to the operator. The Applicant shall control access via key locks, administrative procedures, and other means to limit access.

7.2.2.3.2.19 Identification of Protective Action. Indication lights are provided for all protective actions, including identification of channel trips. The breaker status and current indication are available to the operator.

7.2.2.3.2.20 Information Readout. Means are provided to allow the operator to monitor all trip system inputs, outputs and calculations. The specific displays that are provided for continuous display are described in section 7.5.

7.2.2.3.2.21 System Repair. Identification of a defective input channel will be accomplished by observation of system status lights or by testing as described in section 7.2.1.1.9. Replacement or repair of components is accomplished with the affected input channel bypassed. The affected trip function then operates in a two-out-of-three trip logic while maintaining the coincidence of two required for trip.

7.2.2.3.2.22 Identification. All equipment, including panels, modules, and cables, associated with the trip system

will be marked in order to facilitate identification. Interconnecting cabling will be color coded as discussed in section 7.1.3.16. Interface requirements of section 7.2.3 ensure that equipment supplied by the Applicant meets this requirement.

7.2.2.3.3 Testing Criteria

Conformance to IEEE 338-1971 and Regulatory Guide 1.22 are discussed in paragraphs 7.1.2.7 and 7.1.2.15. Test intervals and their bases are included in the Technical Specifications and their Bases. A complete channel can be tested without causing a reactor trip and without affecting system operability. Overlap in the RPS channel tests is provided to assure that the entire channel is functional. The testing scheme is discussed in detail in paragraph 7.2.1.1.9. For the organization for testing and documentation, refer to chapter 13.

Since operation of the RPS will be infrequent, the system is periodically and routinely tested to verify its operability. A complete channel can be individually tested without initiating a reactor trip, without violating the single failure criterion, and without inhibiting the operation of the system. The system can be checked from the sensor signal through the circuit breakers of the RTSS. The RPS can be tested during reactor operation. The sensors can be checked by comparison with similar channels or channels that involve related information. Minimum frequencies for checks, calibration, and testing of the RPS instrumentation are given in the Technical Specifications. Overlap in the checking and testing is provided to assure that the entire channel is functional. The use of individual trip and ground detection lights, in conjunction with those provided at the supply bus, assures that possible grounds or shorts to another source of voltage will be detected.

7.2.2.4 Failure Modes and Effects Analysis (FMEA)

A FMEA for the RPS and ESFAS is provided in table 7.2-4A. The FMEA is for protection systems' sensors, and coincidence and actuating logics. The logic interface for the protection systems is shown in figure 7.2-11.

7.2.2.4.1 Potential Impacts of Control Systems Failures

Table 7.2-5 identifies the control systems that were considered in the evaluation of potential impacts on plant safety due to common power source or common sensor failures. As discussed below, the consequential malfunctioning of these systems due to a common power/sensor failure has less impact on plant safety than the bounding chapter 15 analyses.

Table 7.2-5
CONTROL SYSTEMS CONSIDERED TO HAVE POTENTIAL IMPACTS UPON PLANT SAFETY DUE TO COMMON POWER SOURCE OR COMMON SENSOR FAILURES

Control System	Acronym
Reactor regulating system	RRS
Control element drive mechanism control system	CEDMCS
Reactor power cutback system	RPCS
Boron control system	BCS
Steam bypass control system	SBCS
Turbine-generator control system	TGCS
Moisture separator reheat control system	MSRCS
Feedwater control system	FWCS
Main feedwater turbine pump control system	MFTPCS
Condenser level control system	CLCS
Pressurizer level control system	PLCS
Pressurizer pressure control system	PPCS

7.2.2.4.1.1 Power Source Failures. The power source failures which would affect more than one control system, and a brief description of the impact on each control system, are provided below. Except for the loss of offsite electrical power, which is specifically addressed by the chapter 15 analyses, no other power failures have been identified which would introduce additional control system malfunctions to those described. This is due to the degree of separation inherent in the electrical power distribution network and the availability of backup power sources within the network.

7.2.2.4.1.1.1 Impact Due to Loss of 120 V-ac Distribution Panel E-NNN-D11.

SBCS - The control system cannot generate quick open and modulate open signals to open the turbine bypass valves. In addition, control room indication of the automatic permissive signal will be lost.

RPCS - The control system will be unable to generate CEA drop demand and turbine runback signals.

PLCS - The letdown control valve closes and the
PPCS normally running and standby charging pumps will not operate. They can be started manually from BO3. With either HS-100 and/or HS-100-3 in "Y" position, the 1E and non-1E backup heaters and the proportional heaters will trip off.

CEDMCS - Loss of one of two redundant power sources to the interlock relays. Therefore, CEDMCS will not be impacted.

7.2.2.4.1.1.2 Impact Due to Loss of 120 V-ac Distribution Panel E-NNN-D12.

SBCS - Inability to generate an automatic motion inhibit (AMI) signal. In addition, the SBCS valves will fail closed and cannot be operated in manual due to a loss of logic power.

RRS - Inability to generate CEA motion demand signals. Loss of CEA motion demand indication in the control room

PPCS - The PPCS controller fails to zero causing the pressurizer spray valve to fail close. With

either HS-100 and/or HS-100-3 in "X" position, all 1E and non-1E backup heaters and proportional heaters will trip off. With both HS-100 and HS-100-3 in "Y" position, the proportional heaters will turn fully on with no controls, while the 1E and non-1E backup heaters will be fully on with control. PPCS pressure indication on recorder PR100 in the control room goes to 0 psia.

CLCS - Inability to generate condensate storage tank control valve opening signal. The valve will remain in its normally closed state.

CEDMCS - Loss of one of two redundant power sources to the interlock relays. Therefore, CEDMCS will not be impacted.

7.2.2.4.1.1.3 Impact Due to Loss of 125 V-dc Load Center E-NKN-M45.

SBCS - Inability to actuate turbine bypass valve quick open or permissive solenoids. Loss of quick open indication in the control room.

PPCS - All the non-Class 1E backup heaters will
PLCS remain at their previous (on or off) setting. The 1E backup heaters will trip off. Silicon controlled rectifiers of proportional heaters cannot be tripped.

CLCS - Inability to open condensate storage tank control valve due to solenoid deenergization.

MSRCS - Inability to isolate the extraction lines from the high- and low-pressure turbines to the feedwater heaters.

MFTPCS - Inability to automatically trip main feedwater pumps or use pump logic. Manual trip is still available.

Table 7.2-6 identifies the control systems that share a common sensor or instrument tap. No other common sensors/ taps have been identified.

Table 7.2-6
CONTROL SYSTEMS SHARING A COMMON SENSOR OR COMMON INSTRUMENT TAP

Sensor	Control Systems[a]
RCS cold leg temperature	CEDMCS, RRS, PLCS
Pressurizer level	PLCS, PPCS
Pressurizer pressure	PPCS, SBCS
Main steam flow	FWCS, SBCS
<u>Sensors Sharing Tap</u>	
Pressurizer level and	PPCS, PLCS
pressurizer pressure	PPCS, SBCS

a. Control system acronyms are defined in table 7.2-5.

7.2.2.4.1.2 <u>Evaluation of Common Failures</u>. As discussed below, the consequences of common power source, common sensor, and common instrument tap failures are bounded by chapter 15.

7.2.2.4.1.2.1 Evaluation of Common Power Source Failures.

A. Panel E-NNN-D11 Failure

The failure of distribution panel E-NNN-D11 will: 1. cause the PLCS and the PPCS to reduce letdown flow to 0 gpm, 2. stop flow from two of the three charging pumps, 3. may result in loss of control of primary system mass, and 4. may cause the 1E and non-1E pressurizer backup and proportional heaters to trip off on loss of pressurizer level control.

All charging pumps remain available if manually started, and the concurrent closing of the letdown control valves ensures primary system mass is controllable within the time frame before operator action. The loss of backup heaters is within the analysis, and they become available in any event upon switching control to the unaffected loop.

The SBCS and RPCS will be unable to automatically respond to any challenges on a failure of distribution panel E-NNN-D11.

This scenario is bounded by the CVCS Malfunction-Pressurizer Level Control System malfunction with loss of offsite power presented in subsection 15.5.2.

B. Panel E-NNN-D12 Failure

The loss of this panel will result in the loss of automatic pressurizer pressure control. However, if HS-100 and HS-100-3 are in the "Y" position, the 1E and non-1E backup heaters will be available. With either hand switch in the "X" position, backup heaters will trip off. Also, when HS-100 and HS-100-3 are in the "Y" position, proportional heaters will turn full on with no

control, and with either hand switch in the "X" position, the proportional heaters will trip off. The condenser hotwell level may decrease due to the inability to automatically control it. In addition, the RRS will behave as if it is in manual mode of operation. In addition, the SBCS valves will fail closed and cannot be operated due to a loss of logic power.

The loss of heaters with closure of spray valves is not a concern. Auxiliary spray remains available to control increases in RCS pressure and all heaters will be available if control is switched to the unaffected control loop. With HS-100 or HS-100-3 in the "Y" position, proportional heaters will turn full on with no automatic control, but are still able to be deenergized from the control room. A total loss of feedwater flow (LOFW) due to the condenser hotwell level decrease may occur. However, the LOFW event presented in subsection 15.2.7 assumed that the PPCS, SBCS, and RRS are in the manual mode of operation, unable to automatically respond to challenges. Therefore, the LOFW event bounds the panel failure event.

C. Load Center E-NKN-M45 Failure

Failure of this load center effectively results in the CLCS and MFTPCS being placed in the manual mode of operation. The SBCS valves will fail closed and cannot be operated in manual due to a loss of logic power. In addition, pressurizer pressure control will be hindered, due to lack of control of all the non-Class 1E heaters. If RCS pressure drifts below the backup heater actuation setpoint the class 1E-powered backup heaters cannot be energized due to the presence of a trip signal. The

loss of backup heaters is within the bounds of chapter 15 analyses and is listed in the analyzed failures of table 15.0-0. This panel failure is not of concern with respect to peak RCS pressure, fuel performance, or radiological releases.

7.2.2.4.1.2.2 Evaluation of Common Sensor Failures.

A. RCS Cold Leg Temperature Sensor (CEDMCS, RRS, PLCS)

The PLCS receives an average reactor coolant temperature (T_{avg}) signal from the RRS based on either loop or both loop cold leg and hot leg temperatures (T_{cold} and T_{hot}) measurements. The measured T_{avg} determines the programmed pressurizer level. If a T_{cold} channel fails such that T_{avg} (indicated) does not agree with T_{avg} (actual) then the PLCS will adjust charging and letdown to change the pressurizer level to the new programmed level within the normal operating band.

The RRS and CEDMCS have several features which protect against inadvertent CEA motion following failure of T_{cold} channel. These include input channel deviation alarm, automatic motion inhibit, and automatic withdrawal prohibit. In addition, the consequences of inadvertent CEA insertion (withdrawal) resulting from indicated T_{cold} failing higher (lower) than actual T_{cold} in combination with pressurizer level variations within the control band are bound by the CEA withdrawal event described in subsection 15.4.2.

B. Pressurizer Level Sensor (PPCS, PLCS)

In response to a high indicated pressurizer level (L_{pzr}) the PLCS will decrease charging flow and increase letdown flow resulting in a slow decrease in RCS inventory and pressurizer level. If the indicated L_{pzr} is high enough, a high level alarm will be generated, the normally running charging pump will be secured, and an insufficient charging alarm will be generated. In addition, if the pressurizer level error L_{pzr} (indicated) - L_{pzr} (programmed) is large enough, the PLCS will signal the PPCS to energize pressurizer heaters. The high indicated L_{pzr} will disable one of two channels of heater cutout. Normally, however, one channel is sufficient to activate the heater interlock and generate a low L_{pzr} alarm. Also, under the conditions of maximum letdown flow and minimum charging flow, it would require in excess of 30 minutes for pressurizer level to drop from the full power programmed level to the level corresponding to the top of the heaters. This time interval would allow the operator to arrest the level transient prior to heater uncovery.

The thermal-hydraulic effects of the slow decrease in RCS inventory are bounded by the double-ended break of a letdown line as described in subsection 15.6.2.

If the indicated L_{pzr} fails low, the PLCS would increase charging and decrease letdown. This would result in a slow increase in RCS inventory. If the indicated L_{pzr} fails low enough, a low level alarm would be activated, as would the heater interlock in the PPCS, thus preventing pressurizer heater operation. The effects of

this transient are bounded by the PLCS malfunction event described in subsection 15.5.2.

C. Pressurizer Pressure Sensor (PPCS, SBCS)

Failure of a pressurizer pressure (P_{pzr}) sensor cannot result in inadvertent operation of the SBCS. The SBCS has two independent circuits (main circuit and permissive circuit) both of which must be activated in order to generate either a turbine bypass valve (TBV) modulation signal or quick open signal. Failure of a P_{pzr} sensor, therefore, can only affect the PPCS. Failures in single control systems have already been considered in the chapter 15 safety evaluation.

D. Main Steam Flow Sensor (FWCS, SBCS)

Similarly, failure of a main steam flow (Fms) sensor cannot result in inadvertent operation of the SBCS. Failure of an Fms sensor, therefore, can only affect the FWCS. Failures in single control systems have been considered in the chapter 15 safety evaluation.

7.2.2.4.1.2.3 Evaluation of Common Instrument Tap Failure: Tap for Pressurizer Pressure and Level Sensors (PPCS, PLCS, SBCS). As previously indicated, the SBCS utilizes two independent circuits; therefore, the SBCS will not open bypass valve due to the instrument tap failure. The response to the tap failure is limited to various combinations of PPCS and PLCS malfunctions which can cause slow pressurizer pressure and level increases or decreases. The evaluation is similar to that provided above for the pressurizer level sensor failure. The potential consequences of this instrument tap failure are bounded by the PLCS malfunction event and the double-ended break of a letdown line

event described in subsection 15.5.2 and subsection 15.6.2, respectively.

7.2.3 REACTOR PROTECTIVE SYSTEM INTERFACE REQUIREMENTS

The interface requirements discussed below are specific to the RPS. General interface requirements are discussed in subsection 7.1.3.

7.2.3.1 Power

Vital instrument power interface requirements are discussed in subsection 8.3.1. Power failure evaluations for the control systems are also discussed in paragraph 7.2.2.4.1.

7.2.3.2 Protection From Natural Phenomena

Refer to subsection 3.1.2. Class 1E equipment shall be located so as to be provided with the maximum protection from natural phenomena which are specific to the PVNGS site.

7.2.3.3 Protection From Pipe Failure

Refer to paragraph 7.1.3.3.

7.2.3.4 Missiles

Refer to paragraph 7.1.3.4.

7.2.3.5 Separation

Refer to paragraph 7.1.3.5.

Preamplifiers for the fission chambers shall be mounted outside the biological shield, with two inside the containment building and two outside the containment building in the auxiliary

building. The preamplifiers and cabling shall be provided with physical and electrical separation.

7.2.3.6 Independence

Refer to paragraph 7.1.3.6.

7.2.3.7 Thermal Limitations

Refer to paragraph 7.1.3.7.

7.2.3.8 Monitoring

Refer to paragraph 7.1.3.8.

7.2.3.9 Operational/Controls

Administrative procedures or other suitable means shall be used to control changes to CPC constants, adjustments to variable setpoints, and the bypassing of channels which could affect operation.

7.2.3.10 Inspection and Testing

Refer to paragraph 7.1.3.10.

7.2.3.11 Chemistry/Sampling

Refer to paragraph 7.1.3.11.

7.2.3.12 Materials

Not applicable.

7.2.3.13 System Component Arrangement

Refer to paragraph 7.1.3.13. The separation, independence, etc., criteria specified in paragraph 7.2.2.3.2 shall be adhered to.

7.2.3.14 Radiological Waste

Refer to paragraph 7.1.3.14.

7.2.3.15 Overpressure Protection

Refer to paragraph 7.1.3.15.

7.2.3.16 Related Services

Refer to paragraph 7.1.3.16.

7.2.3.17 Environmental

Refer to section 3.11 and CENPD-255.[3]

7.2.3.18 Mechanical Interaction

Refer to section 3.10 and CENPD-182.[4]

7.2.4 REACTOR PROTECTIVE SYSTEM INTERFACE EVALUATION

The interface requirements listed in CESSAR Section 7.2.3 are met by the PVNGS design as discussed in paragraphs 7.2.4.1 through 7.2.4.18.

7.2.4.1 Power

Vital instrument power interface evaluations are discussed in subsection 8.3.5.

7.2.4.2 Protection From Natural Phenomena

Refer to subsection 3.1.2. Class 1E equipment has been located so as to be provided with the maximum protection from natural phenomena which are specific to the PVNGS site.

7.2.4.3 Protection From Pipe Failure

Refer to paragraph 7.1.4.3.

7.2.4.4 Missiles

Refer to paragraph 7.1.4.4.

7.2.4.5 Separation

Refer to paragraph 7.1.4.5.

Preamplifiers for the fission chambers have been mounted outside the biological shield, with two inside the containment building and two outside the containment building in the auxiliary building. The preamplifiers and cabling are provided with physical and electrical separation.

7.2.4.6 Independence

Refer to paragraph 7.1.4.6.

7.2.4.7 Thermal Limitations

Refer to paragraph 7.1.4.7.

7.2.4.8 Monitoring

Refer to paragraph 7.1.4.8.

7.2.4.9 Operational/Controls

Administrative procedures or other suitable means are used to control changes to CPC constants, adjustments to variable setpoints, and the bypassing of channels which could affect operation.

7.2.4.10 Inspection and Testing

Refer to paragraph 7.1.4.10.

7.2.4.11 Chemistry/Sampling

Refer to paragraph 7.1.4.11.

7.2.4.12 Materials

Not applicable.

7.2.4.13 System Component Arrangement

Refer to paragraph 7.1.4.13. The separation, independence, and other criteria specified in paragraph 7.2.2.3.2 have been adhered to in the PVNGS design.

7.2.4.14 Radiological Waste

Refer to paragraph 7.1.4.14.

7.2.4.15 Overpressure Protection

Refer to paragraph 7.1.4.15.

7.2.4.16 Related Services

Refer to paragraph 7.1.4.16.

7.2.4.17 Environmental

Refer to section 3.11.

7.2.4.18 Mechanical Interaction

Refer to section 3.10.

7.2.5 SUPPLEMENTARY PROTECTION SYSTEM

The supplementary protection system (SPS) augments reactor protection by utilizing a separate and diverse trip logic from the reactor protective system (RPS) for initiation of reactor trip to satisy the requirments of 10CFR50.62 for Anticipated Transient Without Scram (ATWS). The addition of the SPS provides a simple, reliable, yet diverse mechanism which is designed to increase the reliability of initiating reactor trip. The SPS will initiate a reactor trip when pressurizer pressure exceeds a predetermined value shown on Table 7.2-1. The SPS logic is shown in Figure 7.2-5.

The SPS design uses a selective two-out-of-four logic to interrupt the power supplied to the CEDM's and thereby causes the CEA's to drop into the core by gravity. The Technical Specifications provide the required actions if a channel is removed for testing or maintenance. The SPS is independent and separate from all control systems.

The SPS is designed to conform to the same criteria as the PPS. Each SPS channel is called the Supplementary Protection Logic Assembly (SPLA).

Four identical SPLA's are provided for each SPS system. Each SPLA is electrically and physically separated from each other.

7.2.5.1 Functional Description of the SPLA

Each SPLA contains an input circuit, comparator circuit, output circuit, test circuit, annunciator circuit, trip circuit breaker (TCB) control and indication circuit, and instrumentation power supplies. See figure 7.2-5.

7.2.5.1.1 Input Circuit

The input circuit receives a 4 to 20 milliampere (ma) "Process Current" signal from its pressurizer pressure transmitter. This signal is converted within the circuit to a (+) 1 to (+) 5 VDC signal via a precision dropping resistor. This "Converted Process" signal is then transmitted via conditioning circuits to the comparator circuit (as the "Process Voltage" signal) for further processing and to the digital voltmeter for displays. A second dropping resistor in the input circuit provides a (+) 1 to (+) 5 VDC "Process Indication" signal to a remote display indicator.

The input circuit also receives a 0 to (+) 5 VDC "Test" signal from the test circuit. The "Test" signal, when applied, adds a 0 to (+) 5 VDC signal to the "Converted Process" signal.

The input circuit contains conditioning circuits for overvoltage protection and noise suppression. The purpose of the overvoltage protection circuit is to protect the equipment downstream of the input circuit from damage due to a high voltage fault on the transmitter field cabling. The purpose of the noise suppression circuit is to filter out unwanted noise picked up during "Process Current" signal transmission.

7.2.5.1.2 Comparator Circuit

The comparator circuit continuously compares the 1 to 5 VDC "Process Voltage" signal to a fixed trip setpoint signal. When

the "Process Voltage" signal passes through the trip setpoint level, the comparator circuit recognizes this and generates a trip output signal.

The trip signal derived from the comparator circuitry must be present for a specified period of time before it is allowed to pass through to the output circuit. When the trip signal has been present for the required period of time (adjustable from 10-150 msec), the time delay circuit recognizes this and provides the trip signal to the initiation relay drive circuit.

Upon receipt of a trip signal, the initiation relay drive circuit de-energizes the output circuit's initiation relay. When a trip signal is not present, the drive circuit maintains the initiation relay energized. A front panel tripped indicator is provided and receives its logic from the initiation relay drive circuit.

7.2.5.1.3 Output Circuit

The output circuit provides the necessary contact switching to affect the opening of a remotely located trip circuit breaker (TCB) and M-G set load output contactors.

The output circuit receives a trip signal from the comparator circuit's initiation relay drive circuit. This signal controls the application and removal of initiation relay input power. During normal operation, the initiation relay is energized and its contacts maintain the TCB and M-G set load output contactors closed. For a trip condition, the initiation relay is deenergized and its contacts change state to affect opening of the TCB and M-G set load output contactors.

The initiation relay provides two contacts which interface with the TCB undervoltage and shunt trip coils. This contact interface controls TCB opening. A third contact provided by the

initiation relay interfaces via an isolation relay with each of the M-G set load output contactors. These contact interfaces provide for opening the M-G set load output contactors upon a selective two-out-of-four SPLA channel trips. An open signal by this contact also indirectly results in a signal to the remote annunciator. The annunciator serves to inform the operator of a SPLA "trip" condition.

7.2.5.1.4 Trip Circuit Breaker (TCB) Control and Indication Circuit

This circuit provides a signal to control the closing of a remotely located trip circuit breaker. In addition, this circuit receives "OPEN" and "CLOSED" position indication signals from this same trip circuit breaker. These position indication signals are used to light indicators mounted on the front panel.

The TCB closing signal is a contact closure provided by a momentary switch. This switch is located on the front panel. Closing the switch contacts completes the TCB closing coil control circuit. Completing the TCB closing coil control circuit affects closure of the breaker.

This circuit receives two contact input position indication signals from TCB auxiliary switches. These indication signals are used to energize "OPEN" and "CLOSED" indicators on the front panel. An indicator is energized when a contact closure input is received from its respective auxiliary switch. Power to the indicators and auxiliary switch is supplied by the SPLA.

7.2.5.1.5 Test Circuit

The purpose of the test circuit is to provide the capability for testing the SPLA. Testing of the SPLA is performed to verify its proper operation.

Testing of the SPLA is accomplished by applying a 0 to 5 vdc "Test" signal to the input circuit. The "Test" signal is applied in such a way that it is added to the 1 to 5 vdc "Converted Process" signal. The "Test" signal is manually adjusted until the "Process Voltage" signal reaches the trip setpoint value. Upon reaching the trip setpoint value, the trip circuit breaker associated with the SPLA opens.

The test circuit is comprised of a voltage reference, a voltage adjust circuit, a test enable switch, a digital voltmeter (DVM), and a DVM input select switch. The voltage adjust circuit, in conjunction with the voltage reference, generates the "Test" signal. The test enable switch applies the "Test" signal to the Input Circuit. The DVM indicates the value of the "Converted Process," "Test" signal, calibration voltages, setpoint value, or external input.

7.2.5.1.6 Annunciator Circuit

The annunciator circuit provides the circuitry necessary for interfacing SPLA status signals with remote annunciators.

Three status signals are generated within the SPLA. Only two of the status signals are supplied to the annunciator circuit.

The annunciator circuit receives one status signal from the SPLA door alarm switch and one status signal from the test enable switch.

The third status signal is generated indirectly by the output circuit and is termed the "Trip" status signal. This status signal directly interfaces with its remote annunciator and therefore is not supplied by the annunciator circuit.

7.2.5.1.7 Instrumentation Power Supplies

The power supplies contain the equipment required for powering all SPLA equipment including the pressurizer pressure transmitter.

7.2.5.1.8 SPLA Test Points

The front panel has the following test jacks available for external measurement: 1) voltage reference, 2) time delay input, 3) time delay output, and 4) test jacks for each of the supply voltages provided. Also available for measurement via test jacks in the SPLA are the following: 1) the setpoint voltage value, and 2) the process input voltage value.

7.2.5.2 Supplementary Protection System (SPS) Diversity to the Reactor Protective System (RPS)

The supplementary protection logic assembly (SPLA) of the SPS is designed to be a diverse design with respect to the RPS. The following design differences between the systems outline these qualities:

Each of the SPLA circuits is described below:

A. Manufacturing Diversity - Different vendors were used which produced a (1) different design,
(2) different system production techniques, and
(3) different testing procedures.

B. System Part Diversity - The vendor used different Components than the RPS, and MIL spec parts whenever possible.

C. Cabinet Diversity - The SPLA uses one cabinet per channel (4 channel system).

D. Electrical Diversity - Each SPLA channel is electrically isolated and separated from the others. There is no crosschannel communication between SPLA channels.

E. Initiation Logic Diversity - The RPS and SPLA utilize different designs for initiation logic.

F. Sensor Diversity – The sensors (pressure transmitters) used in the RPS and SPLA are produced by the same manufacturer. Both systems monitor the pressurizer pressure via a common tap per channel in the pressurizer. The instruments have separate shut-off valves and a common root valve per channel.

   10CFR50.62 requires that each pressurized water reactor must have equipment from sensor output to final actuation device that is diverse from the reactor trip system. Based on this requirement, lack of diversity between the sensors is satisfactory, since the equipment from the sensor output to the actuation devices in the SPLA is diverse from that of the RPS.

G. Power Supply Diversity - The SPLA uses a custom power supply while the RPS uses a commonly available "off-the-shelf" power supply.

H. Human Factors Diversity - 1) smaller SPLA cabinet, 2) each SPLA channel is in its own cabinet, 3) front panel controls are in different locations and are much fewer in the SPLA, 4) adjustment controls for the test and setpoint voltages are different, and 5) the SPLA front panel has fewer test points than the RPS system.

7.2.6 REFERENCES

1. "Functional Design Requirements for a Core Protection Calculator," CEN-305-P, Rev. 01-P, Combustion Engineering, Inc., May, 1986.

2. "Review of Reactor Shutdown System (PPS Design) for Common Mode Susceptibility," CENPD-148, Combustion Engineering, Inc.

3. "Qualification of Combustion Engineering Class 1E Instrumentation," CENPD-255-P-A, Combustion Engineering, Inc., June, 1983.

4. "Seismic Qualification of Instrumentation and Electrical Equipment," CENPD-182, Combustion Engineering, Inc.

5. "Description of the C-E Nuclear Steam Supply System Quality Assurance Program," CENPD-210A, Combustion Engineering, Inc.

6. "Functional Design Requirement for a CEAC," CEN-304-P, Rev. 01-P, Combustion Engineering, Inc., May, 1986.

7. "CPC/CEAC System Phase 1 Software Verification Test Report," CEN-217 (V)-P, Combustion Engineering, Inc.

8. "CPC/CEAC System Phase 2 Software Verification Test Report," CEN-219 (V)-P, Rev. 01, Combustion Engineering, Inc., June, 1983.

9. "PVNGS-1 Cycle 1 CPC and CEAC Data Base Document, "CEN-226 (V)-P, Combustion Engineering, Inc., January, 1983.

10. "CPC Protection Algorithm Software Change Procedure," CEN-39 (A)-P, Rev. 03-P, Combustion Engineering, Inc., January, 1986.

11. "CPC/CEAC Software Modifications for the CPC Improvement Program Reload Data Block," CEN-330-P-A, Combustion Engineering, Inc., October, 1987.

12. "Reload Data Block Constant Installation Guidelines," CEN-323-P-A, Combustion Engineering, Inc., September, 1986.

13. "Modified Statistical Combination of Uncertainties," CEN-356(V)-P-A, Rev. 01-P-A, Combustion Engineering, Inc., May, 1988.

14. "Reload Analysis Methodology for the Palo Verde Nuclear Generating Station," Rev. 00-P, acceptance letter from Charles M. Trammell, Office of Nuclear Reactor Regulation to William F. Conway, Executive Vice President, Nuclear, PVNGS, dated June 14, 1993. Docket Nos. 50-528, 50-529, 50-530 (TAC Nos. M85153, M85154, and M85155).

15. "CPC/CEAC Software Modification for the CPC Improvement Program," CEN-308-P-A, Combustion Engineering, Inc., April, 1986.

16. "CPC and Methodology Changes for the CPC Improvement Program," CEN-310-P-A, Combustion Engineering, Inc., April, 1986.

17. "Module Test Report for the Common Q Core Protection Calculator," 00000-ICE-37366, Westinghouse Electric Company LLC.

18. "Input Sweep Test Report for the Common Q Core Protection Calculator," 00000-ICE-37373, Westinghouse Electric Company LLC.

19. "Software Design Description for the Common Q Core Protection Calculator System Database and Utility Functions," 00000-ICE-30140, Westinghouse Electric Company LLC.

20. Software Program Manual for Common Q Systems, CE-CES-195 Rev. 01.

21. "Reload Data Block Constant Installation Guidelines," Westinghouse Electric Company LLC.

22. "Common Qualified Platform Topical Report," CENPD-396-P, Rev. 01, May 2000.

23. "System Requirements Specification for the Palo Verde Nuclear Generating Station Core Protection Calculator System," 00000-ICE-30158, Rev. 10.

24. "Failure Modes and Effects Analysis for the Core Protection Calculator System," 00000-ICE-3338.

7.3 ENGINEERED SAFETY FEATURE SYSTEMS

7.3.1 Description

BOP ESFAS. The following actuation signals are generated by the BOP Engineered Safety Feature Actuation System (ESFAS) when the monitored variables reach levels that require protective action:

- Fuel building essential ventilation actuation signal (FBEVAS)
- Containment purge isolation actuation signal (CPIAS)
- Control room essential filtration actuation signal (CREFAS)
- Control room ventilation isolation actuation signal (CRVIAS)

These actuation signals automatically actuate the following ESF systems:

- Fuel building essential ventilation system
- Containment purge isolation system
- Control room essential ventilation system

The control room essential ventilation system is also actuated by a manually initiated ESF signal, the control room ventilation isolation actuation signal (CRVIAS).

The manually actuated ESF systems are the containment combustible gas control system and the CRVIAS.

The BOP ESFAS system hardware and software also provides load sequencing and logic for the diesel generator start signal (DGSS), loss of power (LOP), and load shed (LS) functions. These functions are described in section 8.3.

The additional automatically actuated ESF systems use one-out-of-two input signal logic. The actuation circuits for all one-out-of-two actuation systems are described in paragraph 7.3.1.1. The actuated devices for these systems are described in paragraph 7.3.1.1.10.

NSSS ESFAS. The safety-related instrumentation and controls of the Engineered Safety Features Systems (ESF Systems) are those of the NSSS and BOP Engineered Safety Features Actuation System (ESFAS) which consists of the electrical and mechanical devices and circuitry, from sensors to actuation device input terminals, involved in generating those signals that actuate the required ESF Systems.

The NSSS ESFAS includes sensors to monitor selected generating station variables. The following actuation signals use a two-out-of-four logic system and are generated by the NSSS ESFAS when the monitored variable reaches the levels that are indicative of conditions which require protective action:

A. Containment Isolation Actuation Signal (CIAS)

B. Containment Spray Actuation Signal (CSAS)

C. Main Steam Isolation Signal (MSIS)

D. Safety Injection Actuation Signal (SIAS)

E. Recirculation Actuation Signal (RAS)

F. Auxiliary Feedwater Actuation Signal (AFAS)

The ESF System actuation device circuitry receives actuation signals from the ESFAS or the operator. The ESFAS signals actuate the ESF Systems equipment. The control circuitry for the components provides sequencing necessary to provide proper ESF Systems operation.

The actuation circuitry for all ESF Systems is essentially identical, except for the sensed parameter and its setpoint. Therefore, the actuation circuits for all ESF Systems are described in one section. The specific instrumentation and controls associated with each system are described separately in section 7.3.1.1.10.

7.3.1.1 NSSS Engineered Safety Features Actuation System (ESFAS)

The ESFAS system consists of the sensors, bistables, initiation logic, and actuation logic that monitor selected plant parameters and provide an actuation signal to each individual actuated component in the ESF system if the plant parameters reach preselected setpoints. There is one actuation system for each of the ESF systems. Each actuation system is identical except that specific inputs and logic (and blocks, where provided) vary from system to system and the actuated devices are different.

Within the PPS, the matrix logic is like that shown in figures 7.3-9a, 7.3-9b and 7.3-9c. This provides the AB, AC, AD, BC, BD, and CD combinations which create the coincidence of two logic. Each of these matrices operates an initiation circuit which opens the initiation relays. The outputs of the initiation relays go to the ESFAS auxiliary relay cabinets where they create the selective two-out-of-four logics, i.e., 1A/2A, 1A/4A, 3A/2A, or 3A/4A for the given train shown in figures 7.3-8a and 7.3-8b.

Only those ESF systems that, when actuated, do not cause a plant condition requiring protective action, or disturb reactor operations, are controlled by the one-out-of-two BOP ESFAS.

The one-out-of-two BOP ESFAS logic is contained in the separate enclosures isolated from the two-out-of-four ESFAS and reactor protective system (RPS) logic. The overall logic is shown in figures 7.3-1, 7.3-2, 7.3-7a through 7.3-7d.

7.3.1.1.1 Engineered Safety Features Actuation System Measurement Channels

BOP ESFAS. Process measurement channels are used to perform the following functions:

- Continuously monitor each selected generating station variable
- Provide indication of operational availability of each sensor to the operator.
- Transmit signals to bistables within the BOP ESFAS initiating logic.

Protective parameters are measured with two independent process measurement channels.

A measurement channel consists of instrument sensing lines, sensor, transmitter, power supplies, isolation device, indicator, and interconnecting wiring. For the radiation measurement channels description see section 11.5.

Each measurement channel is separated from other like measurement channels to provide physical and electrical isolation of the signals to the ESFAS initiating logic. The isolation devices will prevent a high voltage fault to either the A or B sensor outputs from disabling both of the one-out-of-two actuation logic devices. Signal isolation is provided for computer inputs and annunciation. Each BOP ESFAS channel

is supplied by two sources from a separate 120V vital ac distribution bus and its associated 125 VDC vital ESFAS.

Display information, which provides the operator with the operational availability of each measurement channel, is described and tabulated in section 7.5.

Testing of the BOP and NSSS ESFAS measurement channels is described in paragraph 7.3.1.1.8.

NSSS ESFAS. Process measurement channels, similar to those described in section 7.2.1.1.2.1 are utilized to perform continuous monitoring of each selected generating station variable, provide indication of operational availability of each sensor to the operator, and transmit analog signals to bistables within the ESFAS initiating logic. All protective parameters are measured with four independent process instrument channels.

A typical measurement channel is shown in Figure 7.2-0A. It consists of a sensor/transmitter, current loop resistors, converter/power supply, indicators, outputs for the Plant Monitoring System, and interconnecting wiring.

Each measurement channel is separated from other like measurement channels to provide physical and electrical separation of the signals to the ESFAS coincidence logic. Associated circuits are handled in accordance with the interface requirements of Section 7.3.3. Cabling is separated within the cabinets and signals to non-IE indicators are isolated. Each channel is supplied from a separate 120 volt vital AC distribution bus.

7.3.1.1.2 Logic

7.3.1.1.2.1 Engineered Safety Features Actuation System Bistable and Initiating Logic.

BOP ESFAS. The Balance of Plant Engineered Safety Features Actuation System (BOP ESFAS) provides initiation signals to components requiring automatic or manual actuation. These signals are generated whenever monitored variables reach levels that require protective action.

The BOP ESFAS uses two measurement channels for the one-out-of-two logic and four measurement channels for the two-out-of-four logic as inputs to the initiation signal.

The ESFAS initiating logic consists of bistables, bistable output relays, trip output signals, indicating lights, and interconnecting wiring. For the radiation measurement signal initiation logic description, see section 11.5.

Signals from the protective measurement channels are sent to comparator circuits (bistables) where the input signals are compared to predetermined setpoints. Whenever a channel parameter reaches the predetermined setpoint, the channel bistable deenergizes an output relay. When the coincidence logic is satisfied an actuation signal is provided to the appropriate components. Each bistable relay (i.e., each channel) is supplied from a separate 120V vital ac distribution bus. The bistable setpoints are adjustable from the front of the cabinet. Access is limited, however, by means of a key-operated switch. Bistable setpoints are capable of being read out on a display located on the cabinet.

NSSS ESFAS Bistable and Coincidence Logic. The ESFAS Coincidence Logic compares the analog signal from the sensors

with predetermined initiation setpoints in the bistable circuit (see Figure 7.2-6). If the signal exceeds the setpoint the channel bistable output relay deenergizes three trip relays.

The setpoint values are controlled administratively. The setpoints are adjusted at the PPS cabinet. Access to the adjustments is limited by means of a key-operated cover with an annunciator indicating cabinet access. The bistable setpoints are capable of being read out on a meter located on the PPS cabinet. Some setpoints are externally variable to avoid inadvertent initiation during normal operations such as startup, shutdown, and cooldown, and evolutions such as low power testing. The steam generator and pressurizer pressure setpoints can be decreased by pushbuttons and will automatically increase as pressure increases.

The output of the trip relays is formed into the six logic matrices (refer to Figure 7.3-10). The four channels, A, B, C, and D, form into AB, AC, AD, BC, BD, and CD to create all possible coincidence of two combinations. Each logic matrix actuates four matrix relays. Six matrix relays (one from each of the six logic matrices) have their output contacts joined in series to form an initiation circuit. Four initiation circuits are used to form four channels 1, 2, 3, and 4. The output of the initiation circuits are initiation relays, A and B which send signals to the actuation logics in their respective ESF train cabinet.

Besides the automatic actuation of the initiation circuit by the matrix relays, the circuit can be tripped by remote manual switches. All ESFAS can be manually initiated by the operator in accordance with procedures provided by the Applicant. Following initiation, each ESFAS, except AFAS, must be manually

reset to restore the initiation logic to the non-actuated state.

7.3.1.1.2.2 Actuating Logic.

NSSS ESFAS. The ESFAS actuation logic is physically located in two ESFAS auxiliary relay cabinets. One cabinet contains the logic for ESF train A equipment the other cabinet contains the logic for ESF train B.

The four initiation circuits in the PPS actuate a selective two-out-of-four logic in the ESFAS auxiliary relay cabinets. In an actuation matrix (see figures 7.3-8a and 7.3-8b), each signal also deenergizes the lockout relays when the selective two-out-of-four logic actuates the train's group actuation relays. The lockout relays ensure that the signal is not automatically reset once it has been initiated.

Receipt of two selective ESFAS initiation channel signals will deenergize the ESF subgroup relays, which generate the actuation channel signals. This is done independently in both ESFAS auxiliary relay cabinets, generating both train A and train B signals. The group relays are used to actuate the individual ESF components which should be actuated to mitigate the consequences of the occurrence which caused the ESFAS.

BOP ESFAS. The BOP ESFAS actuating logic, however performs the following functions:

- Receive ESFAS signals from the ESFAS initiating logic
- Form one-out-of-two coincidence of like ESFAS signals
- Provide a means for remote manual initiation
- Provide status information to the operator

The BOP ESFAS actuating logic is physically located in two cabinets. One cabinet contains the logic for ESF load group 1 equipment, while the other cabinet contains the logic for ESF load group 2 equipment. These two cabinets are in addition to those ESFAS auxiliary relay cabinets described above.

Actuation signals are generated following receipt of the proper combination of initiation signals, resulting in de-energizing the appropriate ESF group relay. This actuates all components required by the particular ESF system. The final actuation devices are the sub-group relays and the actuated equipment consists of valves, air handling units (AHU), air filtration units (AFU), large electrical loads as listed in section 8.3, and diesel generators.

Each actuation channel is supplied from a separate 120 V-ac distribution bus and a separate Class 1E 125 V-dc distribution bus.

Figure 7.3-3 is a simplified functional diagram of a typical one-out-of-two ESFAS logic.

Testing of logic and trip is described in paragraph 7.3.1.1.8.

7.3.1.1.2.2.1 Group Actuation.

BOP ESFAS. Components in each ESF system are actuated by actuation relays. The actuation relay contacts are in the power control circuit for the actuated components of each ESF system.

The logic described in paragraph 7.3.1.1.2 causes deenergization of the actuation relay whenever the BOP ESFAS logic is satisfied. The circuit is shown in figure 7.3-3 for a

typical ESFAS. Deenergization of the actuation relay actuates the ESF system components.

NSSS ESFAS. The group relays actuate all of the ESF System components required by the ESFAS. These generally consist of either solenoid operated valves, motor operated valves, or motors of pumps. Figures 7.3-11a, b and c show how each of these components can be operated by the ESFAS signals.

In Figure 7.3-11a, a solenoid operated valve can be operated by a relay contact. If the valve control switch contact is closed and the ESFAS contact is closed the solenoid valve will open. In the circuit shown in Figure 7.3-11a, the ESFAS signal opens the contact which closes the valve.

The valve motor circuit of Figure 7.3-11b shows the valve closed. When an ESFAS actuating signal is reset, the ESFAS contact in the closing circuit is closed and the contact in the opening circuit is open, thereby restoring normal operation. Upon receipt of an ESFAS signal the valve which is normally closed would open in the following sequence. The Mc_b contact and the Ts and Ls Contacts in the Mo circuit are closed because the valve is fully closed. The ESFAS contact would close causing the Mo coil to pick up which shuts the Mo contactors driving open the valve.

The pump motor control circuit shown in Figure 7.3-11c shows that the ESFAS actuation signal will take out the time overcurrent contacts (numbered 51) but leaves in the instantaneous overcurrent contacts (numbered 50). With the circuit breaker lockout relay (numbered 86) contact closed and the ESFAS contact closed the pump motor breakers will close if

the control switch is in the automatic position. Thus an ESFAS actuation signal will cause the pump motor to start.

If components have to be sequenced the sequencing will be done in the components' control circuit. Sequencing is described in section 7.3.1.1.7.

7.3.1.1.3 Bypasses

7.3.1.1.3.1 Channel Bypasses.

BOP ESFAS. Trip channel bypasses are provided in the one-out-of-two ESFAS as shown in table 7.3-1. The trip channel bypass is similar to the RPS trip channel bypass (Section 7.2.1.1.5) and is employed to remove a trip channel from service for maintenance.

The trip logic is thus converted to a single active channel for the trip type bypassed. Other type trips that do not have bypasses in either of their two channels remain in a one-out-of-two logic. The bypass time interval for maintenance is so short that the probability of failure of the remaining channel is acceptably low during maintenance bypass periods. The bypass is manually initiated and manually removed. An electrical interlock allows only one channel for any one type trip to be bypassed at one time. Bypasses are annunciated visually and audibly to the operator.

In some cases, bypass of more than one parameter within a channel may be required in the event of an equipment failure. Specific requirements are provided in the Technical Specifications.

NSSS ESFAS. For two-out-of-four logic bypass capability, refer to section 7.2.1.1.5.

Bypasses are provided, in the PPS, as shown in table 7.3-1c. The trip channel bypass is identical to the RPS trip channel bypass (section 7.2.1.1.5) and is employed for maintenance and testing of channel.

7.3.1.1.3.2 Operating Bypasses

BOP ESFAS. For the one-out-of-two logic, there are no operating bypasses.

NSSS ESFAS. The low pressurizer pressure bypass as shown in figure 7.3-7a, is provided to allow plant depressurization without initiating protective actions when not desired. The bypass may be initiated manually in each protective channel. However, the bypass cannot be initiated if pressurizer pressure is greater than that shown in table 7.3-1c. Once the bypass is initiated, it is automatically removed when the pressurizer pressure increases above the value shown in the table.

Table 7.3-1

ONE-OUT-OF-TWO ESFAS BYPASSES

Title	Function	Initiated By	Removed By
Trip Channel Bypass[a]	Disables any given trip channel	Manually by controlled access switch	Same switch

a. Interlocks allow only one channel for any type trip to be bypassed at one time.

7.3.1.1.3.3 DAFAS Bypasses. The key-lock bypasses shown in table 7.3-1A are provided in the auxiliary relay cabinets for maintenance and test purposes. The bypasses function to block actuation of the DAFAS-1 or DAFAS-2 initiation relays in trip legs 1-3 and 2-4. There are no interlocks associated with the bypass functions other than a separate key-lock switch for each

bypass. There are two key-lock bypasses for DAFAS-1 and DAFAS-2, one each for trip legs 1-3 and 2-4 in the auxiliary relay cabinet bay 5 and bay 8. The bypasses are indicated locally on the ARC status indicator assemblies, located within the ARC. The bypasses are also installed and removed by the MMI (man machine interface) automated test programs when each DAFAS PLC is placed in test by control of a key-locked test switch and the appropriate password protected automated test program command is given.

Table 7.3-1A

DAFAS BYPASSES

TITLE	FUNCTION	INITIATED BY	REMOVED BY
DADAS-1 OR DAFAS-2	DISABLE TRIP LEG 1 - 3 OR 2 - 4	DAFAS-1 OR DAFAS-2 BYPASS SWITCH IN BAY 5 OR BAY 8 OF ARC OR MMI AUTO TEST	BYPASS SWITCH OR TEST SWITCH

7.3.1.1.4 Interlocks

BOP ESFAS. The one-out-of-two ESFAS interlocks prevent the operator from bypassing more than one trip channel for one type trip at a time. Different type trips may be bypassed simultaneously, either in the same channel or in different channels.

NSSS ESFAS. The ESFAS interlocks, located in the PPS, prevent the operator from bypassing more than one trip channel of a trip parameter at a time. Different trip parameters may be

bypassed simultaneously, either in the same channel or in different channels. This function is shown in figure 7.2-9.

During system testing an electrical interlock prevents more than one set of four matrix relays from being held at one time. The same circuit will allow only one process measurement loop signal to be perturbed at a time for testing. The matrix relay hold and loop perturbation switches are interlocked so that only one or the other may be used at any one time.

7.3.1.1.5 Redundancy

BOP ESFAS. Redundant features of the one-out-of-two ESFAS include:

A. Two independent channels, from process sensor/transmitter through and including bistable output relays, are provided.

B. Two trip paths are present for each actuation signal.

C. Each actuation signal actuates two output trains so that redundant system components may be actuated from separate trains.

D. Power for the system is provided from two separate buses. Power for control and operation of redundant actuated components comes from separate buses. Load group 1 components and systems are energized only by the load group 1 bus and load group 2 components and systems are energized only by the load group 2 bus.

E. Power to each BOP ESFAS division is provided from a vital AC source (PN) and a vital DC source (PK) to redundant power supplies that are auctioneered.

The result of the redundant features is a system that meets the single failure criterion and can be tested during plant operation.

NSSS ESFAS. There are many redundant features within the ESFAS. There are four independent channels for each parameter from process sensor through and including the initiation circuits located in four PPS bays. There are six logic matrices, to actuate the initiation circuits, each of which has two power supplies for the four logic relays of each matrix.

In the ESFAS Auxiliary Relay Cabinets the selective two-out-of-four logic matrix has two power supplies per leg. Each Auxiliary Relay Cabinet controls one ESF System train and there are two totally redundant Auxiliary Relay Cabinets used to operate two totally redundant ESF trains.

Overall, the entire ESFAS receives vital AC power from four separate buses and the power for control and operation of separate trains comes from separate buses.

The result is a system which meets the single failure criterion, can be tested during operation and shifted to two-out-of-three logic, when a channel is removed for testing or maintenance without affecting system availability.

7.3.1.1.6 Diversity

BOP ESFAS. The one-out-of-two ESFAS is designed to eliminate credible dual channel failures originating from a common cause. The failure modes of redundant channels and the conditions of operation that are common to them are analyzed to ensure reasonable assurance that:

A. The monitored variables provide adequate information during the accidents.
B. The equipment can perform as required.
C. The interactions of protective actions, control actions, and the environmental changes that cause, or are caused by, the design basis events do not prevent the mitigation of the consequences of the event.
D. The system cannot be made inoperable by the inadvertent actions of operating and maintenance personnel.

In addition, the design is not encumbered with additional components or channels without reasonable assurance that such additions are beneficial.

NSSS ESFAS. The system is designed to eliminate credible multiple channel failures originating from a common cause. The failure modes of redundant channels and the conditions of operation that are common to them are analyzed to assure that a predictable common failure mode does not exist.

The design provides reasonable assurance that the protective system cannot be made inoperable by the inadvertent actions of operating or maintenance personnel. The design is not encumbered with additional channels or components without reasonable assurance that such additions are beneficial.

7.3.1.1.7 Sequencing

There is no sequencing for any ESF equipment other than that necessary for ESF bus loading. The automatic load sequencer is discussed in paragraph 8.3.1.1.3.

7.3.1.1.8 Testing

Provisions are made to permit periodic testing of the BOP and NSSS ESFAS. These tests cover the trip actions from sensor input through the protection system and the actuation devices. The system test does not interfere with the protective function of the system. The testing system meets the criteria of IEEE Standard 338-1971 and Regulatory Guide 1.22. Testing criteria is presented in Section 7.3.2.3.3. For the testing of the radiation measurement channels, see section 11.5 and the ODCM.

For the two-out-of-four ESFAS overlap between individual tests exist so that the entire ESFAS can be tested.

Testing of the BOP ESFAS load sequencer functions is discussed in section 8.3.1.1.3.10.1.

Since actuation of the ESF systems controlled by the BOP ESFAS does not disturb normal plant operating conditions, the one-out-of-two ESFAS is tested by complete actuation. Frequency of accomplishing the tests is listed in the Technical Specifications.

7.3.1.1.8.1 Sensor Checks. During reactor operation, the measurement channels providing an input to the BOP and NSSS ESFAS are checked by comparing the outputs of similar channels, and by cross-checking with related measurements.

During extended shutdown periods or refueling, these measurement channels are checked and calibrated against known standards.

7.3.1.1.8.2 Trip Bistable Test.

BOP ESFAS. Testing of the system is accomplished by manually varying the input signal to the trip setpoint level on one bistable at a time and observing the trip action.

When the bistable of a protective channel is in a tripped condition, the following conditions should exist:

- The bistable output relay is deenergized.
- The group relay in each actuation channel is deenergized.
- The ESF components are in the ESFAS actuation position.
- Actuation is annunciated on the control room annunciator panel.

Proper operation may be verified by the following:

- Checking the position of each ESF component
- Checking the actuation annunciation
- Checking the ESF component status indication

The test is repeated for the other bistable.

NSSS ESFAS. Testing of a trip bistable, located in the PPS, is accomplished by manually varying a simulated process input signal locally on the PPS Bistable Control Panel. This signal is increased, or decreased, until the trip setpoint is reached and the trip action is observed (See Figure 7.2-6).

Varying the simulated input signal is accomplished by means of a trip test circuit which consists of a digital voltmeter and a test circuit which can change the magnitude of the signal supplied by the measurement channel. The trip test circuit is

electrically interlocked so that it can be used in only one channel at a time (See Figure 7.2-9). A switch selects the measurement channel and a pushbutton applies the test signal. The digital voltmeter indicates the test signal value. The test circuit permits various rates of change of signal input to be used. Trip action of each of the bistable trip relays is indicated by individual lights on the front of the cabinet (See Figure 7.2-7), indicating that the contacts of these relays, which are located in the coincidence of two logic matrices, operated as required for a trip condition.

The variable setpoint test is accomplished by manually varying a simulated process input signal. Upon decreasing this input, the setpoint is verified to remain constant and the trip setpoint is within specified tolerances. By manually decreasing this input, and then depressing the setpoint reset button, the setpoint incremental change can be tested and verified. The tracking ability of the circuit can be tested by manually increasing the test input and observing that the setpoint tracks.

When one of the bistables of a protective channel is in the tripped condition, a channel trip exists and is annunciated on the control room annunciator panel. In this condition, an actuation would take place upon receipt of a trip signal in one of the other three like channels. The trip channel under test is, therefore, bypassed for this test converting the ESFAS to a two-out-of-three logic which is still a coincidence of two for the particular trip parameter.

7.3.1.1.8.3 Logic Matrix Tests. This PPS logic test is carried out to verify proper operation of the six coincidence

logic matrices, located in the PPS, any one of which will initiate a system actuation for any possible coincidence of two trip condition from the signal inputs of each measurement channel. The test circuits are shown in Figures 7.2-8 and 7.2-7.

The system is interlocked so that only one logic matrix set (i.e., all AB or all AC, etc.) can be held at a time as discussed in CESSAR Section 7.3.1.1.4. Rotating the switch to the "Hold" position will apply a test voltage to the test system hold coils of the double coil matrix relays in their energized position. The deactuation of the trip relay contacts in the matrix ladder being tested caused deenergization of the primary matrix relay coils (see Figure 7.2-7).

The logic matrix to be tested is selected using the System Channel Trip Select Switch. By holding the matrix hold switch in the "trip" position and rotating the System Channel Trip Select Switch through each of its positions, the trip relays in the logic matrix will be deenergized. The System Channel Trip Select Switch applies a test voltage of the opposite polarity to the bistable trip relay test coils so that the magnetic flux generated by these coils cancels that of the primary coil causing the relays to release.

Trip action can be observed by illumination of the trip relay indication located on the front panel and by loss of voltage to the four matrix relays, which is indicated by loss of illumination of the indicator lights connected across each matrix relay coil. During the test the matrix relay hold lights will remain on, indicating that a test voltage has been applied to the holding coils of the matrix relays of the logic matrix under test.

This test is repeated for each actuation signal, by use of the System Channel Trip Select Switch, and for all six logic matrices. This test will verify that the logic matrix relays will deenergize if the logic matrix continuity is interrupted.

7.3.1.1.8.4 Initiation Channel Tests. Each initiation circuit, in the PPS, is tested individually by rotating a matrix hold switch to the "trip" position (holding four matrix relays), selecting any trip position on the System Trip Select Switch and selecting a matrix relay on the Matrix Relay Trip Select Switch (see Figure 7.2-11). This causes the appropriate initiation circuit to deenergize. Proper operation of both initiation relay coils and contacts is verified by monitoring the current through the appropriate leg of the actuation logics selected two-out-of-four circuit.

The matrix Relay Trip Select Switch is turned to the next position, re-energizing the test matrix relay and permitting the reset of the initiation circuit relays. The whole sequence is repeated for the remaining three initiation circuits from the selected matrix. The entire sequence is repeated for the remaining five matrices. Upon completion of testing, all six matrices, all 24 matrix relay contacts, and all eight initiation relays have been tested.

In addition, the remote manual switches for the initiation circuits can be tested. The indication of proper manual initiation will be the same as for automatic initiation. Only one switch is used at a time.

7.3.1.1.8.5 ESFAS Actuation Logic Test. This test verifies the proper operation of the ESFAS actuating logic circuits

(refer to Figure 7.3-8a). The selective two-out-of-four logic circuit, located in the ESFAS Auxiliary Relay Cabinets, of each ESFAS train is tested in a manner identical to the RPS trip breaker system. (See Section 7.2.1.1.9.5). One current leg of the selective two-out-of-four logic matrix is interrupted by opening one of the current legs contacts and loss of current in that current leg is verified. Each contact in both current legs is checked in this manner.

The lockout contacts are checked via the group relay test system as described below and the PPS initiation relay contacts are checked as described in the preceding section.

7.3.1.1.8.6 ESFAS Actuating Device Test. Proper operation of the ESFAS group relays, in the ESFAS Auxiliary Relay Cabinets, is verified by deenergizing the group relays one at a time via a test relay contact (See Figure 7.3-8a) and noting proper operation of all actuated components in that group. The relay will automatically reenergize and return its components to the pretest condition when the test keylock pushbutton is removed from the test position.

The design of the test system is such that only one group relay may be deenergized at a time. The test switch must be positioned to the group to be tested; selection of more than one group is impossible. The test circuit is electrically locked out upon actuation of a particular test group and another test group cannot be actuated for one minute after selecting another switch position. This time delay is a "stop and think" feature to assist the operator in conducting tests.

Since this test causes the ESF components to actuate by interrupting the normal safety signal current leg to individual

group relays, the propagation of a valid trip during test is not impeded and the system will proceed to full actuation by interrupting the current leg to all group relays.

7.3.1.1.8.7 Bypass Tests. System bypasses in the PPS, as itemized in Table 7.2-2, are tested on a channel basis using internally generated test signals. This testing includes both manual initiation and automatic removal features.

7.3.1.1.8.8 Response Time Tests. The design of the ESFAS is such that connections may be made for any of a variety of methods. The hardware design includes test connections on instrument lines for pressure and differential pressure transmitters, and test points wired out to convenient test jacks or terminal strips.

Response time testing required at refueling intervals are given in the Technical Specifications. These tests include the sensors for each ESFAS channel and are based on the criteria defined in paragraph 7.3.2.3.3. The ESF response time limits are identified in table 7.3-1B.

7.3.1.1.9 Vital Instrument Power Supply

The vital instrument power supply for the ESFAS is described in chapter 8.

7.3.1.1.10 Actuated Systems

The ESF Systems are maintained in a standby mode during normal operations. Actuating signals, generated by the ESFAS are provided to assure that the ESF Systems provide the required protective actions. The following descriptions of the

instrumentation and controls of the ESF Systems is applicable to each ESF System. Table 7.3-2 presents the Design Basis Events (DBE) which require specific ESF System action. Table 7.3-3 presents the monitored variables required for ESF System actuation. The variables and their ranges are shown on Table 7.3-3a.

7.3.1.1.10.1 Containment Isolation System. Section 6.2.4 contains a description of the Containment Isolation System. The actuation system is composed of redundant trains A and B. The instrumentation and controls of the two trains are physically and electrically separate and independent as discussed above such that the loss of one train will not impair the safety function.

The Containment Isolation System instrumentation and controls are designed for operation during all phases of plant operation as required by the Technical Specifications.

The Containment Isolation System is automatically actuated by a CIAS from the ESFAS.

A. See table 6.2.4-2 for a list of devices actuated on a containment isolation actuation signal (CIAS).

B. Figure 7.3-7B, ESFAS signal logic (CIAS).

C. Figure 6.2.4-1, containment penetration valve arrangements.

D. Figure 7.2-2, instrumentation location layout drawing for CIAS input services.

Removal of the containment isolation system from service is controlled by plant procedures.

Table 7.3-1B
ENGINEERED SAFETY FEATURES RESPONSE TIMES

(Sheet 1 of 3)

INITIATING SIGNAL AND FUNCTION	RESPONSE TIME IN SECONDS
1. Manual	
a. SIAS	
Safety Injection (ECCS)	Not Applicable
Containment Isolation	Not Applicable
Containment Purge Valve Isolation	Not Applicable
b. CSAS	
Containment Spray	Not Applicable
c. CIAS	
Containment Isolation	Not Applicable
d. MSIS	
Main Steam Isolation	Not Applicable
e. RAS	
Containment Sump Recirculation	Not Applicable
f. AFAS	
Auxiliary Feedwater Pumps	Not Applicable
2. Pressurizer Pressure - Low	
a. Safety Injection (HPSI)	≤ 30[a]/30[b]
b. Safety Injection (LPSI)	≤ 30[a]/30[b]
c. Containment Isolation	
1. CIAS actuated mini-purge valves	≤ 10.6[a]/10.6[b]
2. Radwaste Drain System Inside CIV RDA-UV023	≤ 59[a]/59[b]
3. Other CIAS actuated valves	≤ 31[a]/31[b]
d. Safety Injection (Control Room Normal HVAC Isolation Dampers[e])	≤ 51[a]/51[b]
3. Containment Pressure - High	
a. Safety Injection (HPSI)	≤ 30[a]/30[b]
b. Safety Injection (LPSI)	≤ 30[a]/30[b]

Table 7.3-1B

ENGINEERED SAFETY FEATURES RESPONSE TIMES

(Sheet 2 of 3)

INITIATING SIGNAL AND FUNCTION	RESPONSE TIME IN SECONDS
c. Containment Isolation	
1. CIAS actuated mini-purge valves	≤ 10.6[a]/10.6[b]
2. Radwaste Drain System Inside CIV RDA-UV023	≤ 59[a]/59[b]
3. Other CIAS actuated valves	≤ 31[a]/31[b]
d. Safety Injection (Control Room Normal HVAC Isolation Dampers[e])	≤ 51[a]/51[b]
e. Main Steam Isolation	
1. MSIS actuated MSIV's	≤ 5.6[a]/5.6[b]
2. MSIS actuated MFIV's[c]	≤ 10.6[a]/10.6[b]
f. Containment Spray Pump	≤ 33[a]/23[b]
4. Containment Pressure - High-High	
a. Containment Spray	≤ 33[a]/23[b]
5. Steam Generator Pressure – Low	
a. Main Steam Isolation	
1. MSIS actuated MSIV's	≤ 5.6[a]/5.6[b]
2. MSIS actuated MFIV's[c]	≤ 10.6[a]/10.6[b]
6. Refueling Water Tank – Low	
a. Containment Sump Recirculation	≤ 45[a]/45[b]
7. Steam Generator Level – Low	
a. Auxiliary Feedwater (Motor Drive)	≤ 46[a]/23[b]
b. Auxiliary Feedwater (Turbine Drive)	≤ 46[a]/46[b]
8. Steam Generator Level – High	
a. Main Steam Isolation	
1. MSIS actuated MSIV's	≤ 5.6[a][f]/5.6[b][f]
2. MSIS actuated MFIV's(c)	≤ 10.6[a][f]/10.6[b][f]

Table 7.3-1B

ENGINEERED SAFETY FEATURES RESPONSE TIMES

(Sheet 3 of 3)

INITIATING SIGNAL AND FUNCTION	RESPONSE TIME IN SECONDS
9. Steam Generator ΔP-High-Coincident with Steam Generator Level Low	
a. Auxiliary Feedwater Isolation From the Ruptured Steam Generator	≤ 16[a]/16[b]
10. Control Room Essential Filtration Actuation	≤ 50[a][d]/50[b][d]
a. Control Room Normal HVAC Isolation Dampers	
11. 4.16 kV Emergency Bus Degraded Voltage LOP	≤ 35.0
12. 4.16 kV Emergency Bus Loss of Voltage LOP	≤ 2.4

TABLE NOTATIONS

a. Diesel generator starting and sequence loading delays included. Response time limit includes movement of valves and attainment of pump or blower discharge pressure.

b. Diesel generator starting delays not included. Offsite power available. Response time limit includes movement of valves and attainment of pump or blower discharge pressure.

c. MFIV valves tested at simulated operating conditions; valves tested at static flow conditions to ≤ 8.6[a]/8.6[b] seconds.

d. Radiation detectors are exempt from response time testing. The response time of the radiation signal portion of the channel shall be measured from the detector output or from the input of first electronic component in channel to closure of dampers M-HJA-M01, M-HA-M52, M-HJB-M01 and M-HJB-M55.

e. Dampers M-HJA-M01, M-HJA-M52, M-HJB-M01, and M-HJB-M55.

f. For Mode 3 operation, the Palo Verde Safety Analyses do not credit Main Steam Isolation due to a Steam Generator Level - High initiating signal. A 15 second response time was selected to comply with Palo Verde Technical Specification Surveillance Requirement 3.3.5.4 and Table 3.3.5-1.

TABLE 7.3-1C

NSSS ESFAS BYPASSES

Title	Function	Initiated By	Removed By	Notes
Trip Channel Bypass	Disables any given trip channel	Manually by controlled access switch	Same switch	Interlocks allow one channel for any type trip to be bypassed at one time.
Pressurizer Pressure Bypass	Disables low pressurizer pressure portion of SIAS/CIAS*	Manual switch (1 per channel) If pressure is < 400 psia	Automatic if pressurizer pressure is ≥ 500 psia	

* SIAS/CIAS actuation due to high containment pressure not affected.

Table 7.3-2

DESIGN BASIS EVENTS REQUIRING ESF SYSTEM ACTION (Sheet 1 of 2)

Design Basis Events / Systems	Containment Isolation System	Containment Spray System	Main Steam Isolation System	Safety Injection System	Auxiliary Feedwater System [f]	Fuel Building Essential Ventilation System	Containment Purge Isolation System	Control Room essential Ventation System	Containment Combustible Gas Control System
Loss of reactor coolant -- large break	*	*		*		* [e]	* [c]	*	* [b]
Loss of reactor coolant -- small break. [a]	*	*		*	*	* [e]	* [c]	*	* [b]
Steam generator tube rupture			* [b]	*	*				
Steam line break (inside containment)	*	*	*	*	*				
Steam line break (outside containment) [d]			*	*	*				

a. Includes CEA ejection and pressurizer safety valve opening

b. Manual actuation

c. Actuated by initiation of CPIAS or CIAS

d. Includes opening of secondary safety valve

e. On SIAS the fuel building essential ventilation system starts and is aligned to exhaust from the auxiliary building

f. Design basis event not defined for an ATWS event

Table 7.3-2

DESIGN BASIS EVENTS REQUIRING ESF SYSTEM ACTION (Sheet 2 of 2)

Design Basis Events / Systems	Containment Isolation System	Containment Spray System	Main Steam Isolation System	Safety Injection System	Auxiliary Feedwater System	Fuel Building Essential Ventilation System	Containment Purge Isolation System	Control Room Essential Ventilation System	Containment Combustible Gas Control System
Fuel handling accident - - containment building							*	*	
Fuel handling accident - - spent fuel pool						*		*	
Feedwater line break (inside containment)	*	*	*	*					
Fire / smoke - plant vicinity								* (b)	
Letdown line Break (15.6.2)								* (b)	

Table 7.3-3

MONITORED VARIABLES FOR ESF SYSTEM PROTECTIVE ACTION (Sheet 1 of 2)

Variable / Systems	Containment Isolation System	Containment Spray System	Main Steam Isolation System	Safety Injection System	Auxiliary Feedwater System [f]	Fuel Building Essential Ventilation System	Containment Purge Isolation System	Control Room Essential Ventilation System	Containment Combustible Gas Control System
Pressurizer pressure	*			*		* [e]	* [b]	* [c]	
Containment pressure	*	*	*	*		* [e]	* [b]	* [c]	
Steam generator pressure			*		*				
Refueling water tank level		*		*					
Steam generator level			*		* [f]				

a. Manual actuation post-LOCA

b. Actuated by initiation of CRVIAS or CIAS

c. Actuated by initiation of CREFAS or SIAS

d. Manual actuation - detectors are nonsafety-related

e. Actuated by initiation of SIAS, system aligned to exhaust from the auxiliary building

f. Steam generator level is also used to initiate an ATWS DAFAS actuation if diverse scram system is present and normal ESFAS has not initiated AFAS or MSIS.

Table 7.3-3

MONITORED VARIABLES FOR ESF SYSTEM
PROTECTIVE ACTION (Sheet 2 of 2)

Variable / Systems	Containment Isolation System	Containment Spray System	Main Steam Isolation System	Safety Injection System	Auxiliary Feedwater System	Fuel Building Essential Ventilation System	Containment Purge Isolation System	Control Room Essential Ventilation System	Containment Combustible Gas Control System
Containment airborne activity							*	*	
Fuel handling airborne activity						*		*	
Control room ventilation intake activity								*	
Control room ventilation intake smoke								*(d)	
Containment hydrogen									*

Table 7.3-3a

ENGINEERED SAFETY FEATURES

ACTUATION SYSTEM PLANT VARIABLE RANGES

Monitored Variable	Minimum	Typical Full Power	Maximum
Pressurizer Pressure	0 psia	2250 psia	3000 psia
Containment Pressure	-4 psig	0 psig	20 psig
Steam Generator Pressure	0 psia	1039 psia	1524 psia
Refueling Water Tank Level	0	70-95%	100%
Steam Generator Level	0%	82%	100%

7.3.1.1.10.2 Containment Spray System. Refer to Section 6 for a description of the containment spray system, and:

A. Table 6.2.4-2 for a list of devices actuated on a containment spray actuation signal (CSAS) and recirculation actuation signal (RAS).

B. Table 7.3-4 for additional CSAS actuated devices.

C. Table 7.3-5 for additional RAS actuated devices.

D. Figure 7.3-7b, ESFAS signal logic (CSAS and RAS).

E. P&I diagram 01, 02, 03-M-SIP-001,-002 and -003(safety injection system)

F. Figures 7.2-2 and 7.2-4, instrumentation location layout drawing for CSAS and RAS input devices.

G. Subsection 6.5.2 for a discussion of iodine removal capabilities of the CSS.

Table 7.3-4
CONTAINMENT SPRAY ACTUATION SIGNAL
ACTUATED DEVICES LIST

P&ID	Description	Function
01, 02, 03-M-DGP-001	Diesel Generator System	Refer to Paragraph 7.4.1.1.1
01, 02, 03-M-SIP-001, -002 and -003	Containment spray pumps and pump room cooling unit (2)	Start

Table 7.3-5

RECIRCULATION ACTUATION SIGNAL

ACTUATED DEVICES LIST

P&ID	Description	Function
01, 02, 03-M-SIP-001, -002 and -003	Low pressure safety injection pumps (2)	Stop
01, 02, 03-M-SIP-001, -002 and -003	LPSI pump miniflow valves (2)	Close
01, 02, 03-M-SIP-001, -002 and -003	HPSI pump miniflow valves (2)	Close
01, 02, 03-M-SIP-001, -002 and -003	Containment spray miniflow valves (2)	Close
01, 02, 03-M-SIP-001, -002 and -003	Combined SI miniflow return to RWT valves (2)	Close

Removal of the containment spray system from service is controlled by plant procedures.

7.3.1.1.10.3 IODINE REMOVAL SYSTEM(Abandoned in Place)

7.3.1.1.10.4 Main Steam Isolation System. Refer to Section 10.3, "Main Steam Supply System," for a description of the Main Steam Isolation System. Refer to Section 10.4.7, "Condensate and Feedwater System," for a description of the Main Feedwater Isolation System. Refer to Section 10.4.8, "Steam Generator Blowdown System," for a description of the Blowdown Isolation System. Interface requirements for the Main Steam Isolation System are provided in Section 5.1.4.

The actuation system is composed of redundant trains A and B. The instrumentation and controls of the train A valve actuators are physically and electrically separate and independent of the instrumentation and control of the train B valve actuators. The separation and independence are such that a failure of one train will not impair the protective action.

The Main Steam Isolation Valves (MSIV), Main Feedwater Isolation Valves (MFIV) and the isolation valves for the blowdown lines are actuated by an MSIS.

These valves effectively isolate the steam generators from the rest of the main steam and feed systems.

A variable steam generator pressure setpoint is implemented to allow controlled pressure reductions, such as shutdown depressurization, without initiating an MSIS. The pressure setpoint will track the pressure up until it reaches its normal setpoint value. Also, refer to figures and tables listed below:

A. Table 6.2.4-2 for a list of devices actuated on a main steam isolation signal (MSIS)

B. Figure 7.3-7c, ESFAS signal logic (MSIS)

C. P&I diagram 01, 02, 03-M-SGP-002 and -001 (main steam system)

D. Figures 7.2-2 and 7.2-3, instrumentation location layout drawing for MSIS input devices

7.3.1.1.10.5 Safety Injection System. Refer to Section 6.3, "Emergency Core Cooling System," for a description of the Safety Injection System (SIS). The SIS is actuated by an SIAS. Interface requirements for the Safety Injection System are provided in Section 6.3.1.3.

The actuation system is composed of redundant trains A and B. The instrumentation and controls of train A are physically and electrically separate and independent of instrumentation and controls in train B. Since each train is a 100% capacity

system the SIS can sustain the loss of an entire train and still provide its required protective action. The SIS instrumentation and controls are designed to operate under all plant conditions. The low pressurizer pressure setpoint can be decreased as described in section 7.2.1.1.1.6 to avoid inadvertent operation during startup and shutdown. As pressurizer pressure increases, the setpoint will follow up to its normal value. Also refer to figures and tables listed below:

A. Table 6.2.4-2 for a list of devices actuated on a safety injection actuation signal (SIAS)

B. Table 7.3-6 for additional SIAS actuated devices

C. Figure 7.3-7a, ESFAS signal logic (SIAS)

D. P&I diagram 01, 02, 03-M-SIP-001, -002 and -003 (safety injection system)

E. Figures 7.2-1 and 7.2-2, instrumentation location layout drawing for SIAS input devices

In addition, the procedure for removing the safety injection system from service is controlled by plant procedures.

7.3.1.1.10.6 Recirculation Actuation. An RAS is generated when the level in the RWT falls below a predetermined level. When an RAS is received the LPSI pumps are stopped and the HPSI and CSS pumps shift suction to the containment recirculation sump. Refer to Section 7.3.1.1.10.2 for references applicable to the recirculation actuation signal.

In addition, removing a RAS from the LPSI pumps to allow them to be used for the shutdown cooling system is controlled by plant procedures.

7.3.1.1.10.7 Auxiliary Feedwater System. Interface requirements are provided in section 5.1.4.

The AFWS is actuated by an AFAS. The instrumentation and controls of train A are physically and electrically separate and independent of the instrumentation and controls of train B. Thus, if a single failure prevents actuation of one train the other train will still receive an actuation signal.

The AFAS signal latches the pumps in either the manual or automatic mode and will cycle the valves on the steam generator level signals.

The Seismic Category I portion of the auxiliary feedwater system is provided to automatically initiate residual heat removal capability during emergency conditions such as a steam line rupture, loss of normal feedwater, or loss of offsite and normal onsite power. The non-Seismic Category I portion of the auxiliary feedwater system is provided for normal nonemergency operation during startup, cooldown, and hot standby. The non-Seismic Category I portion of the auxiliary feedwater system is not an engineered safety feature system and, therefore, is not addressed in this section. Subsequent references in this section to the auxiliary feedwater system apply to the Seismic Category I portions only. The Seismic Category I portion of the auxiliary feedwater system is described in subsection 10.4.9.

Table 7.3-6

SAFETY INJECTION ACTUATION SIGNAL ACTUATED DEVICES LIST (Sheet 1 of 2)

P&ID	Description	Function
01, 02, 03-M-SIP-001 -002 -003	SI tanks No. 1 through 4 fill and sample isolation valves (4)	Close
01, 02, 03-M-SIP-001 -002 -003	SI tanks No. 1 through 4 check valve leakage line isolation valves (4)	Close
01, 02, 03-M-SIP-001 -002 -003	HPSI pumps and pump room essential cooling units (2)	Start
01, 02, 03-M-SIP-001 -002 -003	LPSI pumps and pump room essential cooling units (2)	Start
01, 02, 03-M-SIP-001 -002 -003	CS pumps and pump room essential cooling units (2)	Start
01, 02, 03-M-SIP-001 -002 -003	SI tanks No. 1 through 4 isolation valves (4)	Open
01, 02, 03-M-CHP-001, 002 -003, -004 and -005	Letdown line isolation valve (1)	Close
01, 02, 03-M-IAP-001 and -002	Hot leg injection check valve leak isolation valve (2)	Close
01, 02, 03-M-NCP-001, -002 and -003	Essential cooling water system and pump room essential cooling units	Refer to paragraph 7.4.1.1.5
01, 02, 03-M-SPP-001	Essential spray pond system	Refer to paragraph 7.4.1.1.1
01, 02, 03-M-DGP-001	Diesel generator system	Refer to paragraph 7.4.1.1.1
01, 02, 03-M-HJP-001, -002 and 03-M-HJP-003	Control room essential filtration system	Refer to table 7.3-9 and paragraph 7.3.1.1.10.10
01, 02, 03-M-TCP-001, -002 and -003	Condensate transfer system	Refer to subsection 9.2.6

Table 7.3-6
SAFETY INJECTION ACTUATION SIGNAL ACTUATED
DEVICES LIST (Sheet 2 of 2)

Figure No.	Description	Function
01, 02, 03-M-PWP-001	Essential chilled water system	Start
01, 02, 03-M-ECP-001	Normal chilled water system	Stop
01, 02, 03-M-HFP-001	Fuel building essential ventilation system	Refer to paragraph 9.4.5.2
01, 02, 03-M-HTP-001	Containment normal reactor cavity cooling units (4)	Stop
01, 02, 03-M-HTP-001	Containment normal cooling unit (4)	Stop
01, 02, 03-M-HTP-001	Containment CEDM cooling unit (2)	Stop
01, 02, 03-M-HAP-001, -002, -003 and -004	Elect penetration room ESS Acu (2)	Start
	PZR backup heaters (6)	Trip
	480V MCC incoming feeders (4)	Trip
	Essential lighting panel (2)	Trip
01, 02, 03-M-AFP-001	Non safety related Aux Feedwater pump	Stop

The safety-related display instrumentation for the auxiliary feedwater system, which provides the operator with sufficient information to monitor and perform the required safety features, is described in section 7.5.

Further information on the actuation system is provided by the following:

A. Table 6.2.4-2 for a list of valves actuated on an AFAS

B. Table 7.3-7 for additional AFAS actuated devices.

C. FSAR figure 7.4-4, ESFAS signal logic

D. P&I diagram 01, 02, 03-M-AFP-001

E. Figure 7.2-2, instrumentation location layout drawing for AFAS input devices

7.3.1.1.10.8 Fuel Building Essential Ventilation Systems. Radioactive contamination may occur in the spent fuel area in the unlikely event that a spent fuel element is severely damaged during handling. If a fuel handling accident occurs, sensors in the fuel building detect the fission products released from the fuel and initiate appropriate action, as discussed in section 9.4, to reduce the release of fission products into the environment.

Table 7.3-7

AUXILIARY FEEDWATER ACTUATION SIGNAL
ACTUATED DEVICES LIST (Sheet 1 of 2)

P&ID	Description	Function
01, 02, 03-M-AFP-001	Seismic Category I motor-driven auxiliary feedwater pump and pump room cooling unit (1)	Start
01, 02, 03-M-AFP-001	Seismic Category I steam turbine driven auxiliary feedwater pump and pump room cooling unit (1)	Start (b)
01, 02, 03-M-AFP-001	Auxiliary feedwater regulating valves SG1 (2)	(a)
01, 02, 03-M-AFP-001	Auxiliary feedwater regulating valves SG2 (2)	(a)
01, 02, 03-M-AFP-001	Auxiliary feedwater isolation valves SG1 (2)	(c)
01, 02, 03-M-AFP-001	Auxiliary feedwater isolation valves SG2 (2)	(c)
01, 02, 03-M-DGP-001	Diesel generator system	Refer to paragraph 7.4.1.1
01, 02, 03-M-NCP-001, -002 and -003	Essential cooling water system	Refer to paragraph 9.2.2

a. Cycles open and close to intact steam generator.

b. SGA-UV134 and SGA-UV134A; steam supply valves from steam generator No. 1 to the turbine-driven AFS pump, both open on either an AFAS-1 or AFAS-2.

   SGA-UV138 and SGA-UV138A; steam supply valves from steam generator No. 2 to the turbine-driven AFS pump, both open on either an AFAS-1 or AFAS-2.

c. Isolates damaged steam generator and allows flow to undamaged steam generator.

Table 7.3-7

AUXILIARY FEEDWATER ACTUATION SIGNAL

ACTUATED DEVICES LIST (Sheet 2 of 2)

P&ID	Description	Function
01, 02, 03-M-PWP-001	Essential chilled water system	Refer to paragraph 9.2.9
01, 02, 03-M-SCP-004	Steam generator blowdown isolation valves (4)	Close

The fuel building essential ventilation system, as described in section 9.4, is composed of components in redundant load groups, load group 1 and load group 2. The instrumentation and controls of the components and equipment in load group 1 are physically and electrically separate and independent of the instrumentation and controls of the components and equipment in load group 2. Independence is adequate to retain the redundancy required to maintain equipment functional capability following those design basis events shown in table 7.3-2 that require fuel building ventilation isolation.

The fuel building essential ventilation system is automatically actuated by a FBEVAS from the ESFAS. The FBEVAS is initiated by one-out-of-two high airborne activity signals from radiation monitors, one of which is a gaseous monitor in the fuel building normal exhaust duct, and the other of which is an area radiation monitor on a wall overlooking the fuel pool. The system is designed so that loss of electric power to one-out-of-two electronic remote indication and control units or to the actuating logic actuates the fuel building essential ventilation system.

Manual initiation of the fuel building essential ventilation system is provided in the control room.

The safety-related display instrumentation for the fuel building essential ventilation system, which provides the operator with sufficient information to monitor and perform the required safety functions, is described in section 7.5. Further information on the actuation system is provided by the following:

A. Table 7.3-8(A), fuel building essential ventilation actuation signal actuated devices list during FBEVAS

B. Table 7.3-8(B), fuel building/auxiliary building essential ventilation actuated devices list during SIAS

C. Figure 7.3-1, ESFAS signal logic (FBEVAS)

D. P&I diagram 01, 02, 03-M-HFP-001 (fuel building HVAC)

E. Section 12.3, instrument location layout drawing for FBEVAS input devices

The FBEVAS is combined with the SIAS in the device control circuits so that any one of the signals (logical OR) activate the devices listed in table 7.3-8B. During SIAS operation, the fuel building/auxiliary building essential ventilation system is aligned to exhaust from the auxiliary building. The SIAS signal takes precedence over FBEVAS should both signals be present at the same time.

Table 7.3-8

FUEL BUILDING ESSENTIAL VENTILATION
ACTUATION SIGNAL ACTUATED DEVICES LIST

(P&ID 01, 02, 03-M-HFP-001)

Description	Function
A. DURING FBEVAS	
Fuel building normal supply dampers (4)	Close
Fuel building normal supply AHU	Stop
Fuel building normal exhaust dampers (4)	Close
Fuel building normal exhaust fans (2)	Stop
Fuel building exhaust to fuel building/auxiliary building essential AFU isolation dampers (2)	Open
Fuel building/auxiliary building essential exhaust AFU (2)	Start
Auxiliary building exhaust to fuel building/auxiliary building essential exhaust AFU isolation dampers (2)	Close
B. DURING SIAS	
Fuel building exhaust to fuel building/auxiliary building essential exhaust AFU isolation dampers (2)	Close
Fuel building/auxiliary building essential exhaust AFU (2)	Start
Auxiliary building exhaust to fuel building/auxiliary building essential exhaust AFU isolation dampers (2)	Open

7.3.1.1.10.9 Containment Purge Isolation System. Radioactive contamination may occur in the containment building in the event that a spent fuel element is severely damaged during handling. The containment purge isolation system detects abnormal amounts of radioactive material in the containment building and initiates appropriate action to prohibit the release of radioactive material into the environment. Refer to section 9.4 for a description of the containment purge isolation system.

The containment purge isolation system is composed of components in redundant load groups, load group 1 and load group 2. Instrumentation and controls of the components and equipment in load group 1 are physically and electrically separate and independent of instrumentation and controls of the components and equipment in load group 2. Independence is adequate to retain the redundancy required to maintain equipment functional capability following those design basis events shown in table 7.3-2 that are mitigated by the containment purge isolation system.

The containment purge isolation system is automatically actuated by the CPIAS from the ESFAS. CPIAS is initiated by one-out-of-two high airborne activity signals from two redundant radiation monitors located in close proximity to the power access purge exhaust duct and the refueling purge exhaust duct. The monitors are identified as the "PAPA-A" and "PAPA-B" monitors.

The system is designed so that loss of electric power to one-out-of-two electronic remote indication and control units or to the actuating logic actuates the containment purge isolation system.

The CPIAS is combined with the CIAS in the control circuits of the isolation valving common to both the containment purge isolation system and the containment isolation system so that either signal (logical OR) can actuate these valves. Figure 7.3-4 presents a typical control logic for these valves.

The safety-related display instrumentation for the containment purge isolation system that provides the operator with sufficient information to monitor and perform the required safety functions is described in section 7.5.

Further information on the actuation system is provided by the following:

A. Table 6.2.4-2 for a list of devices actuated on a CPIAS

B. Figure 7.3-1, ESFAS signal logic (CPIAS)

C. P&I diagram 01, 02, 03-M-HTP-001 (containment purge system)

D. Section 12.3, instrument location layout drawing for CPIAS input devices

7.3.1.1.10.10 Control Room Essential Ventilation Systems.

The control room essential ventilation systems are the control room ventilation isolation system and the control room essential filtration system.

Upon detection of a high airborne activity signal in the normal air intake, the control room essential filtration system is actuated. Both control room essential ventilation systems, as discussed in section 6.4, are composed of components in redundant load groups, load group 1 and load group 2.

Instrumentation and controls of the components and equipment in load group 1 are physically and electrically separate and independent of instrumentation and controls of the components and equipment in load group 2. Independence is adequate to retain the redundancy required to maintain control room habitability following those design basis events shown in table 7.3-2.

The control room essential filtration system is automatically actuated by a CREFAS. The CREFAS is initiated by one-out-of-two air intake high airborne activity signals, a FBEVAS, or a CPIAS as shown in figure 7.3-2. The CPIAS is discussed in paragraph 7.3.1.1.10.9. The FBEVAS is discussed in paragraph 7.3.1.1.10.8. The system is designed so that loss of electrical power to one-out-of-two electronic remote indication and control units or to the actuating logic actuates the control room essential filtration system.

The CREFAS is combined with the SIAS in the device control circuits so that any one of the signals (logical OR) actuates the devices listed in table 7.3-9. The development of the SIAS is discussed in CESSAR Section 7.3.2.2.1. Figure 7.3-5 presents a typical control logic to show the combination of these signals.

In addition to the automatic initiating signals, two independent smoke detectors are provided in the outside air intake plenum.

Upon detection of smoke, an audible and visible alarm will alert the operator to manually initiate the control room ventilation isolation system.

Manual initiation of the control room ventilation isolation system and the control room essential filtration system is provided in the control room.

The safety-related display instrumentation for the control room essential ventilation systems, which provides the operator with sufficient information to monitor and perform the required safety functions, is described in section 7.5.

Further information on the actuation system is provided by the following:

A. Table 7.3-9, Control Room Essential Filtration Actuation Signal Actuated Devices List

B. Table 7.3-10, Control Room Ventilation Isolation Actuation Signal Actuated Devices List

C. Figure 7.3-2, ESFAS signal logic (CREFAS and CRVIAS)

D. P&I diagram 01, 03-M-HJP-001, -002 and 02-M-HJP-001, -002 and -003 (control building HVAC)

7.3.1.1.10.11 Containment Combustible Gas Control System. The containment hydrogen gas concentration may increase to a combustible concentration following a LOCA. In the unlikely event that a LOCA does occur, the containment hydrogen gas concentration is maintained less than the lower combustible limit by operation of the containment combustible gas control system.

The containment combustible gas control system, as described in subsection 6.2.5, is composed of components in redundant load groups, load group 1 and load group 2. Instrumentation and controls of components and equipment in load group 1 are physically and electrically separate and independent of

Table 7.3-9

CONTROL ROOM ESSENTIAL FILTRATION ACTUATION SIGNAL
ACTUATED DEVICES LIST

P&ID	Description	Function
01, 03-M-HJP-001, -002, 02-M-HJP-001, -002 & -003	Outside air smoke exhaust makeup dampers (2)	Close
01, 03-M-HJP-001, -002, 02-M-HJP-001, -002 & -003	Normal exhaust isolation dampers (6)	Close
01, 03-M-HJP-001, -002, 02-M-HJP-001, -002 & -003	Normal HVAC unit discharge isolation dampers (2)	Close
01, 03-M-HJP-001, -002, 02-M-HJP-001, -002 & -003	Normal recirculation isolation dampers (2)	Close
01, 03-M-HJP-001, -002, 02-M-HJP-001, -002 & -003	Essential supply duct dampers (4)	Open
01, 03-M-HJP-001, -002, 02-M-HJP-001, -002 & -003	Essential HVAC units (2)	Start
01, 03-M-HJP-001, -002, 02-M-HJP-001, -002 & -003	Normal supply unit	Stop
01, 03-M-HJP-001, -002, 02-M-HJP-001, -002 & -003	Communication room inlet dampers (2)	Close
01, 03-M-HJP-001, -002, 02-M-HJP-001, -002 & -003	Communication room outlet dampers (2)	Close
01, 02, 03-M-TCP-001, -002 and -003	Condensate transfer system	Refer to paragraph 9.2.6
01, 02, 03-M-SPP-001	Essential spray pond system	Refer to paragraph 7.4.1.1.4
01, 02, 03-M-NCP-001 -002 and -003	Essential cooling water system	Refer to paragraph 7.4.1.1.5
01, 02, 03-M-PWP-001	Essential chilled water system	Refer to paragraph 9.2-9
01, 02, 03-M-HAP-001 -002, -003 and -004	Essential cooling water pump rooms cooling units (2)	Start
01, 02, 03-M-HAP-001, -002, -003 and -004	Essential cooling water pump rooms isolation dampers (8)	Close

Table 7.3-10

CONTROL ROOM VENTILATION ISOLATION ACTUATION SIGNAL ACTUATED DEVICES LIST

P&ID	Description	Function
01, 02, 03-M-HJP-001, -002 and 02-M-HJP-003	Normal HVAC unit discharge isolation dampers (2)	Close
01, 02, 03-M-HJP-001, -002 and 02-M-HJP-003	Outside air smoke exhaust makeup dampers (2)	Close
01, 02, 03-M-HJP-001, -002 and 02-M-HJP-003	Normal exhaust isolation dampers (6)	Close
01, 02, 03-M-HJP-001, -002 and 02-M-HJP-003	Normal recirculation isolation dampers (2)	Close
01, 02, 03-M-HJP-001, -002 and 02-M-HJP-003	Essential supply duct dampers (4)	Close
01, 02, 03-M-HJP-001, -002 and 02-M-HJP-003	Essential HVAC units (2)	Start
01, 02, 03-M-HJP-001, -002 and 02-M-HJP-003	Normal supply unit	Stop
01, 02, 03-M-HJP-001, -002 and 02-M-HJP-003	Communication room inlet dampers (2)	Close
01, 02, 03-M-HJP-001, -002 and 02-M-HJP-003	Communication room outlet dampers (2)	Close
01, 02, 03-M-TCP-001, -002 and -003	Condensate transfer system	Refer to paragraph 9.2.6
01, 02, 03-M-SPP-001	Essential spray pond system	Refer to paragraph 7.4.1.1.4
01, 02, 03-M-NCP-001, -002 and -003	Essential cooling water system	Refer to paragraph 7.4.1.1.5
01, 02, 03-M-PWP-001	Essential chilled water system	Refer to paragraph 9.2-9
01, 02, 03-M-HAP-001, -002, -003 and -004	Essential cooling water pump rooms cooling units (2)	Start
01, 02, 03-M-HAP-001, -002, -003 and -004	Essential cooling water pump rooms isolation dampers (8)	Close

instrumentation and controls of components and equipment in load group 2. Independence is adequate to retain the redundancy required to maintain equipment functional capability following those design basis events in table 7.3-2 that are mitigated by the containment combustible gas control system.

The containment combustible gas control system components are controlled manually from control switches located at local panels. The local panel(s) will be accessible after a design basis accident (DBA).

The safety-related display instrumentation for the combustible gas control system that provides the operator with sufficient information to monitor and perform the required safety functions is described in section 7.5.

The principal parameter monitored, for determining when the containment combustible gas control system is to be placed in service, is hydrogen. The containment hydrogen analyzer is not normally in service; however, following a DBA, the hydrogen analyzer is placed in service with controls mounted in the main control room.

A control switch with an override feature is provided for each of the containment combustible gas control system isolation valves. This control switch override feature is functional only after receipt of the CIAS, and permits control of each valve independent of the CIAS. The open and closed positions of these valves, in addition to the override status, are indicated in the control room. A typical logic diagram showing implementation of the override signal is shown in figure 7.3-6.

The containment combustible gas control system test pressure is greater than the peak containment design pressure. This precludes system overpressurization by the inadvertent opening of the isolation valves.

Further information on the system is provided by the following:

A. Table 7.3-11, Containment Combustible Gas Control System Actuated Devices List

B. P&I diagram 01, 02, 03-M-HPP-001 (containment combustible gas control system)

7.3.1.2 Design Basis Information

BOP ESFAS. The actuation setpoints are given in table 7.3-12. The design bases for the additional one-out-of-two ESFAS are as follows.

The one-out-of-two ESFAS is designed to provide initiating signals for components that require automatic actuation following a DBA.

The systems are designed on the following bases to ensure adequate performance of their protective functions:

A. The system is designed in compliance with the applicable criteria of Appendix A of 10CFR50, 1971.

B. System testing conforms to the requirements of IEEE Standard 338-1971 and Regulatory Guide 1.22.

C. IEEE 279-1971 establishes specific protection system design bases. The following paragraphs describe how the design bases listed in Section 3 of IEEE 279-1971 are implemented.

1. The additional generating station condition that requires protective action is:

Table 7.3-11

CONTAINMENT COMBUSTIBLE GAS CONTROL SYSTEM ACTUATED DEVICES LIST

P&ID	Description	Relation to Containment	Function
01, 02, 03-M-HPP-001	Containment combustible gas control hydrogen purge exhaust air filtration unit heater (1)	Outside	Start[a]
01, 02, 03-M-HPP-001	Containment combustible gas control hydrogen purge exhaust air filtration unit inlet (2)	Outside	Open[a]
01, 02, 03-M-HPP-001	Containment combustible gas control system inlet isolation valves (2)	Inside	Open[b]
01, 02, 03-M-HPP-001	Containment combustible gas control recombiner and hydrogen purge air filteration unit inlet isolation valves (2)	Outside	Open[b]
01, 02, 03-M-HPP-001	Containment combustible gas control recombiner outlet isolation valves (2)	Outside	Open[b]
01, 02, 03-M-HPP-001	Containment combustible gas control analyzer valves (4)	Outside	Open[a]
01, 02, 03-M-HPP-001	Containment hydrogen recombiners (2)	Outside	Start[a]

a. Manually actuated

b. CIAS overridden

Table 7.3-11A
ENGINEERED SAFETY FEATURES ACTUATION SYSTEM SETPOINTS AND MARGINS TO ACTUATION

Actuation Signal	Typical Full Power	Normal Operation Range	Trip Setpoint	Margin to Actuation
SIAS & CIAS				
Low pressurizer pressure	2,250 psia	2,100-2,350 psia	≥ 1,837 psia[a]	263 psi
High containment pressure	0 psig	0 psig	≤ 3 psig	3 psi
CSAS				
High-High containment pressure	0 psig	0 psig	≤ 8.5 psig	8.5 psi
RAS				
Low refueling water tank level	--	81.2-98%[h]	9.4% of span	71.8%
MSIS				
Low steam generator pressure	1039 psia	1010-1170 psia	960 psia[d]	79 psi
High containment pressure	0 psig	0 psig	≤ 3 psig	3 psi
High steam generator level	55%	30-74%	≤ 91% NR[e]	17%
AFAS				
Low steam generator level and	82%	72-90%	≥ 25.8% WR[f]	46.2
Steam generator differential pressure[b]	0 psid	0 psid	≤ 185 psid	185 psi
DAFAS				
Low steam generator level[c]	82%	72-90%	20.3%	51.7
LOP				
4.16 kV Emergency Bus Loss of Voltage	4160 V		[g]	
4.16 kV Emergency Bus Degraded voltage	4160 V		3744 V	

a. In MODES 3-4, the value may be decreased manually, to a minimum of 100 psia, as pressurizer pressure is reduced, provided:

(a) the margin between the pressurizer pressure and this value is maintained at less than or equal to 400 psi; and
(b) when the RCS cold leg temperature is greater than or equal to 485 degrees F, this value is maintained at least 140 psi greater than the saturation pressure corresponding to the RCS cold leg temperature.

The setpoint shall be increased automatically as pressurizer pressure is increased until the trip setpoint is reached. Trip may be manually bypassed below 400 psia; bypass shall be automatically removed whenever pressurizer pressure is greater than or equal to 500 psia.

b. This is a calculated, not sensed, variable.

c. Low steam generator levels, diverse scram signals present without normal ESFAS initiation of AFAS or MSIS (ATWS requirements).

d. In MODES 3-4, value may be decreased manually as steam generator pressure is reduced, provided the margin between the steam generator pressure and this value is maintained at less than or equal to 200 psi; the setpoint shall be increased automatically as steam generator pressure is increased until the trip setpoint is reached.

e. % of the distance between steam generator upper and lower level narrow range instrument nozzles.

f. % of the distance between steam generator upper and lower level wide range instrument nozzles.

g. See figure 8.3-3.

h. Technical Specification minimum required RWT level to high level alarm (Mode 1-4 limits).

Table 7.3-12

BOP ESF SYSTEM ACTUATION SETPOINTS AND MARGINS TO ACTUATION (Sheet 1 of 2)

Actuation Signal	(Full Power) Nominal	Normal Operation Limit	Actuation Setpoint Refer to Table 11.5-1	Margin to Actuation
FBEVAS				
Fuel building exhaust duct high activity	Less than sensitivity $\left(< 10^{-6}\ \frac{\mu Ci}{cm^3}\right)$	Less than sensitivity $\left(< 10^{-6}\ \frac{\mu Ci}{cm^3}\right)$	$2x10^{-6}\ \frac{\mu Ci}{cm^3}$	$1x10^{-6}\ \frac{\mu Ci}{cm^3}$
Fuel pool high radiation level	0.5mr/h	0.5 mr/h	< 15 mr/h	14.5 mr/h
CPIAS				
Power access purge exhaust area radiation level	‹2.5 mr/h	‹2.5 mr/h	2.5 mr/h	Negligible
CREFAS				
Control room air intake high activity level	Less than sensitivity $\left(< 10^{-6}\ \frac{\mu Ci}{cm^3}\right)$	Less than sensitivity $\left(< 10^{-6}\ \frac{\mu Ci}{cm^3}\right)$	$2x10^{-5}\ \frac{\mu Ci}{cm^3}$	$1.9x10^{-5}\ \frac{\mu Ci}{cm^3}$

Table 7.3-12

BOP ESF SYSTEM ACTUATION SETPOINTS AND MARGINS TO ACTUATION (Sheet 2 of 2)

Actuation Signal	(Full Power) Nominal	Normal Operation Limit	Actuation Setpoint	Margin to Actuation
CRVIAS				
Control room air intake high smoke level (manual initiation of CRVIAS upon detection of smoke)	Less than sensitivity	Less than sensitivity	1.25% obscuration	1.25% obscuration

a. Fuel handling accident

b. Fire/smoke-plant vicinity

2. The system is designed to monitor the following additional parameters in order to provide protective actions:

   a. Containment radiation/airborne activity

   b. Fuel building radiation/airborne activity

   c. Control room air intake activity

   d. Control room air intake smoke

3. The number and location of the sensors required to monitor the variables listed in sublisting C.2 above are contained in table 7.3-13A.

4. The normal operation limits for each variable are provided in table 7.3-12.

5. The margin between the operation limits and actuation setpoints are provided in table 7.3-12.

6. The actuation setpoints are provided in table 7.3-12.

7. System components are qualified for the environmental conditions discussed in section 3.11. In addition, the system is capable of performing its intended functions under the most degraded conditions of the electric support system as discussed in section 8.3.

8. The one-out-of-two ESFAS is designed with consideration given to unusual events that could degrade system performance so that:

Table 7.3-13A

BOP ESF SYSTEMS ACTUATION SENSORS

Monitored Variable	Type	Number of Sensors	Location
Power access purge exhaust area radiation level	Geiger-Mueller	2	Outside containment between power access purge exhaust duct and refueling purge exhaust duct
Fuel building exhaust duct radiation level	β-Scintillation	1	Fuel building exhaust duct
Fuel pool area radiation level	Geiger-Mueller	1	Overlooking spent fuel pool
Control room air intake activity level	β-Scintillation	2	Control room outside air intake duct
Control room air intake smoke detector	Ionization (Products of combustion detector)	2	Control room outside air intake duct

TABLE 7.3-13B

NSSS ENGINEERED SAFETY FEATURES ACTUATION SYSTEM SENSORS

Monitored Variable	Sensor Type	Number of Sensors	Location
Pressurizer Pressure	Pressure Transducer	4* (wide range)	Pressurizer
Containment Pressure	Pressure Transducer (Wide and Narrow range)	8*	Enclosure Complex
Steam Generator Pressure	Pressure Transducer	4/Steam Generator*	Steam Generator
Refueling Water Tank Level	Differential Pressure Transducer	4	Refueling Water Tank
Steam Generator Level	Differential Pressure Transducer (Wide and Narrow Range)	8/Steam Generator*	Steam Generator

*Shared with the Reactor Protective System

a. A loss of power to the measurement channels and/or to the logic system causes system actuation.

b. Any single failure within the system shall not prevent proper protective action at the system level. The single failure criterion is discussed in paragraph 7.3.2.3.2.

c. The environmental conditions under which the ESFAS shall be capable of performing its intended function are described in section 3.11.

d. The seismic conditions under which the ESFAS shall be capable of performing its intended function are described in section 3.10.

9. The minimum performance requirements of the one-out-of-two ESFAS are as follows:

a. The ESFAS system response times are provided below. The total ESFAS response times represent the sum of the sensor response time plus the one-out-of-two ESFAS response time.

		Sensor Response Time	One-Out-of-Two ESFAS Response Time
(1)	Containment power access purge exhaust area radiation	Ref.table 11.5-1 note aa +	2.0s

(2)	Fuel pool area radiation	Ref.table 11.5-1 +	2.0s
(3)	Fuel building exhaust air-borne activity	Ref.table 11.5-1 +	2.0s
(4)	Control room air intake airborne activity	Ref. table 11.5-1 +	2.0s
(5)	Control room air intake smoke	50s	N.A. (Manual Initiation)

b. The accuracies of the ESFAS measurement channels are:

(1)	Containment power access purge exhaust area radiation	±20%
(2)	Fuel pool area radiation	±20%
(3)	Fuel building exhaust airborne activity	±25%
(4)	Control room air intake airborne activity	±25%
(5)	Control room air intake smoke	±10%

NSSS ESFAS. The design bases of the ESF Systems are discussed in Chapter 6.0. The ESFAS is designed to provide initiating

signals for ESF components which require automatic actuation following the design bases events shown on Table 7.3-2.

The systems are designed in compliance with the applicable criteria of the NRC, "General Design Criteria for Nuclear Power Plants," Appendix A, 10CFR50. System testing conforms to the requirements of IEEE 338-1971, "Trial Use Criteria for Periodic Testing of Nuclear Power Generating Station Protection Systems," and Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions."

Specific design criteria for the ESFAS are detailed in IEEE 279-1971 "Criteria for Protection Systems for Nuclear Power Generating Stations," Section 3. The following is a discussion of the specific items in IEEE 279-1971 and their implementation.

The generating station conditions requiring actuation of the ESFAS are listed on Table 7.3-2, which also shows which system will actuate for each event. The monitored variables required for ESF System protective action are listed on Table 7.3-3, which also shows which signals are generated by the variable. The number and location of the sensors required to monitor the variables are listed in Table 7.3-13B. The normal operating ranges, actuation setpoints, the nominal full power value, and the margin between the last two are listed on Table 7.3-11A.

The ESFAS is designed with consideration given to unusual events which could degrade system performance. System components are qualified for the environmental conditions discussed in Section 3.11 and the seismic conditions discussed in Section 3.10. These two topics are discussed in Combustion Engineering Topical Reports CENPD-182, "Seismic Qualification

of Instrumentation and Electrical Equipment," and CENPD 255, "Qualification of Combustion Engineering Class IE Instrumentation," (References 2 and 3). A single failure within the system will not prevent proper protective action at the system level. The single failure criterion is discussed in section 7.3.2.3.2.

7.3.1.3 Final System Drawings

The signal logic and typical control circuits are shown in figures following this section.

The RAS has added manual actuation which gives the operator greater operational flexibility.

The MSIS logic (Refer to Figure 7.3-7c) has added the high steam generator water level and high containment pressure. This protects downstream equipment from two-phase flow and reduces the amount the Reactor Coolant System could be cooled due to excessive feedwater flow.

For a list of applicable design drawings and diagrams, see section 1.7.

7.3.1.4 Engineered Safety Features Actuation System Supporting Systems

The systems required to support the ESFAS are discussed in Section 7.4. The electrical power distribution is discussed in Section 8.3.

7.3.2 ANALYSIS

7.3.2.1 Introduction

BOP ESFAS. The analysis for the additional one-out-of-two ESFAS and instrumentation is similar to that presented for the NSSS ESFAS as is the ESF manual actuation of the combustible gas control system.

NSSS ESFAS. The ESFAS is designed to provide protection against the Design Basis Events listed on Table 7.3-2. The ESF Systems that are actuated are discussed in Chapter 6.0, along with their design bases and evaluations.

The signals which will cause each ESFAS are listed on Table 7.3-3; the bases are discussed in Section 7.3.1.2; the actuation setpoints are given on Table 7.3-11a. Most ESFAS signals are single parameter, fixed setpoint actuations. The ESFAS that do not fall into this category are:

A. Low pressurizer pressure - can be decreased to 400 psi below the existing pressurizer pressure by the operator;

B. Low steam generator pressure - can be decreased to 200 psi below the existing steam generator pressure by the operator.

These resets are controlled by administrative procedures.

Additionally, several ESFAS can be actuated by more than one parameter. That is, different parameters can cause the same ESFAS. The ESFAS which fall into this category are:

A. SIAS by either low pressurizer pressure or high containment pressure;

B. CIAS by receiving the SIAS for that channel so that it actuates on low pressurizer pressure or high containment pressure;

C. MSIS by high steam generator water level in either steam generator, low steam generator pressure in either steam generator, or high containment pressure.

One ESFAS is, essentially, a multi-parameter actuation. An AFAS is generated on low steam generator water level unless that steam generator has been identified as being ruptured. A steam generator is identified as being ruptured when its pressure is some differential value below the pressure of the other steam generator, coincident with its own low level signal and with the other steam generator being identified as not ruptured.

Each ESFAS setpoint is selected to be consistent with the function of the respective ESF System requirements. The setpoints are selected to provide ESF actuation in sufficient time to provide the necessary actions to mitigate the consequences of the Design Basis Events which caused the ESFAS.

The adequacy of all ESFAS trip setpoints is verified through an analysis of the pertinent system transients reported in Chapter 15.0. These analyses utilize an Analysis Setpoint (assumed trip initiation point) and system delay times associated with the respective trip functions. The Analysis Setpoint along with instrument uncertainties provides the basis for the calculation of the final equipment setpoints to be reported in the Technical Specifications. Limiting trip delay times are given in Table 7.3-1B. The manner by which these delay times and uncertainties will be verified is discussed in Section 7.2.1.2.

7.3.2.1.1 Design Basis Events (DBE)

The DBE conditions for which the system will take action are those unplanned events under conditions that may occur once during the life of several nuclear generating stations, and certain combinations of unplanned events and degraded systems that are never expected to occur during the life of all nuclear power plants. The consequences of these events should be limited by the ESF Systems. The ESF Systems have a major responsibility to mitigate the consequences of the events listed below. This includes minimizing fuel damage and subsequent release of fission products or other related effects. The limiting fault conditions for which the ESFAS actuate are:

A. RCS pipe rupture including a double ended rupture;

B. Single CEA ejection;

C. Steam system pipe rupture, including a double ended rupture;

D. Depressurization due to inadvertent actuation of primary or secondary safety valves at 100% power; and

E. Feedwater system pipe rupture including a double-ended rupture.

The ESFAS will also act to mitigate the consequences of Incidents of Moderate Frequency (IMF) and Infrequent Events as follows:

A. Excess heat removal due to secondary system malfunctions;

B. Inadvertent pressurization or depressurization of the RCS;

C. Change in normal heat transfer capability between steam and reactor coolant systems including:

   1. Improper main feedwater; and

   2. Loss of external load; and

D. Steam generator tube rupture.

7.3.2.2 Actuation Bases

NSSS ESFAS. The ESFAS consists of six signals based on five parameters. Each ESFAS has manual actuation switches locally on the main control board or at the ESFAS Auxiliary Relay Cabinets.

7.3.2.2.1 Safety Injection Actuation Signal (SIAS)

Input

Pressurizer pressure, containment pressure, or manual pushbuttons. The pressure signals are shared with the RPS.

Function

The SIAS actuates the components necessary to inject borated water into the reactor coolant system and actuates components for emergency cooling. SIAS is also initiated by a loss of power to two channels.

7.3.2.2.2 Containment Spray Actuation Signal (CSAS)

Input

Containment pressure signals or manual pushbuttons.

Function

The CSAS actuates the Containment Spray System. CSAS is also initiated by a loss of power to two channels.

7.3.2.2.3 Recirculation Actuation Signal (RAS)

Input

Refueling Water Tank (RWT) Level, or manual pushbuttons.

Function

The RAS is provided to actuate the recirculation mode of operation of the Emergency Core Cooling System. RAS is also initiated by a loss of power to two channels.

7.3.2.2.4 Containment Isolation Actuation Signal (CIAS)

Input

Pressurizer pressure, containment pressure, or manual pushbuttons. The pressurizer and containment pressure signals are provided via the SIAS.

Function

The CIAS actuates the isolation of lines penetrating the containment. CIAS is also initiated by a loss of power to two channels.

7.3.2.2.5 Main Steam Isolation Signal (MSIS)

Input

Pressure from each steam generator, containment pressure, level from each steam generator, or manual pushbuttons.

Function

The MSIS is provided to actuate the isolation of each steam generator. MSIS is also initiated by a loss of power to two channels.

7.3.2.2.6 Auxiliary Feedwater Actuation Signal (AFAS)

Input

Level and pressure from each steam generator with "not ruptured" calculated signal or manual switches.

Function

The AFAS actuates auxiliary feedwater on low water level to the intact steam generator(s). AFAS is also initiated by a loss of power to two channels. The AFAS is based on the following conditions: where low steam generator water level trip exists, its pressure is greater than the other steam generator's pressure by a predetermined value or the other steam generator is identified as not ruptured.

Actuation circuit AFAS I pertains to steam generator 1 and AFAS II actuation circuit pertains to steam generator 2.

7.3.2.3 Design

7.3.2.3.1 General Design Criteria

BOP ESFAS

A. Criterion 16: Containment Design

Refer to subsection 3.1.12.

B. Criterion 20: Protection System Functions

Engineered safety features action will be automatically initiated upon sensing the presence of accident conditions except for the combustible gas control system and the control room ventilation isolation system. Engineered safety features actuation system action will be manually initiated for this section since it is not required immediately after a DBA. Sufficient information is provided to allow the operator to make a timely decision as to system operating requirements.

C. Criterion 22: Protection System Independence

Independence is ensured through the redundance and diversity described in paragraphs 7.3.1.1.6 and 7.3.1.1.7. Two independent sensor channels are provided for the one-out-of-two ESFAS inputs. Two independent output paths are provided for the one-out-of-two ESFAS outputs.

NSSS ESFAS

Appendix A, 10CFR50, "General Design Criteria for Nuclear Power Plants," established minimum requirements for the principle design criteria for water cooled nuclear power plants. This section describes the requirements that are applicable to the

ESFAS. Most references will be to Section 3.1 where the criteria are first addressed. Section 7.2.2.3.1 will be referenced if other comments from the RPS are applicable.

Criterion 1	-	Quality Standards and Records: Refer to Section 3.1.1 for compliance.
Criterion 2	-	Design Bases for Protection Against Natural Phenomena: Refer to Section 3.1.2 for compliance.
Criterion 3	-	Fire Protection: Refer to Section 3.1.3 for compliance
Criterion 4	-	Environmental and Missile Design Bases: Refer to Section 3.1.4 for compliance.
Criterion 13	-	Instrumentation and Control: Refer to Section 3.1.9 for compliance. Variables monitored are those which affect ESF Systems.
Criterion 16	-	Containment Design: Refer to Section 3.1.12 for compliance.
Criterion 20	-	Protective System Functions: Refer to Section 3.1.16 for compliance.

Criterion 21 - Protection System Reliability and Testability:

Refer to Section 3.1.17 for compliance.

Criterion 22 - Protection System Independence:

Refer to Section 3.1.18 for compliance.

Criterion 23 - Protection System Failure Modes:

Refer to Section 3.1.19 for compliance.

From the PPS cabinet the signals are sent to two ESFAS Auxiliary Relay Cabinets. In each cabinet is the selective actuation logic for each train. There is no interconnection between the two Auxiliary Relay Cabinets or the trains they actuate so that train A is completely independent of train B.

Criterion 24 - Separation of Protection and Control Systems:

Refer to Section 3.1.20 for compliance.

Criteria 34, 35, 37, 38, 40, 41, 43, 44 and 46:

Refer to Sections 3.1.30, 31, 33, 34, 36, 37, 39, 40 and 42 for compliance.

The ESFAS provides the actuation which meets the requirements of IEEE 279-1971 and IEEE 338-1971. The single failure criterion is met for all ESFAS. The ESFAS is fully testable. Those components which cannot be tested during power operations are tested when the plant is shutdown.

7.3.2.3.2 Equipment Design Criteria

BOP ESFAS. IEEE Standard 279-1971 establishes minimum requirements for safety-related functional performance and reliability of the ESFAS. The following additional paragraphs provide the IEEE 279, Section 4, criteria numbers and titles followed by an explanation as to how they are satisfied.

4.2 Single Failure Criterion

The one-out-of-two ESFAS is designed so that any single failure within the protection system shall not prevent proper protective action at the system level when required. No single failure will defeat more than one of the two protective channels associated with any one trip function.

Although no single failure will defeat more than one of the two protective channels, a single failure may cause spurious actuation. However, this spurious actuation is allowable since it does not create plant conditions requiring protective action nor does it interfere with normal reactor operations.

A complete analysis of single failures for one-out-of-two is presented in tables 7.3-14 through 7.3-17. The worst case single failure is the failure of a group actuation relay to deenergize. This condition causes loss of one of the two redundant sets of associated ESF equipment.

4.10 Capability for Test and Calibration

Testing is described in paragraph 7.3.1.1.8 and is in compliance with IEEE 338 as discussed in paragraph 7.3.2.3.3.

4.11 Channel Bypass or Removal from Operation

Testing of the one-out-of-two ESFAS is done by channel actuation. Either one of the two channels may be calibrated or

repaired without detrimental effects on the system. Individual trip channels may be bypassed to effect a single channel logic on the ESFAS signal. Maintenance and calibration of the bypassed channel can be accomplished in a short time interval. Probability of failure of the remaining channel is acceptably low during such maintenance periods.

4.12 Operating Bypasses

There are no operating bypasses.

4.15 Multiple Setpoints

There are no multiple setpoints.

4.21 System Repair

Identification of a defective channel will be accomplished by observation of system status lights or by testing as described in paragraph 7.3.1.1.8. Replacement or repair of components in the actuation logic is accomplished with the affected channel bypassed. The affected trip function then operates in a single active channel trip logic.

NSSS ESFAS

Many of the design criteria for protection systems are discussed in section 7.1.2. IEEE 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," establishes minimum requirements for safety-related functional performance and reliability of the ESFAS. This section describes how the requirements of Section 4 of IEEE 279-1971 are satisfied. The following heading numbers correspond to the section numbers of IEEE 279-1971.

4.1 General Functional Requirements

The ESFAS is designed to actuate the appropriate ESF Systems, when required, to mitigate the consequences of the specified Design Basis Events. Instrument performance characteristics, response times, and accuracies are selected for compatibility with, and adequacy for, the particular function. Actuation setpoints are established by analysis of the RCS parameters, steam generator parameters and containment pressure. Factors such as instrument inaccuracies, bistable trip delay times, valve travel times and pump starting times, are considered in establishing the margin between the actuation setpoints and the safety limits. In addition, the possible loss of AC power and the time required to start standby power and to sequence loads must also be considered. The final determination of all of these times is the Applicant's responsibility. The time response of the sensors or protection systems are evaluated for abnormal conditions. Since all uncertainty factors are considered as cumulative for the derivation of these times, the actual response time may be more rapid. However, even at the maximum times, the system provides conservative protection.

4.2 Single Failure Criterion

The ESFAS is designed so that any single failure within the system will not prevent proper protective action at the system level. No single failure will defeat more than one of the four protective channels associated with any one trip function.

The effects of single faults in the RPS are discussed in section 7.2.2.3.2. A similar analysis is applicable to that portion of the ESFAS located in the PPS cabinet. The initiating signal from the PPS goes to two separate ESFAS

Auxiliary Relay Cabinets. Each cabinet contains the actuation circuitry and group relays for each train, therefore, a failure in one cabinet cannot affect the circuitry and actuated equipment of the other cabinet.

Single faults of initiation relay or actuation relay buses have no effect, as a selective two-out-of-four logic is required for actuation.

Single faults of the actuation (or control) circuitry will cause, at worst, only a failure of a component, group of components, or actuation of a system within one of the two redundant actuation trains; actuation of the remaining redundant train components is sufficient for the protective action.

4.3 Quality Control of Components and Modules

The system is designed in accordance with the Topical Report CENPD-210A, "Description of the C-E Nuclear Steam Supply System Quality Assurance Program" (Reference 4).

4.4 Equipment Qualification

The ESFAS equipment is qualified in accordance with the methodology discussed in Sections 3.10 and 3.11.

4.5 Channel Integrity

Type testing of components, separation of sensors and channels, and qualification of cabling are utilized to ensure that the channels will maintain their functional capability required under applicable extremes of environment, power supplied, malfunction, and DBE conditions. Loss or damage of any one path will not prevent the protective action of the ESFAS. Sensors are piped using materials of comparable quality to the

systems to which they are attached so that, in the unlikely event of blockage or failure of any one connection, protective action is not prevented. The process sensors located in the containment building are specified and rated for the intended service. Components which must operate during or after DBEs are rated for the expected post-event environment. Results of type tests are used to verify these ratings.

The separation requirements for the components not within the CESSAR Licensing scope are discussed in section 7.3.3 "Engineered Safety Features Actuation System Interface Requirements".

4.6 Channel Independence

The location of the sensors, for the ESFAS, and the points at which the sensing lines are connected to the process loop have been selected to provide physical separation of the channels within the system, thereby precluding a situation in which a single event could remove or negate a protective action. The routing of cables from protection system transmitters is arranged so that the cables are separated from each other, and from power cabling, to minimize the likelihood of common event failures. This includes separation of the containment penetration areas. The initiation paths are located in four bays of the PPS cabinet and the actuation devices are fed from the two ESFAS Auxiliary Relay Cabinets. Mechanical and thermal barriers within these cabinets minimize the possibility of a common mode failure. Common mode failure is addressed in Topical Report CENPD-148, "Review of Reactor Shutdown System (PPS Design) for Common Mode Failure Susceptibility" (Reference 5).

The output from these redundant channels are isolated from each other so that loss of a channel does not cause loss of the system. The signals from the ESFAS which supply the PMS are isolated at the PMS input. The ESFAS annunciators are isolated as necessary to ensure the ESFAS maintains its channel independence.

The criteria for separation and physical independence of channels are based on the need for decoupling the effects of DBE consequences and power supply transients, and for reducing the likelihood of channel interaction during testing or in the event of a channel malfunction.

4.7 Control and Protection System Interaction

4.7.1 Classification of Equipment

No portion of the ESFAS is used for both protective and control functions.

4.7.2 Isolation Devices

Signals sent from the ESFAS to the PMS are isolated at the PMS and annunciators are isolated at the annunciators such that a failure in these areas will not affect the protective action of the ESFAS.

4.7.3 Single Random Failure

This criterion is not applicable since there are no channels used for both control and protection. Therefore a single random failure can only occur in either a control or a protection channel.

4.7.4 Multiple Failures Resulting from a Credible Single Event

This cannot exist because control and protection channels have nothing in common.

4.8 Derivation of Signal Inputs

Insofar as possible, inputs are derived from signals that are direct measurements of the desired variable. Directly measured variables include pressurizer, containment, and steam generator pressures. The steam generator and refueling water tank levels are derived from differential pressure signals. The differential between the steam generator pressures, for the AFAS, is a calculated value.

4.9 Capability for Sensor Checks

ESFAS sensors are checked by cross-channel comparison. Each channel has a known relationship with the other channels of the same parameter.

4.10 Capability for Test and Calibration

The ESFAS design complies with IEEE 338-1971, "Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection System Actuation Functions," as discussed in section 7.3.2.3.3.

4.11 Channel Bypass or Removal from Operation

Any one of the four protection channels in the ESFAS may be tested, calibrated, or repaired without detrimental effect on the system. Individual actuation channels (i.e., pressurizer pressure, containment pressure, steam generator level) may be bypassed to create a two-out-of-three logic while maintaining

the coincidence of two on the remaining channels. The single failure criterion is met during this condition.

4.12 Operating Bypasses

Operating bypass is provided as shown on Table 7.3-1c. The operating bypass is automatically removed when the permissive condition is not met. The circuitry and devices which function to remove this inhibit are designed in accordance with IEEE 279-1971.

4.13 Indication of Bypasses

Indication of test or bypass conditions, or removal of any channel from service is given by annunciators. The operating bypass that is automatically removed at a fixed setpoint, is alarmed and indicated.

4.14 Access to Means for Bypassing

Trip channel bypasses have access controlled by means of key locked doors. When the first parameter is bypassed there is an audible and visible alarm to indicate which channel is being bypassed. The specific parameter or parameters which are being bypassed are indicated by lights at the PPS cabinet and its remote operator's module.

The operating bypasses also have audible and visible alarms. The operating bypasses have automatic features which provide a permissive level at which they can be actuated and a second level at which they are automatically removed.

4.15 Multiple Setpoints

Manual reduction of the setpoints for low pressurizer and low steam generator pressures are used for the controlled reduction of pressures as discussed in sections 7.3.1.1.10.4 and

7.3.1.1.10.5. The setpoint reductions are initiated by main control board pushbuttons for each channel, one pushbutton for the pressurizer pressure and one pushbutton for both steam generator pressures within the one channel. Operation of the pushbutton will reduce the pressure actuation setpoint a selected increment below the existing system pressure. As the pressurizer or steam generator pressure increases the actuation setpoint will increase automatically with the pressure, maintaining a fixed increment, until the setpoint reaches its normal actuation setpoint value.

4.16 Completion of Protective Action Once It is Initiated

The ESFAS is designed to ensure that protective action will go to completion once initiated. Actuation of an ESFAS can be cleared by the operator manually resetting the ESFAS at the PPS cabinet and the ESFAS Auxiliary Relay Cabinets. A protective action is initiated when the selective two-out-of-four logic reaches the proper coincidence of two state. A protective action is completed when all of the appropriate ESF actuated components have assumed the proper state for their ESF function. The AFAS valves are not locked into its actuation but the pumps are locked in. AFAS is designed to cycle based on the steam generator level signal. When the low level signal clears, the AFAS is lost, until the level drops to the actuation setpoint again.

4.17 Manual Initiation

A manual initiation is effected by operating manual switches in the main control room or at the ESFAS Auxiliary Relay Cabinets. These are arranged in a selective two-out-of-four logic. No

single failure will prevent a manual actuation at the system level.

4.18 Access to Setpoint Adjustments, Calibration and Test Points

A key is required for access to setpoint adjustments, calibration and test points. Access is also annunciated. Setpoints are continuously monitored by the PMS.

4.19 Identification of Protective Action

Indication lights are provided for all protective actions, including identification of the channel trips.

4.20 Information Readout

Means are provided to allow the operator to monitor all actuation system inputs, outputs, and calculations. The specific displays that are provided for continuous display are described in Section 7.5.

4.21 System Repair

Identification of a defective channel will be accomplished by observation of system status lights, or by testing as described in section 7.3.1.1.8. Replacement or repair of components is accomplished with the affected channel bypassed. The affected function is then in a two-out-of-three logic, but still maintaining a coincidence of two for actuation.

4.22 Identification

All equipment associated with the actuation system, including panels, modules, and cables, is marked in order to facilitate identification. Interconnecting cabling will be color coded as discussed in section 7.1.3.16. The equipment to be supplied by the Applicant shall have this requirement specified in the interface section.

Table 7.3-14

ONE-OUT-OF-TWO-ESFAS

FUEL BUILDING ESSENTIAL VENTILATION ACTUATION SIGNAL

FAILURE MODES AND EFFECTS ANALYSIS (Sheet 1 of 3)

Failure Mode	Effect on System	Detection	Remarks
Loss of one ac load group (diesel)	System isolates (fuel building normal supply and exhaust dampers close)	Immediate annunciator	Redundant system actuates (fuel building essential exhaust)
Loss of one dc load group (1E)	System actuates (fuel building essential exhaust)	Immediate annunciator	Actuation of both load groups (fuel building essential exhaust)
Loss of instrument air system	System isolates	Immediate annunciator	Closure of fuel building normal supply and exhaust dampers
Input sensor fails:			
High	System actuates (fuel building essential exhaust)	Immediate annunciator and periodic testing	Actuation of both load groups (fuel building essential exhaust)
Low	None	Immediate annunciator and periodic testing	Manual actuation available to the operator

Table 7.3-14

ONE-OUT-OF-TWO-ESFAS
FUEL BUILDING ESSENTIAL VENTILATION ACTUATION SIGNAL
FAILURE MODES AND EFFECTS ANALYSIS (Sheet 2 of 3)

Failure Mode	Effect on System	Detection	Remarks
Input sensor wiring fails:			
Open	System actuates (fuel building essential exhaust)	Immediate annunciator and periodic testing	Actuation of both load groups (fuel building essential exhaust)
Short	Loss of one sensing channel	Periodic testing	Other sensor channel and system level manual actuation available to actuate both load groups
Manual input fails:			
Open	Loss of system level manual initiation of one load group (fuel building essen-tial exhaust)	Periodic testing	Automatic actuation available for both load groups, system level manual actu-ation available for redundant load group, and manual device level control fully operable

Table 7.3-14

ONE-OUT-OF-TWO-ESFAS
FUEL BUILDING ESSENTIAL VENTILATION ACTUATION SIGNAL
FAILURE MODES AND EFFECTS ANALYSIS (Sheet 3 of 3)

Failure Mode	Effect on System	Detection	Remarks
Manual input fails: (continued)			
Short	System actuation of one load group (fuel building essential exhaust)	Immediate annunciator	Actuation of one load group (fuel building essential exhaust)
Output relay mechanically jammed	Loss of system level actuation of one load group (fuel building essential exhaust)	Periodic testing	Other load group available and manual device control fully operable
Output relay fails de-energized	System actuation of one load group (fuel building essential exhaust)	Visual observation of system status	Actuation of one load group (fuel building essential exhaust)

Table 7.3-15

ONE-OUT-OF-TWO-ESFAS
CONTAINMENT PURGE ISOLATION ACTUATION SIGNAL
FAILURE MODES AND EFFECTS ANALYSIS (Sheet 1 of 3)

Failure Mode	Effect on System	Detection	Remarks
Loss of one ac load group (diesel)	Loss of system level actuation of one load group	Immediate annunciator	Redundant system actuates
Loss of one dc load group (1E)	System actuates	Immediate annunciator	Actuation of both load groups
Loss of instrument air system	No effect	Immediate annunciator	Instrument air not required for use in this system
Input sensor fails:			
High	System actuates	Immediate annunciator and periodic testing	Actuation of both load groups
Low	None	Immediate annunciator and periodic testing	Manual actuation available to the operator
Input sensor wiring fails:			
Open	System actuates	Immediate annunciator and periodic testing	Actuation of both load groups

Table 7.3-15

ONE-OUT-OF-TWO ESFAS
CONTAINMENT PURGE ISOLATION ACTUATION SIGNAL
FAILURE MODES AND EFFECTS ANALYSIS (Sheet 2 of 3)

Failure Mode	Effect on System	Detection	Remarks
Input sensor wiring fails: (continued)			
Short	Loss of one sensing channel	Periodic testing	Other sensor channel and system level manual actuation available to actuate both load groups
Manual input fails:			
Open	Loss of system level manual initiation of one load group	Periodic testing	Automatic actuation available for both load groups, system level manual actuation available for redundant load group, and manual device level control fully operable
Short	System actuation of one load group	Immediate annunciator	Actuation of one load group

Table 7.3-15

ONE-OUT-OF-TWO ESFAS
CONTAINMENT PURGE ISOLATION ACTUATION SIGNAL
FAILURE MODES AND EFFECTS ANALYSIS (Sheet 3 of 3)

Failure Mode	Effect on System	Detection	Remarks
Output relay mechanically jammed	Loss of system level actuation of one load group	Periodic testing	Other load group available and manual device control fully operable
Output relay fails deenergized	System actuation of one load group	Visual observation of system status	Actuation of one load group

Table 7.3-16

ONE-OUT-OF-TWO ESFAS
CONTROL ROOM VENTILATION ISOLATION ACTUATION SIGNAL
FAILURE MODES AND EFFECTS ANALYSIS (Sheet 1 of 3)

Failure Mode	Effect on System	Detection	Remarks
Loss of one ac load group (diesel)	System isolates	Immediate annunciator	Redundant system actuates
Loss of one dc load group (1E)	System isolates	Immediate annunciator	Redundant system actuates
Loss of instrument air system	System isolates	Immediate annunciator	Closure of control room normal supply dampers

Table 7.3-16

ONE-OUT-OF-TWO ESFAS
CONTROL ROOM VENTILATION ISOLATION ACTUATION SIGNAL
FAILURE MODES AND EFFECTS ANALYSIS (Sheet 2 of 3)

Failure Mode	Effect on System	Detection	Remarks
Manual input fails:			
Open	Loss of system level manual initiation of one load group	Periodic testing	Automatic actuation available for both load groups, system level manual actuation available for redundant load group, and manual device level control fully operable
Short	System actuation of one load group	Immediate annunciator	Actuation of one load group

Table 7.3-16

ONE-OUT-OF-TWO ESFAS
CONTROL ROOM VENTILATION ISOLATION ACTUATION SIGNAL
FAILURE MODES AND EFFECTS ANALYSIS (Sheet 3 of 3)

Failure Mode	Effect on System	Detection	Remarks
Output relay mechanically jammed	Loss of system level actuation of one load group	Periodic testing	Other load group available and manual device control fully operable
Output relay fails deenergized	System actuation of one load group	Visual observation of system status	Actuation of one load group

Table 7.3-17

ONE-OUT-OF-TWO-ESFAS
CONTROL ROOM ESSENTIAL FILTRATION ACTUATION SIGNAL
FAILURE MODES AND EFFECTS ANALYSIS (Sheet 1 of 3)

Failure Mode	Effect on System	Detection	Remarks
Loss of one ac load group (diesel)	System isolates	Immediate annunciator	Redundant system actuates
Loss of one dc load group (1E)	System isolates	Immediate annunciator	Redundant system actuates
Loss of instrument air system	System isolates	Immediate annunciator	Closure of control room normal supply dampers
Input sensor fails:			
High	System actuates	Immediate annunciator and periodic testing	Actuation of both load groups
Low	None	Immediate annunciator and periodic testing	Manual actuator available to the operator
Input sensor wiring fails:			
Open	System actuates	Immediate annunciator	Actuation of both load groups

Table 7.3-17

ONE-OUT-OF-TWO ESFAS
CONTROL ROOM ESSENTIAL FILTRATION ACTUATION SIGNAL
FAILURE MODES AND EFFECTS ANALYSIS (Sheet 2 of 3)

Failure Mode	Effect on System	Detection	Remarks
Input sensor wiring fails: (continued)			
Short	Loss of one sensing channel	Periodic testing	Other sensor channel and system level manual actuation available to actuate both load groups
Manual input fails:			
Open	Loss of system level manual initiation of one load group	Periodic testing	Automatic actuation available for both load groups, system level manual actuation available for redundant load group, and manual device level control fully operable
Short	System actuation of one load group	Immediate annunciator	Actuation of one load group

Table 7.3-17

ONE-OUT-OF-TWO ESFAS
CONTROL ROOM ESSENTIAL FILTRATION ACTUATION SIGNAL
FAILURE MODES AND EFFECTS ANALYSIS (Sheet 3 of 3)

Failure Mode	Effect on System	Detection	Remarks
Output relay mechanically jammed	Loss of system level actuation of one load group	Periodic testing	Other load group available and manual device control fully operable
Output relay fails deenergized	System actuation of one load group	Visual observation of system status	Actuation of one load group

The compliance of the ESFAS to the requirements of IEEE 384-1974, "IEEE Trial-Use Standard Criteria for Separation of Class IE Equipment and Circuits," and Regulatory Guide 1.75, "Physical Independence of Electric Systems," is discussed in section 7.1.2.10.

7.3.2.3.3 NSSS and BOP ESF Testing Criteria

IEEE Standard 338-1971 and Regulatory Guide 1.22 provide guidance for development of procedures, equipment, and documentation of periodic testing. The basis for the scope and means of testing are described in this section. Test intervals and their bases are included in the Technical Specifications. The organization for testing and for documentation is described in chapter 13. Since operation of the ESF system is not expected, the systems are periodically tested to verify operability. Complete channels can be individually tested without violating the single failure criterion and without inhibiting the operation of the systems. The system can be checked from the sensor signal through the actuation devices during reactor operation, except as noted below, since most ESF system actuations do not damage equipment or disturb reactor operation. Thus, testing completely simulates valid actuation. Minimum frequencies for checks, calibration, and periodic testing of the ESFAS instrumentation and control are given in the Technical Specifications.

Additional basis documents for NSSS ESFAS and BOP ESFAS testing criteria include CEN-403, Rev. 1 and the companion NRC SER, NRC Letter from B.A. Boger to CEOG, dated 2/27/1996. The SER includes criteria developed from a study NUREG-1366, “Improvements to Technical Specifications Surveillance

Requirements". The study found that while some testing at-power is essential, 1.) safety can be improved, 2.) equipment degradation decreased, and 3.) unnecessary personnel burden can be prevented by reducing the amount of testing at-power. These three conclusions were formed using the following four criteria that were used to justify changes in surveillance test intervals. These same criteria may be used to justify changes in the surveillance test procedures that control at-power or refueling outage testing of ESFAS relays, "actionuation devices" and "actuated equipment". Criterion that may be used with procedure changes supporting the above conclusions are as follows:

- Criterion 1 – The surveillance could lead to plant transient.
- Criterion 2 – The surveillance results in unnecessary wear to equipment
- Criterion 3 – The surveillance results in radiation exposure to plant personnel not justified by the safety significance of the surveillance.
- Criterion 4 – The surveillance places an unnecessary burden on plant personnel because the time required is not justified by the safety significance of the surveillance.

Most ESF relays are tested during power operation along with all actuated equipment. However, some ESF relays tested at-power have equipment that cannot be actuated, but can be racked out, bypassed or otherwise prevented from actuating while the actuation device/relay is being tested at-power. This will not preclude the relay from being tested but will not actuate the locked-out equipment associated with the relay.

These exceptions are controlled within the surveillance procedures and are acceptable given that one or more of the criteria listed above would potentially be challenged by at-power testing of the actuated equipment. In those instances, the actuated equipment will still be tested in accordance with the test bases in judiciously selected groups during refueling outage tests.

Certain ESF subgroup relays are exempt from testing during at-power operation but shall be tested each 18 months in accordance with the Technical Specification SR 3.3.6.2 note. These exemptions are controlled within the surveillance procedures and are acceptable because one or more of the four criterion listed above would be challenged by at-power testing. In those instances, the relays will still be tested in accordance with the test bases in judiciously selected groups during refueling outage tests.

The use of individual trip and ground detection lights, in conjunction with those provided at the supply bus, ensure that possible grounds or shorts to another source of voltage will be detected.

The response time from an input signal to protect system trip bistables through the opening of the actuation relays is verified by measurement during plant startup testing. Sensor responses are measured during factory acceptance tests. Paragraph 7.3.1.1.8.8 provides additional information on response time testing.

7.3.2.4 Failure Modes and Effects Analysis

Refer to CESSAR Table 7.2-5. The failure modes and effects analysis for the additional ESF systems is given in tables 7.3-14 through 7.3-18.

7.3.3 CESSAR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM INTERFACE REQUIREMENTS

The following interface requirements are repeated from CESSAR Section 7.3.3:

The interface requirements discussed below are specific to the ESFAS.

General requirements are discussed in Section 7.1.3. Those items specific to the RPS are discussed in Section 7.2.3.

7.3.3.1 Power

Refer to Section 8.3.

7.3.3.2 Protection from Natural Phenomena

Refer to Sections 3.1.2 and 7.1.3.2.

7.3.3.3 Protection from Pipe Failure

Refer to Section 7.1.3.3.

Table 7.3-18

FAILURE MODES AND EFFECTS ANALYSIS

CONTAINMENT COMBUSTIBLE GAS CONTROL SYSTEM

Failure	Effect on System	Detection	Remarks
Loss of one channel ac control power (motorized valve control)	Loss of redundancy	Immediate--indicator lights	Remaining channel fully operable
Control switch or wiring failure (motorized valve control)			
Open	Loss of redundancy	Periodic testing or spurious operation	Remaining channel fully operable
Short	Spurious operation may occur		Remaining channel fully operable

7.3.3.4 Missiles

Refer to Section 7.1.3.4.

7.3.3.5 Separation

Refer to Section 7.1.3.5.

7.3.3.6 Independence

Refer to Section 7.1.3.6.

7.3.3.7 Thermal Limitations

Refer to Section 7.1.3.7.

7.3.3.8 Monitoring

Refer to Section 7.1.3.8.

7.3.3.9 Operational/Controls

Refer to Section 7.1.3.9.

7.3.3.10 Inspection and Testing

Refer to Section 7.1.3.10.

7.3.3.11 Chemistry/Sampling

Refer to Section 7.1.3.11.

7.3.3.12 Materials

Not applicable to the safety-related instrument and control equipment.

7.3.3.13 System Component Arrangement

Refer to Section 7.1.3.13.

7.3.3.14 Radiological Waste

Refer to Section 7.1.3.14.

7.3.3.15 Overpressure Protection

Refer to Section 7.1.3.15.

7.3.3.16 Related Services

Refer to Section 7.1.3.16.

7.3.3.17 Environmental

Refer to Section 7.1.3.17.

7.3.3.18 Mechanical Interaction

Refer to Section 7.1.3.18.

7.3.3.19 Plant Monitoring System Inputs

Refer to Section 7.1.3.19.

7.3.4 CESSAR INTERFACE EVALUATION

The CESSAR interface requirements listed in subsection 7.3.3 are met by PVNGS design as follows:

7.3.4.1 Power

Refer to subsection 8.3.1.

7.3.4.2 Protection from Natural Phenomena

Refer to paragraph 7.1.4.2.

7.3.4.3 Protection from Pipe Failure

Refer to paragraph 7.1.4.3.

7.3.4.4 Missiles

Refer to paragraph 7.1.4.4.

7.3.4.5 Separation

Refer to paragraph 7.1.4.5.

7.3.4.6 Independence

Refer to paragraph 7.1.4.6.

7.3.4.7 Thermal Limitations

Refer to paragraph 7.1.4.7.

7.3.4.8 Monitoring

Refer to paragraph 7.1.4.8.

7.3.4.9 Operational/Controls

Refer to paragraph 7.1.4.9.

7.3.4.10 Inspection and Testing

Refer to paragraph 7.1.4.10.

7.3.4.11 Chemistry/Sampling

Refer to paragraph 7.1.4.11.

7.3.4.12 Materials

Not applicable

7.3.4.13 System Component Arrangement

Refer to paragraph 7.1.4.13.

7.3.4.14 Radiological Waste

Refer to paragraph 7.1.4.14.

7.3.4.15 Overpressure Protection

Refer to paragraph 7.1.4.15.

7.3.4.16 Related Services

Refer to paragraph 7.1.4.16.

7.3.4.17 Environmental

Refer to paragraph 7.1.4.17.

7.3.4.18 Mechanical Interaction

Refer to paragraph 7.1.4.18.

7.3.4.19 Plant Monitoring System Inputs

Refer to paragraph 7.1.4.19.

7.3.5 DIVERSE AUXILIARY FEEDWATER ACTUATION SYSTEM (DAFAS)

The DAFAS monitors plant conditions and actuates auxiliary feedwater during conditions indicative of an ATWS event and S/G low level conditions. The DAFAS interfaces with the process protective cabinets(PPC), the auxiliary relay cabinet (ARC), and the diverse scram system (DSS). The interface with the DSS is accomplished through a connection with the supplementary protection system (SPS) trip signal in the Class 1E portions of the electronic isolation system (EIS).

There are two channels of DAFAS, train A and train B. The two DAFAS channels are independent and isolated from each other as well as from the interfacing systems noted above by the use of fiber optic data links.

A DAFAS block diagram is shown in figure 7.3-7e.

7.3.5.1 Design Bases and Design Considerations

The PVNGS DAFAS is designed to be a highly reliable system that initiates auxiliary feedwater flow upon conditions indicative of an ATWS combined with selective low S/G level signals. DAFAS will stop AFW flow to the affected S/G after reaching a predetermined level setpoint (about 30 minutes after actuation) at which time manual operator intervention will control the system. The DAFAS is designed to meet the intent of 10CFR50.62 and is diverse and independent from the existing reactor protective system. The DAFAS design further complies with NRC guidance provided with 10CFR50.62 and the quality assurance requirement of Generic Letter 85-06. Compliance with the guidelines are integrated into the design for PVNGS DAFAS as discussed below.

7.3.5.1.1 Safety Related (IEEE-279)

The DAFAS is not required to be safety related. However, the implementation of DAFAS is such that the existing protection system continues to meet all applicable safety related criteria.

The DAFAS consists of several equipment groups. The DAFAS sub-assembly in the process protective cabinets (J-SBA-C02A, J-SBB-C02A, J-SBC-C02A and J-SBD-C02A), the DAFAS cabinets (J-SAA-C05 and J-SAB-C06), the DAFAS sub-assembly in the auxiliary relay cabinets (J-SAA-C01 and J-SAB-C01), and the DAFAS sub-assembly in the electronic isolation system (EIS) cabinets (J-SAA-C04, J-SAB-C04, J-SAC-C04 and J-SAD-C04). The DAFAS equipment in the PPC, ARC and EIS cabinets are considered safety related equipment since they interface directly with class 1E systems. The DAFAS equipment in the existing 1E cabinets are designed, constructed, and installed in accordance with the requirements for PVNGS safety related equipment.

The DAFAS cabinets are considered safety related. They are designed, constructed, and installed in accordance to the requirements for PVNGS safety related equipment which exceeds requirements of 10CFR50.62. However, the DAFAS does not have a manual trip and utilizes the manual trip capability of the existing AFAS. PVNGS has elected to classify the DAFAS as a safety related system to provide enhanced operability and availability.

The DAFAS power supplies that power the fiber optic transmitters (FOTs) and receivers (FORs) are grounded. The justification for the grounding of the power supplies is discussed below.

IEEE-279 requires that each redundant channel of a safety system be independent from its redundant counterpart. Independence is measured by the ability of a redundant system to perform its function when confronted by a credible "single failure." The single failure, if it compromises the function of the safety system, must be able to be detected by periodic testing. From these criteria, it can be seen that grounding the power supply that powers the fiber optic transmitters and receivers does not compromise the independence of the DAFAS. Postulated single failures, that are credible for the DAFAS in terms of fault voltage and energy, will, at worst, cause a channel failure that is either self annunciating or detectable during periodic testing. There is no failure or fault in the DAFAS that prevent the system from performing its intended function.

7.3.5.1.2 Redundancy

Redundancy alone does not preclude common mode failure occurrences. Therefore, there are no requirements for redundancy of the DAFAS. However, the system should be reliable and minimize the possibility of spurious actuation. PVNGS has elected to install a two train DAFAS for PVNGS units 1, 2, and 3 to increase system reliability and decrease the probability of spurious actuation. The installation of a two train system also permits testing at full power, allowing the remaining DAFAS channel to provide a measure of protection.

7.3.5.1.3 Physical Separation From Existing Reactor Protective System

DAFAS physical separation from existing reactor protective system is not required unless redundant divisions and channels in the existing reactor protective system are not physically separated. The DAFAS implementation must be such that separation criteria applied to the existing protection system are not violated.

DAFAS physical separation from the existing PPS is provided. The DAFAS is isolated via qualified fiber optic devices and is physically and electrically separate from the existing PPS. The DAFAS does not degrade the existing separation criteria of the PPS or the ARC cabinets. Physical separation is maintained and electrical protection is provided for the channel (division) A,B,C and D vital instrument busses providing power to the DAFAS ARC control panel assemblies. The DAFAS ARC control panels are part of the train (division) A or B ARC in which they are located. The required isolation is provided by the circuit breakers in the ARC. These isolation devices have been evaluated as acceptable per IEEE-384, 1981, by calculation 13-JC-SA-202.

7.3.5.1.4 Seismic Qualification (IEEE-344)

The DAFAS equipment mounted inside the PPC, EIS and ARC cabinets are tested and qualified to meet or exceed the seismic qualification criteria of the existing cabinets so that the qualification of the existing safety related cabinets remain valid. Although the DAFAS system is not required to be Class 1E qualified, the DAFAS equipment will be constructed and mounted consistent with the existing requirements of PVNGS Class 1E

safety related equipment. DAFAS equipment will be tested and qualified in accordance with IEEE-344, 1975 to enhance the system performance and reliability.

7.3.5.1.5 Environmental Qualification (IEEE-323)

The DAFAS equipment is not located in a harsh environment. Therefore, environmental qualification requirements of 10 CFR 50.49 are not applicable. However, the equipment inside the DAFAS cabinets and the DAFAS equipment housed inside the PPC, ARC and EIS cabinets will be qualified for the environmental conditions inside the cabinets resulting from AOO's. The environmental qualification is in accordance with IEEE-323, 1974.

7.3.5.1.6 Quality Assurance For Test, Maintenance And Surveillance

Compliance with Generic Letter 85-06 is addressed in section 7.3.5.1.12. Testing, maintenance and surveillance are addressed in section 7.3.5.1.8. below.

7.3.5.1.7 Safety Related Power Supply

The power required to operate the DAFAS is provided by the following sources:

- Two Class 1E 120 VAC vital instrument buses Channel A to the DAFAS A cabinet and Channel B to the DAFAS B cabinet.
- The four existing cabinet Class 1E power sources (A, B, C and D) in the EIS, PPC and ARC.

The power required for the DAFAS cabinets and the DAFAS sub-assembly mounted inside the ARC cabinets is supplied from the 120 VAC vital instrument buses. The 120 VAC vital buses are required to supply power to its respective DAFAS equipment channel. The power required for the DAFAS sub-assembly mounted inside the EIS cabinets is supplied by the existing 24 VDC power supplies in the EIS cabinets. The use of existing DC power supplies was considered to minimize the space required for interfacing with the existing plant equipment. In such cases, a load calculation was performed to verify that the additional load required by the DAFAS would not cause an overload condition to exist.

Power supply faults such as over-voltage and under-voltage conditions, degraded frequencies, and over-current will not compromise the RPS, AFAS or safety related equipment in the ARC cabinets. Loss-of-power to a DAFAS train will cause the "DAFAS Trouble" alarm in the control room. The vital 120 VAC system faults are alarmed in the control room along with battery charger and inverter faults. The control room alarms provide for early detection of degraded voltage and frequency conditions to allow for operator corrective action while the affected circuits/components are still capable of performing their intended functions.

7.3.5.1.8 Testability At Power

The DAFAS provides for both on-line and off-line testing. The on-line testing of the system is performed one train at a time, and is manually initiated at the DAFAS, and the Auxiliary Relay Cabinets.

The DAFAS cabinet testing involves testing the logic system. Testing at the ARC cabinets involves verifying proper operation of the DAFAS circuitry and the initiation relays. The DAFAS total functional testing and calibration will be performed prior to operation to demonstrate that the hardware and software conform to the design specifications. The DAFAS equipment will be periodically tested and calibrated to ensure that the testing requirements established by PVNGS are satisfied. The measuring and test equipment which will be used to determine the DAFAS functionality will be controlled in accordance with existing procedures. A system level test will be conducted each refueling outage, which will consist of functional testing from the sensor output to and including the DAFAS initiation relays. This test will include a check of the input calibration, simulating the inputs, verifying DAFAS initiations, bypasses and alarms.

Maintenance and test bypasses for the DAFAS will not involve installing jumpers, lifting leads, pulling fuses or other circuit modifications. The test bypasses will be provided as an integral part of the DAFAS design.

7.3.5.1.9 Diversity From Existing Reactor Protective System (RPS)

The equipment used in the design of the DAFAS is entirely diverse from the existing PPS (plant protection system) except for the S/G level sensors and the final actuation devices, both of which are not required to be diverse in accordance with the ATWS Rule and guidance. The DAFAS uses programmable logic controllers with solid state I/O modules as compared to the PPS which uses analog bistable trip units to perform the same

function. The DAFAS uses fiber optic communication links to receive and transmit signals to and from its distributed DAFAS subsystems.

The DAFAS final interface devices with the AFAS are the DAFAS initiation relays located on the DAFAS ARC control panel assemblies in the auxiliary relay cabinet. These relays energize to actuate auxiliary feedwater flow while the existing AFAS is a de-energize to actuate system. These relays are of a different manufacturer from the existing PPS/RPS initiation relays, and their use, therefore, is diverse from the existing RPS. The DAFAS and AFAS use the same final actuation devices. The final actuation devices are the existing cycling and subgroup relays used to control the pumps and valves in the auxiliary feedwater system.

7.3.5.1.10 Electrical Independence From Existing Reactor Protective System

The power required to operate the DAFAS is provided by Class 1E power sources which are independent channelized sources. The DAFAS logic is isolated from the auxiliary relay cabinet logic, process protective cabinets, and electronic isolation system cabinets through the use of fiber optic isolation which meets the intent of the guidance for isolation between safety related circuits. The NRC has accepted this configuration to be in compliance with the intent of the ATWS Rule (reference 1).

7.3.5.1.11 Inadvertent Actuation

The DAFAS is designed with features to minimize inadvertent actuations and challenges to the safety system. The DAFAS actuation setpoint is set at a level below the existing AFAS

setpoint in the PPS and the DAFAS response time will be longer than the PPS AFAS response time in order to prevent the possibility of the DAFAS initiating auxiliary feedwater (AFW) flow before the properly operating PPS. The DAFAS initiates AFW flow upon energizing the DAFAS initiation relays while the AFAS initiates AFW flow upon de-energizing the PPS initiation relays. Both signals deenergize the AFW subgroup and cycling relays. The energize-to-actuate design of the DAFAS initiation relays minimizes relay power failures or I/O system power failures from causing an inadvertent actuation since these relays are normally de-energized.

The DAFAS is blocked by AFAS-1 or AFAS-2 signals, if the DAFAS has not actuated since this would indicate normal protection system operation and therefore no need for this ATWS mitigation system actuation. If DAFAS actuates before an AFAS, the DAFAS protection signal will go to completion as required by IEEE-279, unless blocked by an MSIS. The MSIS signals will block a DAFAS actuation prior to, during or after a DAFAS actuation in order to prevent interference with the MSIS capability for S/G high energy line break protection. When the PPS initiates AFAS or MSIS, indicating that PPS is operating normally and that conditions for an ATWS do not exist, blocking logic is activated which disables the DAFAS initiation relay. The DAFAS is further blocked until a selective 2/4 diverse scram system (DSS) logic matrix is satisfied, such that the DAFAS can operate only if a DSS actuation is in progress.

If an inadvertent actuation of the DAFAS were to occur, thus initiating AFW flow, an increase in feedwater flow to the steam generator secondary side could result. Although undesirable,

this event has been considered in the analysis of the plant in section 15.1.2, Increase in Feedwater Flow.

7.3.5.1.12 Conformance to Generic Letter 85-06

Generic Letter 85-06 was issued by the NRC to provide explicit quality assurance (QA) guidance required for non-safety related ATWS equipment. The PVNGS DAFAS is in compliance with the QA guidance of this generic letter by invoking on PVNGS the requirements of a 10CFR50, Appendix B, QA program on the DAFAS and its equipment.

7.3.5.1.13 Conformance to ANSI 45.2.11

The DAFAS was designed in accordance with the PVNGS configuration management program. In addition, ABB-Combustion Engineering (ABB-CE) support was performed in accordance with the ABB-CE Quality Assurance Manual (QAM-100) which complies with ANSI/ASME NQA-1-1983 which is based on the contents of ANSI/ASME N45.211-1977

7.3.5.1.14 Conformance to 10CFR50, Appendix A

The DAFAS is designed in compliance with the applicable criteria of the NRC, "General Design Criteria for Nuclear Power Plants," 10CFR50 Appendix A.

7.3.5.1.15 Conformance to 10CFR50, Appendix B

The DAFAS was designed in accordance with the PVNGS configuration management program. In addition, ABB-CE provided support using their quality assurance program (QAM-100) and is in compliance with the NRC, "Quality Assurance criteria for

Nuclear Power Plants and Fuel Reprocessing Plants," 10CFR50, Appendix B.

7.3.5.1.16 Conformance to Regulatory Guide 1.75

The DAFAS design is in compliance with the "Physical Independence of Electrical System", Regulatory Guide 1.75.

7.3.5.1.17 Conformance to Regulatory Guide 1.22

The DAFAS is in compliance with Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Function", in conjunction with the current AFAS actuation devices.

7.3.5.1.18 Conformance to Regulatory Guide 1.53

The DAFAS is in compliance with Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection System."

7.3.5.1.19 Conformance to IEEE-338, 1971

The DAFAS system testing conforms to the IEEE-338 Standard, "Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems."

7.3.5.1.20 Conformance to IEEE-384

The DAFAS fiber optic and internal module connection wiring conforms to IEEE-384, 1981, "Criteria for Independence of Class 1E Equipment and Circuits." The interfaces with the DAFAS in the PPC, EIS and ARC are also in compliance with this standard.

7.3.5.1.21 Conformance to IEEE-379

The DAFAS is in compliance with the applicable criteria of IEEE-379, 1977, "Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E System."

7.3.5.2 Functional Description of the DAFAS

The DAFAS actuation mitigates the consequence of an ATWS event. This consequence is high RCS pressure due to reduced heat removal through the S/Gs. The DAFAS actuation is provided following an ATWS, which is characterized as an Anticipated Operational Occurrence (AOO) requiring auxiliary feedwater, coincident with a failure of the PPS to initiate a reactor trip. Failure of the PPS is indicated by a reactor trip initiated on high-high pressurizer pressure by the supplementary protection system (SPS), also known as (AKA) the supplementary protection logic assemblies (SPLA), AKA the diverse scram system (DSS). The DAFAS initiation signals cause actuation of the auxiliary feedwater systems (train A and B) only if there is a demand for auxiliary feed as indicated by low S/G level, and there is an SPS initiated reactor trip, and there is no MSIS and an AFAS-1 or -2 has not been generated by the PPS. Indication of an MSIS or an AFAS in the PPS concurrent with the absence of an enable from the DSS indicates that conditions indicative of an ATWS have not occurred and the DAFAS actuation is not necessary. Therefore, under these conditions the DAFAS actuation will be blocked through DAFAS logic in the auxiliary Relay Cabinets.

7.3.5.2.1 DAFAS Input

The DAFAS uses four existing wide range safety channels (A,B,C and D) level sensor inputs from each of the two steam generators at the process protective cabinets (PPC) JSBA-C02A, JSBB-C02A, JSBC-C02A and JSBD-C02A. Each of the DAFAS channels (A and B) receive these eight steam generator level inputs. These level signals are input to a fiber optic transmitter (FOT) which converts the analog voltage signal to an optical signal. The optical signals are then split by fiber optic splitters (FOS) for transmission to both of the DAFAS cabinets over FO cables. These fiber optics communications links provide the required isolation between the PPC signals (Divisions A, B, C, D) and the DAFAS (Divisions A and B).

Similarly, each DAFAS train also receives indication of the four DSS trip inputs from the four channels A, B, C, and D of the SPS via FO cables. Channels A, B, C and D of the EIS (cabinets J-SAA-CO4, J-SAB-CO4, J-SAC-CO4 and J-SAD-CO4) each contains a FOT and a FOS to transmit the associated DSS permissive signals to each DAFAS train. These signals are input to the digital input modules (DIM's) and the selective two-out-of-four logic is performed by the PLC. Channels A and B of the EIS also contain two FOR modules per channel to receive the status of the respective DAFAS train. One FOR carries the TRIP information while the other contains TEST/TROUBLE status. These signals are transmitted to the plant annunciator via the EIS. These fiber optics communications links provide the required isolation between the EIS signals (Divisions A, B, C, D) and the DAFAS (Divisions A and B).

In the ARC (J-SAA-C01 and J-SAB-C01) the DAFAS logic solvers read status of the relays in the ARC through FO links from the I/O systems located within the ARC. These inputs include AFAS and MSIS cycling relay status, initiation relay status, and bypass relay status. The logic solver output logic controls the DAFAS initiation and bypass relays. Isolation between divisions is provided in the ARC by similar (to the EIS and PPC) fiber optic communications links. And for the power systems, the DAFAS is isolated by use of circuit breakers on the vital bus feeder cables.

7.3.5.2.2 DAFAS Logic

Each of the two DAFAS cabinets (J-SAA-C05 and J-SAB-C06) contains the logic for one DAFAS train. Each train consists of F.O. receiver (FOR) modules, F.O. modems (FOM), fiber optic transmitter (FOT) modules, power supplies, the status and test panel or man machine interface (MMI), I/O modules, and two programmable logic controllers (PLC). Each of the DAFAS cabinets contains eight FOR modules that convert the optical input signals from the PPC FOT modules to analog voltage signals. The eight (8) analog signals are sent to input modules for the two PLC systems, which perform the logic to determine if conditions for a DAFAS initiation exist. The FOR modules contain a fault indicator LED and contact output that is activated upon loss of the optical signal (e.g. severed F.O. cable). This fault indication is provided to assist in troubleshooting problems that may be encountered with the input signals. The isolated analog input signals (0-5 VDC) are directed to analog input modules where analog to digital (A/D) conversion is performed. Digitized analog values are

automatically reported to the PLC upon interrogation during each PLC scan cycle. Analog input modules include self test and auto calibration features to minimize the need for periodic calibration of inputs. The converted analog values are compared to the low S/G level setpoint in the PLC processor. The PLC generates a DAFAS-1 or DAFAS-2 initiation signal when the setpoint is exceeded, provided the requisite permissives and block conditions previously discussed are satisfied.

Four DSS trip permissive signals, channels A, B, C, and D are received by digital input modules (DIM's) from the EIS. The DAFAS then performs the same selective two-out-of-four logic that is performed by the DSS supplementary protection logic assembly (SPLA). The DAFAS trip output signal is disabled if the DSS logic indicates DSS has not actuated.

The DAFAS PLC outputs are set up as a two-out-of-two logic system where a DAFAS signal from both PLCs is required to initiate auxiliary feedwater flow. Each PLC provides a trip signal to one of the two AFAS trip legs of each ARC. Putting one of the channels into test will not result in initiating feedwater flow as a DAFAS signal from both PLCs is required to cause feedwater flow and the bypass relay contact is enabled prior to cycling each leg's initiation relay by the automated test features in the MMI. A DAFAS signal from one of the PLCs results in only one ARC trip leg, 1-3 or 2-4, to be tripped. However, both trip legs are required to be tripped in order to drop out the subgroup relays resulting in feedwater flow.

The DAFAS initiation signals cause actuation of the feedwater pumps and valves only if there is a demand for auxiliary feedwater and an AFAS or MSIS has not been generated. The occurrence of AFAS without the DSS enable indicates that

conditions indicative of an ATWS have not occurred and DAFAS actuation is not necessary. Under these conditions, DAFAS actuation is blocked by AFAS through logic in the ARC's.

DAFAS will also be blocked by a MSIS to prevent undesired interactions during non-ATWS events when conditions for a MSIS exist. The MSIS signals initiate isolation of each steam generator to rapidly terminate blowdown and feedwater flow if a high energy line rupture occurs. The MSIS block of DAFAS is done to minimize interference with this type event by preventing DAFAS initiated auxiliary feedwater flow.

The overall logic is shown in figure 7.3-7f.

7.3.5.2.3 DAFAS Output

The auxiliary relay cabinet (ARC) DAFAS equipment includes four I/O systems, two interfacing with DAFAS A (PLC-A1 and PLC-A2) and two with DAFAS B (PLC-B1 and PLC-B2). The I/O systems consist of FOMs, high speed logic solver (HSLS) assemblies with a discrete input and output capacity, initiation relays, bypass relays and power supplies. The I/O systems are located in Bay 5 and Bay 8 of each ARC. The I/O systems receive inputs from the DAFAS cabinet through a serial F.O. data link. The HSLS then generates discrete outputs which control the DAFAS-1 and DAFAS-2 initiation and bypass relays. The bypass relays may be activated through the HSLS using a key-lock switch or by the MMI during a manually initiated automated test. The I/O system also acquires inputs and makes them available to be read by the PLC through the serial data link. The inputs include AFAS-1, AFAS-2, MSIS, as well as initiation and bypass relay status.

DAFAS initiation demand is directed to the ARC via RS-232 F. O. data links. The data links are supported by ASCII/Basic modules in the PLC chassis. The trip demand is received by the HSLS which energizes the initiation relay thereby interrupting power to the existing 1-3 or 2-4 trip paths. These HSLS also accept AFAS and MSIS actuation status signals from the ARC logic to block a DAFAS actuation as required.

7.3.5.3 DAFAS Diversity From Existing Reactor Protective System

Refer to Section 7.3.5.1.9

7.3.5.4 Failure Modes and Effects

As previously discussed, the DAFAS is designed to be a highly reliable system and the equipment used in the system will be qualified to the requirements of PVNGS Class 1E safety related equipment. The qualification includes seismic, environmental, electro-magnetic interference (EMI) and fault testing. The DAFAS design includes circuits that allow the plant operators to periodically test the overall operational status of the system. Controls and indicators located on the DAFAS test and control panel permit actuation of one train at a time to demonstrate the functionality of the components in that train. Any failures of the DAFAS will be detected during periodic testing of the system.

The provisions inherent in the DAFAS design which compensate for component failures include the following:

- The redundancy provided by the four S/G level signal paths which permit the system to still function in the event of a channel failure.

- The redundant PLCs within each DAFAS channel. Two-out-of-two ARC initiation logic which minimizes inadvertent operation of the system and is compatible with the existing ARC logic scheme in the event of a spurious actuation signal.
- Power is required for the energize-to-actuate DAFAS initiation relays. Therefore, the relay and the system are normally in a similar mode to the failure mode, which is consistent with the ATWS guidance.
- There is an interlock between the DAFAS and the AFAS which prevents activation of the DAFAS if the AFAS has been activated.
- There is a selective two-out-of-four permissive signal from the DSS which enables the DAFAS for a condition of abnormally high RCS pressure.
- There is a DAFAS inhibit on a MSIS which prevents actuation of the DAFAS in the event of a S/G high energy line break.

The DAFAS is designed so that any single failure within the system will not prevent protection action at the system level. No single failure will defeat more than one of the two DAFAS trains. The failure modes analyzed for the design of the DAFAS include DAFAS initiation relay failure to actuate, and DAFAS inadvertent actuation. These failure modes are discussed below.

7.3.5.4.1 DAFAS Initiation Relay Failure to Actuate

A failure to actuate either a train A or train B DAFAS initiation relay (mounted in the ARC cabinets J-SAA-C01 or J-SAB-C01) could be caused by the following component failures:

- Failure of the fiber optic modems or cables used for transmitting input and output signals to the DAFAS cabinets.
- Failure of one of the programmable logic controllers (PLC) or supporting equipment located in either one of the two DAFAS cabinets.
- Failure of one of the HSLS modules located in the ARC cabinets.

A single failure described above could result in disabling one of the two DAFAS trains. Each of the two DAFAS trains is capable of performing the intended function of the system. The DAFAS initiation relay which is added to the ARC cabinets has its output contact located in series with a string of relay contacts. These contacts are normally held closed and open to initiate auxiliary feedwater flow. The added DAFAS relay contacts are closed when the relay is not energized. The failures with the highest probability for one of the DAFAS trains would leave the DAFAS relay in the de-energized state (contacts closed) and thereby have no effect on the normal operation of AFAS, nor would this cause an inadvertent actuation of auxiliary feedwater flow. Therefore, the postulated failure is in a safe direction.

7.3.5.4.2 DAFAS Inadvertent Actuation

As discussed in section 7.3.5.1.11, the DAFAS is designed with features to minimize inadvertent actuations. However, per the Standard Review Plan (NUREG 0800 Sections 7.1, 7.3 and 7.7) and IEEE-279 and IEEE-379, it is required to assume the DAFAS will fail to a mode which will result in a DAFAS actuation signal at the system level.

If an inadvertent actuation of the DAFAS were to occur, thus initiating auxiliary feedwater flow, an increase in feedwater flow to the steam generator secondary side could result. Although this event has been considered in the analysis of the plant (section 15.1.2, Increase in Feedwater Flow), it is undesirable, and the addition of another auxiliary feedwater initiation system will increase the probability of the occurrence of the event. However, the number of system interlocks has provided sufficient protection from inadvertent actuation. The NRC has concluded in a Safety Evaluation (reference 1) that this design is acceptable.

7.3.6 REFERENCES

1. Letter from S. R. Peterson, NRC, to W. F. Conway, APS, dated October 18, 1990, "Compliance With the Anticipated Transients Without Scram (ATWS) Rule, Palo Verde Nuclear Generating Station (PVNGS) Units 1, 2, and 3 (TAC NOS. 59124, 62698, 67168)."
2. CENPD-182, "Seismic Qualification of Instrumentation and Electrical Equipment", Combustion Engineering, Inc.
3. CENPD-255, "Qualification of Combustion Engineering Class IE Instrumentation", Combustion Engineering, Inc.
4. CENPD-210A, "Description of the C-E Nuclear Steam Supply System Quality Assurance Program", Combustion Engineering, Inc.
5. CENPD-148 "Review of Reactor Shutdown System (PPS Design) for Common Mode Failure Susceptibility", Combustion Engineering, Inc.

This page intentionally blank

7.4 SYSTEMS REQUIRED FOR SAFE SHUTDOWN

A listing of systems fulfilling the functional requirements for safe shutdown in the event of a fire (per 10CFR50, Appendix R) is provided in appendix 9B.

The instrumentation and control functions which are required to be aligned for maintaining safe shutdown of the reactor are discussed in this section. These functions will permit the necessary operations that will:

A. Prevent the reactor from achieving criticality in violation of the Technical Specifications.

B. Provide an adequate heat sink such that design and safety limits are not exceeded.

7.4.1 DESCRIPTION

The following systems are required for safe shutdown of the reactor:

- Auxiliary feedwater system (AFS) (paragraph 7.4.1.1.6)
- Atmospheric steam dump system (ASDS) (paragraph 7.4.1.1.7)
- Shutdown cooling system (SCS) (paragraph 7.4.1.1.8)
- Chemical and volume control system (CVCS), boron addition portion (paragraph 7.4.1.1.9)
- Condensate storage system (CSS) (subsection 9.2.6)

The following auxiliary support systems are also required to function.

- Essential spray pond system (ESPS) (subsection 9.2.1 and paragraph 7.4.1.1.4)
- Essential cooling water system (ECWS) (subsection 9.2.2 and paragraph 7.4.1.1.5)
- Onsite power system (OPS) (paragraph 8.3.1.1.2), including diesel generator systems (DGSs) (subsections 9.5.4 through 9.5.8 and paragraph 7.4.1.1.1)
- Heating, ventilating, and air conditioning (HVAC) systems (sections 6.4 and 9.4)

7.4.1.1 System Description

7.4.1.1.1 Emergency Generators

Two independent, 100% capacity diesel generators provide a dependable onsite power source capable of starting and supplying the essential loads necessary to shut down the plant safely and to maintain it in a safe shutdown condition under loss of offsite power (LOP) conditions (voltage degradation to the 4.16 kV ESF bus). Load sequencers are provided to sequentially load the diesel generators and are a part of the engineered safety features (ESF) system actuation.

The diesel generators are started automatically by a loss of offsite power (LOP), by an auxiliary feedwater actuation signal (AFAS), by a safety injection actuation signal (SIAS), or by a containment spray actuation signal (CSAS). All are DG emergency mode starts with the exception of CSAS, which starts the DG in test mode. A LOP also initiates automatic load sequencing of the diesel generators.

The actuation system instrumentation and controls for the diesel generators are described below. Refer to paragraph 8.3.1.1.3 for a description of the ESF power system, including automatic load shedding and load sequencing. Paragraph 8.3.1.1.4 describes the standby power supply (diesel generator) and the diesel generator starting system is described in subsection 9.5.6. Additional information on diesel generator supporting auxiliaries may be found in subsections 9.5.4, 9.5.5, 9.5.7, and 9.5.8.

A. Sensors

The undervoltage monitors consist of four sensor circuits for each 4.16 kV ESF bus. The components and operation of the undervoltage monitors are described in section 8.3.1.1.3.13, subsection B.

The sensors for AFAS, CSAS and SIAS signals are described in section 7.3.

B. Initiating Circuits and Logic

The undervoltage starting signal (LOP) for the diesel generators is produced by coincidence of two-out-of-four trip of the undervoltage sensors described in section 8.3.1.1.3.13, subsection B.

There is no time delay in initiating start of the diesel generator for loss of offsite power except for an inverse time response lag and delayed time lag provided in the undervoltage monitors. Manual starting control also is provided at the diesel generator and in the control room to facilitate testing.

C. Interlocks and Bypasses

The various interlocks and actuation bypasses built into the diesel generator system are presented in paragraphs 8.3.1.1.4.4 and 8.3.1.1.4.5, respectively.

D. Redundancy

Redundant sensing with two-out-of-four coincidence logic and control is provided for diesel generator automatic actuation. Independent actuation is provided so that each diesel generator is started by its own actuation system.

E. Actuated Devices and Automatic Load Sequencing System

The actuated devices for automatic diesel generator starting are the diesel air starting solenoid valves.

In the event that diesel generators are required to power ESF or safe shutdown loads, sequential loading must be employed to avoid diesel generator overloading. Loads to be supplied and the loading sequences are described in subsection 8.3.1.

Diesel generator load sequencing is actuated when the diesel generator output breakers close. The signal to close the diesel generator output breaker is blocked by circuit breaker interlocks that are provided to prevent automatic closing of a diesel generator breaker to an energized or faulted bus. A faulted bus is detected by inverse time overcurrent relays in the main feeder circuits of each 4.16 kV ESF bus. A sequencer is provided for

each load group. The sequencer loads safe shutdown and ESF equipment onto the ESF bus so that essential loads are started within the time limits specified in Table 8.3-3.

Undervoltage trip outputs are delayed in accordance with the inverse time characteristics of the loss of voltage relays and the discrete time delay setting of the degraded voltage relays. These relays are used to confirm that a power failure has occurred. The time delays prevent spurious diesel generator actuation.

Undervoltage on the ESF bus trips all bus load automatically. After the diesel generator attains rated speed and voltage, its own circuit breaker is ready to close automatically without delay, but automatic or manual closure is blocked whenever an ESF bus fault exists. A diesel generator breaker closed signal starts the loading sequence.

Redundant actuation and control are provided for diesel generator automatic load sequencing in that each load group is provided with its own independent automatic load sequencing system. The time at which energization of the various loads is permitted by the automatic ESF load sequencers is given in table 8.3-3. The automatic ESF load sequencing system is supported by independent 120V vital ac and Class 1E 125 V-dc sources described in paragraphs 8.3.1.1.6 and 8.3.2.1.2. The automatic load sequencing system logic is shown in figure 8.3-1.

7.4.1.1.1.1 Design Bases Information. The design bases for the diesel generator automatic load sequencing are the emergency power source requirements listed in subsection 8.3.1.

Design bases for diesel generator automatic actuation are listed in paragraph 8.1.4.2.

The diagrams used to support the design bases are given by the following:

- Logic diagram, figure 8.3-1
- P&I diagram, 01, 02, 03-M-DGP-001
- Electrical one-line diagram, 13-E-MAA-001 and 01, 02, 03-E-MAA-002

7.4.1.1.2 Emergency Generator Fuel Oil Storage and Transfer System

The controls and instrumentation for this system are discussed in paragraphs 9.5.4.3 and 9.5.4.6. The diagrams used to support the design bases are given by the following:

- Logic diagram, figure 7.4-1
- P&I diagram, 01, 02, 03-M-DFP-001

7.4.1.1.3 Class 1E AC System

This system is described in paragraph 8.3.1.1.3.

7.4.1.1.4 Essential Spray Ponds System

The controls and instrumentation for this system are discussed in paragraphs 9.2.1.6 and 9.2.1.9. The diagrams used to support the design bases are given by the following:

- Logic diagram, 01, 02, 03-M-SPP-001

- P&I diagram, figure 9.2-1

7.4.1.1.5 Essential Cooling Water System

The controls and instrumentation for this system are discussed in paragraphs 9.2.2.1.6 and 9.2.2.1.9. The diagrams used to support the design bases are given by the following:

- Logic diagram, figure 7.4-3
- P&I diagram, 01, 02, 03-M-NCP-001, -002 and -003

7.4.1.1.6 Auxiliary Feedwater System (Emergency Feedwater System) and Condensate Storage System

The safe shutdown features of these systems are discussed in subsections 10.4.9 and 9.2.6, respectively. The controls and instrumentation for the auxiliary feedwater system are discussed in paragraph 7.3.1.1.10.7. The diagram used to support the design bases are given by the following:

- Logic diagram, figure 7.4-4
- P&I diagram, 01, 02, 03-M-AFP-001 and 01, 02, 03-M-CTP-001

7.4.1.1.7 Atmospheric Dump System

The atmospheric dump valves are discussed in subsection 10.3.2. The valves are located outside the containment upstream of the main steam isolation valves.

The valves are used to remove decay heat from the steam generator in the event that the main condenser is unavailable for service for any reason, including a loss of ac power. The decay heat is dissipated by venting steam to the atmosphere. In this way, the reactor coolant system (RCS) can either be

maintained at hot standby conditions or cooled down. The system instrumentation and controls for the atmospheric dump valves are described below and are shown on in engineering drawings 01, 02, 03-M-SGP-002 and -001.

A. Initiating Circuits and Logic

There are no automatic initiating circuits for operation of the atmospheric dump valves.

The atmospheric dump valves are positioned manually by a controller (manual loading station) from either the main control room or the remote shutdown panel as part of the capability for emergency shutdown from outside the control room (see Section 7.4.1.1.10). Each valve has two separate permissive control circuits. Valve position indication is provided at each remote control station. A handwheel is also provided with the atmospheric dump valve for hand operation.

B. Bypasses, Interlocks, and Sequencing

No bypasses, interlocks, or sequencing are provided for the atmospheric dump valves.

C. Redundancy

Atmospheric dump valves are provided to maintain the reactor at hot standby or to initiate a plant cool-down. Two redundant atmospheric dump valves are provided for each steam generator, one per main steam line. However, in the event of failure of these valves, reactor decay heat will be removed through the main steam line safety valves, which will be opened when pressure in the steam generator reaches the pressure relief setpoint. Steam release will continue until the pressure is reduced to the safety valve reset pressure. The safety valves will

continue to cycle in this manner as steam generator pressure rises and is relieved. The RCS will remain at hot standby conditions during this pressure relief cycling. Cooldown of the reactor coolant can be accomplished through remote manual operation of the atmospheric dump valves. Each valve has a handwheel that can be operated locally.

D. Design Bases

1. Refer to section 10.3 for design bases for the atmospheric dump valves.
2. The two separate permissive control circuits are designed to IEEE Standards 279-1971 and 308-1974. This ensures that no single failure of the control circuits will cause a spurious opening of a valve or prevent the operation of at least one atmospheric dump valve on each steam generator.
3. The operation of the atmospheric dump valves is considered in determining the release of iodine due to steam escaping from the dumps during cooldown.

7.4.1.1.8 Shutdown Cooling System

The Shutdown Cooling System (SCS) and its interface requirements are discussed in section 5.4.7. The SCS instrumentation and control necessary to achieve cold shutdown are discussed below. The logic and piping are shown on Figure 7.4-6 and engineering drawings 01, 02, 03-M-SIP-001, -002 and -003.

7.4.1.1.8.1 Initiating Circuits And Logic. The SCS is designed to be manually initiated upon the attainment of the required Reactor Coolant System (RCS) conditions of temperature (less than 350°F) and pressure (less than 400 psia). The SCS valve interlocks are discussed in Section 7.6; they prevent overpressurization of the low pressure portion of the system.

Control board process indication and status instrumentation is provided to enable the operator to determine system status, to evaluate system performance, and detect malfunctions. Control panel hand switches and valve position limit indication lights are provided for the isolation valves and the heat exchanger inlet, outlet, and bypass valves. Indication is provided of Low Pressure Safety Injection (LPSI) pump discharge header pressure and temperature, heat exchanger outlet temperature, and shutdown cooling injection flow and pressure. LPSI pump operating status is also indicated on the control board.

7.4.1.1.8.2 Interlocks, Sequencing And Bypasses. The SCS has overpressure protection interlocks as discussed in Section 7.6.

The system sequencing will be in approved operating procedures provided by the Applicant for the manually controlled equipment. There are no bypasses in the SCS instrumentation which would jeopardize the protection afforded by the interlocks.

7.4.1.1.8.3 Redundancy And Diversity. Each of the two SCS trains has sufficient instrumentation to assure adequate monitoring during all modes of operation. The isolation valves are discussed in Section 7.6.

7.4.1.1.8.4 Supporting Systems. The SCS has four independent power supplies for the SCS Isolation Valve Interlocks. Pumps, valves, etc. are required to be capable of being powered by the normal 1E and emergency power sources.

Also, refer to UFSAR section 7.6.1.1.1 for SCS interlocks.

7.4.1.1.9 Chemical and Volume Control System (Boron Addition Portion

The boron addition portion of the CVCS is used in the hot and cold shutdown processes. The CVCS is discussed in section 9.3.4. The system instrumentation and controls which are utilized to achieve cold shutdown are described below. The piping and logic are shown in engineering drawings 01, 02, 03-M-CHP-001, -002, -003, -004, -005 and 03-M-GHP-001.

7.4.1.1.9.1 Initiating Circuits And Logic. To aid in achieving cold shutdown the CVCS component actuation steps required are:

A. Coordinated control of the charging pumps, letdown control valves, and letdown back pressure valves to adjust and maintain the correct pressurizer water level;

B. Periodic sampling and adjustment of the boron concentration to compensate for the temperature decrease and other variables until shutdown concentration is reached.

Pressurizer level is automatically controlled during normal operation by the Pressurizer Level Control System (PLCS) as discussed in section 7.7.1.1.3. The operation of the CVCS system is discussed in section 9.3.4. Boric acid is injected to ensure that sufficient shutdown margin is maintained as the RCS is cooled down. Control board process indication and

status instrumentation is provided to enable the operator to evaluate system performance and control system operation manually.

7.4.1.1.9.2 Interlocks, Sequencing And Bypasses. The interlocks, sequence of operation, and bypasses of the CVCS are discussed in section 9.3.4.

7.4.1.1.9.3 Redundancy And Diversity. The CVCS uses multiple signals as discussed in section 9.3.4.

7.4.1.1.9.4 Supporting Systems. The major powered components of the system are required to be capable of being powered from two separate electrical buses.

7.4.1.1.10 Emergency Shutdown from Outside the Control Room

In the unlikely event that the control room should become inaccessible, sufficient instrumentation and controls are provided outside the control room to:

A. Achieve prompt hot shutdown of the reactor (hot shutdown, as used here, means the reactor is subcritical at operating pressure and temperature);

B. Maintain the unit in a safe condition during hot shutdown; and

C. Achieve cold shutdown of the reactor through the use of suitable procedures.

Postulated conditions or events resulting in control room inaccessibility are not defined; however, it is assumed these circumstances are not attended by destruction of any equipment within the control room.

See engineering drawing 13-P-OOB-003 for location of remote shutdown panels.

7.4.1.1.10.1 Hot Shutdown. Sufficient instrumentation and controls are provided external to the control room to achieve and maintain hot shutdown of the reactor should the control room become inaccessible and under the assumption that (1) the operator trips the reactor prior to evacuation from the control room, and (2) that no other adverse consequences occur in addition to the evacuation (i.e., events proceed as expected as a result of a reactor trip). For shutdown outside the control room under postulated 10CFR50, Appendix R considerations, refer to appendix 9B. Hot shutdown, as used here, means that the reactor is subcritical at normal operating pressure and temperature.

Table 7.4-1 lists the instrumentation and controls available at the remote shutdown station on PVNGS.

The atmospheric dump valve manual loading stations and the auxiliary feedwater turbine speed controller are provided with control transfer from the main control room to the remote shutdown panel.

7.4.1.1.10.2 Cold Shutdown. Cold shutdown can be achieved from outside the control room through the use of suitable procedures and by virtue of local control of the equipment listed in tables 7.4-1 and 7.1-2. No further equipment controls are needed to achieve cold shutdown.

Table 7.4-1

REMOTE SHUTDOWN PANEL INSTRUMENTATION AND CONTROLS

(Sheet 1 of 2)

Instrumentation
1. Auxiliary FW regulating valve position indicators (4)
2. Auxiliary FW turbine speed indicator (1)
3. Channel A and B neutron power level (2)
4. Channel A and B reactor coolant hot/cold leg dual temperature indicators (2)
5. Channel A and B pressurizer pressure (2)
6. Channel A and B pressurizer level (2)
7. Channel A and B safety injection tank pressure (4)
8. Channel A and B steam generator pressure (4)
9. Channel A and B steam generator level (4)
10. Channel A and B refueling water tank level (2)
11. Letdown system pressure (1)
12. Letdown system flow (1)
13. Letdown system temperature (2)
14. Volume control tank level (1)
15. Channel A charging line pressure (1)
16. Channel B charging line flow (1)
17. Channel A and B shutdown cooling heat exchanger outlet temperatures (2)
18. Channel A and B shutdown cooling flow (2)
19. Condensate storage tank level (2)
20. Auxiliary FW flow to steam generators 1/2 (2 duals)
21. Channel A and B LPSI pump discharge temperature (2)

Table 7.4-1

REMOTE SHUTDOWN PANEL INSTRUMENTATION AND CONTROLS

(Sheet 2 of 2)

Controls

1. SG atmospheric dump valve permissive controls (8)
2. Auxiliary FW regulating valve controls (4)
3. Auxiliary FW isolation valve controls (4)
4. SG atmospheric steam dump modulating controllers (4)

NOTE:

The tripping of RCPs can be performed at the switchgear.

5. Auxiliary FW turbine steam supply valve control (2)
6. Auxiliary FW turbine speed control transfer switch (1)
7. Auxiliary FW turbine speed control potentiometer (1)
8. Auxiliary FW turbine trip valve control (1)
9. Auxiliary FW turbine trip pushbutton (1)
10. All channels of MSIS actuation pushbuttons (4)
11. Channel A and B auxiliary pressurizer spray valve controls (2)
12. RCP controlled bleedoff containment isolation valve controls (2)
13. RCP controlled and bleedoff relief isolation valve control (1)
14. Letdown isolation valve controls (2)
15. Backup heater groups 1 and 2 controls (2)
16. Safety injection tank vent valve control and power disconnect switch (10)
17. Shutdown cooling pumps recirculation valve controls (2)
18. Steam generator pressure variable setpoint reset (4)
19. Pressurizer pressure variable setpoint reset (4)
20. Low pressurizer pressure bypass (4)

7.4.1.2 Design Basis Information

Refer to the design bases discussion in the appropriate section of this chapter. In addition, see section 5.4.7 for discussion of SCS design basis and section 9.3.4 for CVCS design basis.

7.4.1.3 Final System Drawings

Section 1.7 includes a list of applicable electrical and instrumentation drawings and piping and instrumentation diagrams which have been provided. Furthermore, equipment location layout drawings are included in section 1.2. Logic diagrams are shown in figures 7.4-1 through 7.4-4, and 7.4-6.

7.4.2 ANALYSIS

7.4.2.1 Conformance to IEEE 279-1971

IEEE 279-1971, "Criteria For Protection Systems For Nuclear Power Generating Station," establishes minimum requirements for protection systems. The instrumentation and controls associated with the safe shutdown systems are not protection systems as defined in IEEE 279-1971; however, many criteria of IEEE 279-1971 have been incorporated in the design of the instrumentation and controls of the safe shutdown systems. Conformance of the instrumentation and controls to Section 4 of IEEE 279-1971 is discussed below.

The discussion below only pertains to those instrument and control systems and components within the CESSAR Licensing scope.

4.1 General Functional Requirements:

The instrumentation and controls of the safe shutdown systems enable the operator to:

a. Determine when a condition monitored by display instrumentation reaches a predetermined level requiring action; and

b. Manually accomplish the appropriate safety action(s).

4.2 Single Failure Criterion:

The instrumentation and controls required for safe shutdown are designed and arranged such that no single failure can prevent a safe shutdown. Single failures considered include electrical faults and physical events resulting in mechanical damage. Each system is composed of redundant trains, including instrumentation and controls which are physically separated.

4.3 Quality Control of Components:

The instrumentation and controls associated with the safe shutdown systems within the CESSAR Licensing scope are designed in accordance with The Combustion Engineering Topical Report CENPD 210A "Description of C-E Nuclear Steam Supply System Quality Assurance Program."

4.4 Equipment Qualification:

The instrumentation and controls associated with the safe shutdown systems are designed for the normal ambient conditions of the area in which they are located. Those components located in the control room, which is normally air conditioned, are designed to operate with a loss of air conditioning for the time necessary to achieve safe shutdown.

4.5 Channel Integrity:

Section 14.2 provides description of procedure for pre-operational tests and inspections to verify that all automatic and manual controls, and sequences of the integrated systems provided for safe shutdown, accomplish the intended design function. Essential instrumentation and controls are designed as Seismic Category I to ensure their ability to operate during and following a design basis earthquake.

4.6 Channel Independence:

Safe shutdown instrumentation and control channel independence is achieved by electrical and physical separation. This independence precludes a single event causing multiple channel failures.

4.7 Control and Protection System Interaction:

This does not apply to safe shutdown systems since they are not protection systems and do not interact with protection systems.

4.8 Derivation of System Inputs:

Pressure and temperature are directly measured. Level and flow signals are derived from differential pressure signals. Valve position signals are provided by limit switches. The derivations of various other signals are discussed in the sections where the safe shutdown systems are discussed.

4.9 Capability for Sensor Check:

Sensor checking is discussed in the sections where the safe shutdown systems are discussed.

4.10 Capability for Test and Calibration:

The instrumentation and control components required for safe shutdown which are not normally in operation are capable of being periodically tested. This includes instrumentation and controls for the SCS and CVCS. All automatic and manual actuation devices are capable of being tested to verify their operability. See section 13.5 and the Technical Specifications for periodic testing.

4.11 through 4.14 Bypassing:

There are no bypasses in the instrumentation and controls for the safe shutdown systems that apply to the operation of the safe shutdown systems.

4.15 Multiple Set Points:

This does not apply to the instrumentation and controls for the safe shutdown systems.

4.16 Completion of Protective Action Once it is Initiated:

These are not protection systems and do not take protective action.

4.17 Manual Initiation:

The safe shutdown systems are manually actuated. No single failure in the instrumentation and controls for the safe shutdown systems will prevent achieving a safe shutdown.

4.18 and 4.19 Access to Setpoint Adjustment and Identification of Protective Action:

Do not apply to the instrumentation and controls for the safe shutdown systems.

4.20 Information Readouts:

All safe shutdown system monitoring and control channels have appropriate indicators to provide the operator with sufficient, accurate information to evaluate system performance and to perform necessary actions.

4.21 System Repair:

The safe shutdown systems are actuated manually; therefore, replacement or repair of instrumentation and controls components can be accomplished, in reasonable time, when the systems are not actuated. Outage of system instrumentation and controls components for replacement or repair will be limited by the Technical Specifications.

4.22 Identification:

Identification of redundant channels is as described in sections 7.1.3.16 and 8.3.1.

7.4.2.2 Conformance to IEEE 308-1971

The electrical circuitry of the instrumentation and controls conforms to the criteria of IEEE 308-1971, "IEEE Standard Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations." The instrumentation and controls associated with systems and components not within the CESSAR Licensing scope are discussed in section 8.3.

7.4.2.3 Conformance to General Design Criterion 19

Conformance to GDC 19 is discussed in section 3.1.15. Remote instrumentation enables hot shutdown to be achieved if the control room is not habitable. Hot shutdown, as used here, means the reactor is subcritical at normal operating pressure

and temperature. The reactor can be brought to cold shutdown, outside of the control room, by use of appropriate procedures. See section 6.4 for additional information.

7.4.2.4 Consideration of Selected Plant Contingencies

7.4.2.4.1 Loss of Instrument Air System

None of the essential control or monitoring instrumentation is pneumatic; therefore, loss of instrument air will not degrade instrumentation and control systems associated with systems required for shutdown of the plant.

7.4.2.4.2 Loss Of Cooling Water To Vital Equipment

None of the instrumentation and control equipment relies on cooling water for operation.

7.4.2.4.3 Plant Load Rejection, Turbine Trip, And Loss Of Offsite Power

In the event of loss of offsite power associated with plant load rejection or turbine trip, power for safe shutdown is provided by the on site emergency power system. The standby generators will provide power for operation of pumps and valves; the batteries and standby generators via the battery chargers will provide power for operation of instrumentation and controls systems required to actuate and control essential components.

7.4.2.5 Emergency Shutdown From Outside The Control Room

Equipment and arrangements discussed in section 7.4.1 are in response to GDC 19 which requires certain functional

capabilities outside of the control room, which are met as discussed below.

7.4.2.5.1 Design Capability for Prompt Hot Shutdown and to Maintain Hot Shutdown

Should the control room become inaccessible, the reactor may be manually tripped from the control room, as it is being evacuated, or from the Reactor Trip Switchgear System (RTSS).

Hot shutdown conditions can be maintained from outside the control room as described in section 7.4.1.1.10 by control of pressurizer pressure and level, feedwater flow, and atmospheric steam dump. Hot shutdown, as used here, means the reactor is subcritical at normal operating pressure and temperature.

7.4.2.5.2 Cold Shutdown

Cold shutdown of the reactor without access to the control room is possible by use of instrumentation and controls described in section 7.4.1.1.10 and applicable station procedures.

7.5 SAFETY-RELATED DISPLAY INSTRUMENTATION

7.5.1 DESCRIPTION

This section includes a description of that safety-related display instrumentation which is available to the operator to allow him to monitor conditions in the reactor, the Reactor Coolant System, containment, and safety-related process systems, throughout all operating conditions of the plant so that he may perform manual actions important to plant safety.

Display information identified on Tables 7.5-1, 7.5-2 and 1.8-1, within the Reactor Coolant System, steam generating system and the containment, provides for the remote monitoring of process variables during and following design basis events.

The safety-related display instrumentation is tabulated in the following categories:

A. Safety-Related Plant Process Display Instrumentation

   Information available to the operator for monitoring conditions in the reactor and related systems.

B. Reactor Trip System (RTS) Monitoring

   Information available to the operator for monitoring the status of the RTS.

C. Engineered Safety Feature (ESF) System Monitoring

   Information available to the operator for monitoring the status of each ESF system.

D. CEA Position Indication

   Information available to the operator for monitoring the position of the CEAs.

E. Post-Accident Monitoring

Information available to the operator for monitoring the NSSS conditions following an accident.

F. Automatic Bypass Indication

Refer to section 7.5.2.6.

7.5.1.1 System Description

7.5.1.1.1 Safety-Related Plant Process Display Instrumentation

Table 7.5-2 lists the significant process instrumentation which is provided to inform the operator of the status of the reactor plant. This information which is used for the startup, operation, and shutdown of the plant, is provided in the Control Room. The information is provided in a form that is useful to the operator and may be indicated, recorded, or monitored in conjunction with a controlling function. Alternate indication and control instrumentation is provided at local stations outside the control room to allow reactor shutdown and maintenance of the reactor in a safe condition during hot shutdown should the control room become uninhabitable. (Refer to section 7.4.1.1.10). The control room layout is shown in figure 7.5-1.

7.5.1.1.2 Reactor Trip System Monitoring

Even though the RTS is automatic and does not require operator action (with the exception of a manual trip capability), sufficient information is provided to the operator in the control room to allow him to confirm that a Limiting Safety System Setting (LSSS) has been reached and a trip has taken

place. This information consists of indication of; 1) process parameters which initiate reactor trip; 2) trip, pretrip, and bypass lights; 3) audible alarms; 4) Control Element Assembly (CEA) "dropped rod" information; and 5) trip switchgear circuit breaker position. Operating bypass indication as described in section 7.1.2.19 is provided on the remote modules which are located in the main control room. Individual trip channel bypass indication is provided locally at the PPS as well as on the remote modules in the main control room. (Refer to sections 7.1.2.19, 7.2, 7.5.1.1.1 and 7.5.1.1.4).

7.5.1.1.3 Engineered Safety Features Monitoring

The Engineered Safety Features Actuation System (ESFAS) continuously monitors the system input parameters and employs an actuation logic to initiate the Engineered Safety Features (ESF) Systems should these inputs reach their trip setpoints.

After automatic actuation, the ESF Systems will continue to function properly with limited operator action. When the transfer of safety injection pump suction from the Refueling Water Tank to the containment sump is required, the Recirculation Actuation Signal (RAS) will automatically actuate this transfer. Following the RAS, timely operator action is required to close the RWT isolation valves to prevent ingress of air in the ESF pump suction piping during switchover to recirculation. Operator action is also taken to start other systems such as the Shutdown Cooling System (SCS). The RAS has to be manually overridden to allow certain SCS components to be operated for a plant cooldown.

Information is provided to the operator in the control room to allow him to monitor the operation of the ESF and related

systems in the post-accident period. This information consists of valve position indication, pump operating status, tank level indication, flow indication, and indication of the process parameters which actuate Engineered Safety Feature Systems, (Refer to Table 7.5-1). In addition, four control modules provide indication of the pretrip, trip, bypass, and operating bypass condition of each of the associated actuation system input signals. Individual trip channel bypass indication is provided at the PPS cabinet as well as on the modules in the main control room.

Table 7.5-1 requires two Class 1E channels for the refueling water tank level indicators. The PVNGS design has two Class 1E channels with Class 1E level indicators on the remote shutdown panel, but only one Class 1E level indicator in the control room. The other level indicator in the control room is isolated and powered from a non-Class 1E power supply. Refer to section 1.9.

The following additional discussion relates to:

- Monitoring of equipment automatically actuated by the one-out-of-two engineered safety features actuation signal (BOP-ESFAS) (paragraph 7.1.1.3)
- Monitoring of equipment manually actuated (the containment combustible gas control system) (paragraph 7.1.1.3)
- Monitoring of equipment automatically actuated by an auxiliary feedwater actuation signal (AFAS).

Additional engineered safety features (ESF Class 1E, except as noted) information is presented in table 7.5-1.

A. Monitoring of Equipment Actuated by One-Out-of-Two ESFAS

The systems actuated by the one-out-of-two ESFAS are:

- Fuel building essential ventilation system
- Containment purge isolation system
- Control room/building essential ventilation system

The one-out-of-two ESFAS continuously monitors the system input parameters and performs actuation logic to initiate safeguards should these inputs reach their trip setpoints.

After the automatic actuation of the ESF systems, they will continue to function properly without operator action.

Information is provided in the control room to allow the operator to monitor and evaluate the operation of the active system components during system operation, including periodic tests. Table 7.5-1 lists parameters monitored in each system. In addition, the trip status of each actuation signal in each of the two channels, as well as indication of the process parameters which actuate these ESF systems, is indicated in the control room.

B. Monitoring of Manually Actuated Containment Combustible Gas Control System

Information is provided in the control room to allow the operator to monitor process conditions necessary for manual actuation of the containment combustible

gas control system. Redundant analog instrument channels provide the required information.

Control room indications are provided to allow the operator to monitor and evaluate the operation of active system components during system operation, including periodic tests and the post-accident period. Table 7.5-1 lists parameters monitored in this system.

Control of the containment combustible gas control system is local and indication of system air flow and temperature is provided at the local panel.

C. Monitoring of Auxiliary Feedwater System

Refer to paragraph 7.3.1.1.10.7. Information is provided in the control room to allow the operator to monitor and evaluate the operation of the active system components during system operation including periodic tests and the post-accident period. Table 7.5-1 lists parameters monitored in this system.

7.5.1.1.4 Control Element Assembly Position Indication

Two independent CEA position indication systems provide CEA position information to the operator. The systems are the pulse counting CEA position indication system and the reed switch CEA position indication system. The pulse counting system is discussed in section 7.7.1.3.2; the reed switch system is discussed below. CEA position displays are located on the main control board.

The reed switch CEA position indication system utilizes a series of magnetically actuated reed switches (reed switch position transmitters) to provide signals representing CEA

7.5.1.1.4 (continued)

position. Two independent reed switch position transmitters (RSPT) are provided for each CEA. The RSPT provides an analog position indication signal and three physically separate discrete reed switch position signals. The analog position indication system utilizes a series of magnetically actuated reed switches spaced at 1-1/2-inch intervals along the RSPT assembly and arranged with precision resistors in a voltage divider network. The RSPT is affixed adjacent to the CEDM pressure housing, which contains the CEA extension shaft and actuating magnet. The analog output signal is proportional to the CEA position within the reactor core. The three discrete reed switch position signals are contact closure signals from three separately located reed switches. These signals are an Upper Electrical Limit, a Lower Electrical Limit and a rod drop contact.

The analog reed switch CEA position signals are input to the DNBR/LPD Calculator System (See Section 7.2). CEA position information is provided to the Core Protection Calculators (CPCs) indirectly via a high speed communication bus connecting the CEACs and the CPCs. This analog CEA positional data is sent to the CEA Calculators (CEACs) in each safety channel via the CEA Position Processors (CPPs). Each of the two CEACs in each safety channel has its own CPP, thus supporting the concept of redundancy to increase the margin of error should an input to the CEAC fail.

The CEA Calculators display the position of each regulating, shutdown, and part-strength CEA to the operator in a numeric format on a visual display on the Operator Modules (OMs) from

7.5.1.1.4 (continued)

which the operator can address any analog position signal for display.

Additionally, this information is displayed in both graphical and numeric display on main control board CEA Position Display System (CEAPDS). The CEAPDS also displays in numerical format penalty factor, CEA deviation, and a user adjustable alarm setpoint for various CEA and CPC related functions including deviation. The operator has the capability to select any safety channel for display or any regulating group.

In addition the displays, CEA deviation information is provided by the CEA Calculators to the CPCs and a CEA deviation alarm. The CEA deviation alarm is provided to the plant annunciator system in the event a CEA Calculator indicates that the difference between the highest and lowest CEA positions in a subgroup exceeds a predetermined allowable deviation. The CEA deviation information is used in the CPCs determination of power distribution. The power distribution is then factored into the low DNBR and high local power density trip function. Pre-trip alarms are initiated if the DNBR or Local Power Density trip limits are approached. A pre-trip alarm light is provided on the PPS control panel (both local and remote). Also, a pre-trip alarm is provided to the plant annunciator system.

The three discrete CEA position switches provide signals (contact closure signals) to the Control Element Drive Mechanism Control System (CEDMCS). The signals are utilized to provide CEA limit indication on the main control board and also to provide input to the CEA control interlocks. Each of the

7.5.1.1.4 (continued)

three discrete reed switch contacts actuates an interface relay located within the CEDMCS. These relays provide contact signals for indication and control and, in the case of the rod drop switch, an additional contact signal is provided to the Plant Monitoring System to set the pulse counting system (see section 7.7.1.3.2.3). The upper and lower electrical limits indication appears as two separate lights on the CEDMCS control panel mounted on the main control board. The CEA drop indication appears on the core mimic display mounted on the main control board.

7.5.1.1.4.1 CEA Limit Lights Indication. A light display is provided on the control board to indicate the fully withdrawn and fully inserted position of each CEA and provides indication of a dropped CEA.

Table 7.5-1

ENGINEERED SAFETY FEATURE SYSTEM MONITORING (Sheet 1 of 7)

Parameter	Type of Readout	Number of Channels	Location	Range	Displayed Accuracy
Fuel Building (FB) Essential Ventilation System					
FB ventilation isolation damper position	Indicating lights	1 pair/ damper	Control room	NA	NA
FB essential exhaust fans motor starter contact position	Indicating lights	1 pair/fan	Control room	NA	NA
Fuel pool area radiation monitor	Indicator	1	Control room	10^{-1} - 10^{4} mr/h	±20%[a]
Fuel building exhaust gas activity monitor	Indicator	1	Control room	10^{-6} - 10^{-1} $\mu Ci/cm^3$	±25%[a]
Fuel building AFU charcoal differential temperature monitor	Indicator	2	Control room	0 to 50F	±1%[b]

a. Accuracy as a percentage of the displayed value.

b. Accuracy as a percentage of the monitors full scale.

Table 7.5-1

ENGINEERED SAFETY FEATURE SYSTEM MONITORING (Sheet 2 of 7)

Parameter	Type of Readout	Number of Channels	Location	Range	Displayed Accuracy
Fuel Building negative pressure (diff press across inside of bldg and ambient)	Indicator	1	Control room	0 to 0.27 in. H_2O	+1%[b]
Containment Purge Isolation System					
Normal purge isolation valve position	Indicating lights	1 pair/ valve	Control room	NA	NA
Power access purge area monitors	Indicator	2	Control room	10^{-1} - 10^{4} mr/h	±20%[a]
Control Room/ Building Essential Ventilation System					
Control room/ building ventilation isolation damper position	Indicating lights	1 pair/ damper	Control room	NA	NA
Control room/ building essential fan motor breaker position	Indicating lights	1 pair/fan	Control room	NA	NA

Table 7.5-1

ENGINEERED SAFETY FEATURE SYSTEM MONITORING (Sheet 3 of 7)

Parameter	Type of Readout	Number of Channels	Location	Range	Displayed Accuracy
Control room ventilation intake gas activity monitors	Indicator	2	Control room	10^{-6} to 10^{-1} $\mu Ci/cm^3$	± 25%[a]
Control room temperature monitors	Indicator	2	Control room	0 to 150F	± 2%[b]
Containment Combustible Gas Control System					
Containment hydrogen monitors	Indicator Recorder	2 1	Control room	0 to 10%	± 6.0%[b,c] ± 6.0%[b,d]
Hydrogen control containment isolation valve position	Indicating lights	1 pair/ valve	Control room	NA	NA
Auxiliary Feedwater System					
Auxiliary feedwater pump discharge pressure	Indicator	1/pump	Control room	0 to 2000 psig	± 2.25%[b]

c. Displayed accuracy of control room indicator.

d. Displayed accuracy of control room recorder.

Table 7.5-1

ENGINEERED SAFETY FEATURE SYSTEM MONITORING (Sheet 4 of 7)

Parameter	Type of Readout	Number of Channels	Location	Range	Displayed Accuracy
Auxiliary feedwater flow	Indicator	2 (redundant/each auxiliary feedwater line	Control room	0 to 2000 gal/min	± 35%[b][e]
Auxiliary feedwater regulating valves	Indicating lights	1 pair/valve	Control room	NA	NA
Auxiliary feedwater pump turbine speed	Indicator	1	Control room	0 to 6000 r/min	± 2.5[b]
Auxiliary feedwater suction from CST isolation valves	Indicating lights	1 pair/valve	Control room	NA	NA
ESF Status Panel					
System availability	Indicating lights	1 light/system/trip	Control room	NA	NA

e. Accuracy given is for the rated flow of one AFW pump.

Table 7.5-1

ENGINEERED SAFETY FEATURE SYSTEM MONITORING (Sheet 5 of 7)

Parameter	Type of Readout	Number of Channels	Number of IE Channels	Range	Indicator Accuracy	Location
Containment Isolation System[f]						
Containment Isolation Valve Position	Indicating Lights	1 pair/valve		N/A	N/A	Control Room
Safety Injection System						
Safety Injection/ Shutdown Cooling Valve Position	Indication Lights/ Indicator	1 pair/ valve 1 per valve	(g)	N/A	N/A	Control Room[h]
Safety Injection Tank Level	Indicator Indicator	1/Tank 2/Tank	1/Tank --	0-100% (34 ft. scale) 0-100% (4 ft. scale)	± 2-1/2% ± 2-1/2%	Control Room Control Room
High Pressure Safety Injection Cold Leg Flow	Indicator	4	4	0-750 gpm	± 2-1/2%	Control Room
High Pressure Safety Injection Hot Leg Flow	Indicator	2	2	0-750 gpm	± 2-1/2%	Control Room/ Local
Low Pressure Safety Injection Flow	Indicator	2	2	0-10,000 gpm	± 2-1/2%	Control Room/ Local
Shutdown Cooling Heat Exchanger Inlet Pressure	Indicator	2	--	0-750 psig	± 2-1/2%	Control Room

Table 7.5-1 (Cont'd)

ENGINEERED SAFETY FEATURE SYSTEM MONITORING (Sheet 6 of 7)

Parameter	Type of Readout	Number of Channels	Number of IE Channels	Range	Indicator Accuracy	Location
High Pressure Safety Injection Pump Discharge Header Pressure	Indicator	2	--	(#1) 0-3000 psig (#2) 0-2500 psig	± 2-1/2%	Control Room
Low Pressure Safety Injection Pump Header Pressure	Indicator	2	--	0-750 psig	± 2-1/2%	Control Room
Safety Injection Tank Pressure	Indicator Indicator	1/Tank 2/Tank	1/Tank 1/Tank	0-750 psig 450-650 psig	± 2-1/2% ± 2-1/2%	Control Room/Local Control Room
Safety Injection Line Pressure	Indicator	6	--	0-2500 psig	± 2-1/2%	Control Room
Shutdown Cooling Inlet and Outlet Temperature	Indicator/ Recorder	2	2	40-400F	± 2-1/2%	Control Room/Local
Shutdown Cooling Heat Exchanger Outlet Temperature	Indicator	2	2	40-400F	± 2-1/2%	Control Room
<u>Main Steam Isolation Systems</u>						
Main Steam Isolation Valve Position	Indicating Lights	1 pair/ valve	--	N/A	N/A	Control Room
Main Steam Isolation Valve Bypass Valve Position	Indicating Lights	1 pair/ valve	--	N/A	N/A	Control Room
Main Feedwater Isolation Valve Position	Indicating Lights	1 pair/ valve	--	N/A	N/A	Control Room

Table 7.5-1 (Cont'd)

ENGINEERED SAFETY FEATURE SYSTEM MONITORING (Sheet 7 of 7)

Parameter	Type of Readout	Number of Channels	Number of IE Channels	Range	Indicator Accuracy	Location
Chemical Volume Control System[f]						
Refueling Water Tank Isolation Valve Position	Indicating Lights	1 pair/ valve	1	N/A	N/A	Control Room
Refueling Water Tank Level	Indicator	4	4	0-100%	± 2%	Control Room
Refueling Water Tank Level	Indicator	2	1[i]	0-100%	± 2%	Control Room

NOTES:

f. All CVCS containment isolation valves are open/close type valves.

g. All indication on electrically actuated valves in the Safety Injection/Shutdown Cooling System, with exception of SI-661, receive IE power.

h. Valves which are required to bring the plant to cold shutdown have open/close position indicated outside the Control Room also.

i. Only one indicator is class 1E. The other indicator is non-1E and isolated.

Table 7.5-2
SAFETY-RELATED PLANT PROCESS DISPLAY INSTRUMENTATION (Sheet 1 of 2)

Parameter	Type of Readout	Number of Channels	Range	Indicator Accuracy	Location[b]
Pressurizer Pressure	Indicator	4	1500-2500 psia	± 2%	Control Room
Pressurizer Pressure	Indicator	4	0-3000 psia	± 2%	Control Room
Pressurizer Pressure	Recorder	1	0-3000 psia	± 2%	Control Room
Pressurizer Pressure	Indicator	4	0-750 psia	± 2%	Control Room
Containment Pressure	Indicator	4	-4 to +85 psig	± 2%	Control Room
Containment Pressure	Indicator	4	-4 to +20 psig	± 2%	Control Room
Refueling Water Tank Level	Indicator/Alarm	2	0-100%	± 2%	Control Room
Refueling Water Tank Level	Indicator	4	0-100%	± 2%	Control Room
Steam Generator Pressure	Indicator	4/S.G.	0-1524 psia	± 2%	Control Room
Steam Generator Level (Wide Range)	Recorder	1/S.G.	0-100%	± 2%	Control Room
Steam Generator Level (Wide Range)	Indicator	4/S.G.	0-100%	± 2%	Control Room
Steam Generator Level (Narrow Range)	Indicator	4/S.G.	0-100%	± 2%	Control Room
Pressurizer Level	Indicator	2	0-100%	± 2%	Control Room
Coolant Temperature (Hot)	Indicator	8*	375-675°F	± 2%	Control Room
	Indicator	4	50-750°F	± 2%	Control Room
	Recorder	2	50-750°F	± 2%	Control Room
Coolant Temperature (Cold)	Indicator	8*	465-615°F	± 2%	Control Room
	Indicator	4	50-750°F	± 2%	Control Room
	Recorder	2	50-750°F	± 2%	Control Room
Local Power Density	Indicator	4	0-25 Kw/ft.	± 2% †	Control Room
DNBR[a]	Indicator	4	0-2[a]	± 2% †	Control Room
Neutron Flux Level Rate of Change	Indicator	4	-1 to +7 DPM	± 2%	Control Room
Neutron Flux Power Level	Indicator	4	$2x10^{-8}$ to 200% power	± 2%	Control Room
(Safety Channels)	Recorder	4	0 to 200% power	± 2%	Control Room

* equally divided between Loops 1 & 2.

† indicator accuracy

a. CPC Point ID 107 can display the full 0-10 range on either the operator module or maintenance and test panel.

b. Refer to Table 7.4-1 for channels that also provide indication at the Remote Shutdown Panel.

Table 7.5-2 (Cont'd)

SAFETY-RELATED PLANT PROCESS DISPLAY INSTRUMENTATION (Sheet 2 of 2)

Parameter	Type of Readout	Number of Channels	Range	Indicator Accuracy	Location[b]
Neutron Flux Power Level (Safety Channels)	Recorder	4	0-200% power	± 2%	Control Room
Neutron Flux Power Level (DNBR/LPD Calculators)	Recorder	4	0-200% power	± 2%	Control Room
Charging Pump Discharge Pressure	Indicator	1	0-3000 psig	± 2%	Control Room
Charging Flow	Indicator	1	0-150 gpm	± 2%	Control Room

7.5.1.1.5 Post-Accident Monitoring

The Post-Accident Monitoring (PAM) instrumentation is provided to allow the operator to assess the state of the NSSS following Design Basis Events. Most of these instruments monitor instruments or equipment, or systems which provide automatic action for the Design Basis Event.

Refer to Table 1.8-1, in addition the following are also required as post-accident monitoring instrumentation: extended range noble gas effluent radiation monitoring, containment high-range radiation monitoring, containment pressure monitoring, containment water level monitoring, and containment hydrogen monitoring. Refer to section 18.II.F.1 for TMI-related information pertaining to post-accident monitoring instrumentation.

A detailed discussion on radiation monitoring is provided in section 11.5.

A discussion on hydrogen monitoring is provided in paragraph 6.2.5.2.2.2.

7.5.1.1.6 Automatic Bypass Indication on a System Level

A status monitoring panel in the control room displays the availability of the CESSAR ESFAS, the one-out-of-two ESFAS, all the ESF systems (including the NSSS ESF systems and the containment combustible gas control system), and the automatic ESF supporting systems. The reactor protective system (RPS) has no bypasses or inoperable conditions on a system level; therefore, no RPS condition is indicated on the panel.

The number of bypass features or devices provided for operational purposes or routine testing is minimized by design,

but wherever such features or devices are an integral part of the design and are used more frequently than once a year, a means of indication is provided in the main control room. Each ESF system component (such as pump, valve, or fan, including vital support system equipment) that must operate upon automatic or manual ESF actuation is monitored by a system level annunciator indicating inoperability of that ESF system. A bypass of a component in a given system by operation of a control switch, loss of control circuit power, pulling of a fuse, "racking-out" a breaker, or loss of vital supporting auxiliary systems is annunciated with an audible alarm. Any other piece of plant equipment in a system, not part of the ESF equipment, but that performs some required function in support of a piece of ESF equipment, provides a contact to annunciate the bypass status of the dependent ESF system.

Equipment rendered inoperative because of infrequent maintenance functions (performed on a frequency of once a year or less) is not specifically and automatically indicated. The capability to manually initiate a system inoperable signal is, however, included. Such maintenance activities include manual valves provided for isolation of equipment for repair, electrical cable connectors, screw terminals, motor-pump couplings, or other manual disconnects.

See figure 7.5-2 for panel layout for the safety equipment status system.

7.5.2 ANALYSIS

7.5.2.1 Analysis of Safety-Related Plant Process Display Instrumentation

Plant Process Instrumentation is provided to give the operator information to monitor conditions in the plant and perform operations important to plant safety. In addition, the information allows the operator to perform the cross-checking of Plant Protection System measurement channels to assure operational availability of these channels as discussed in section 7.2.1.1.9 and 7.3.1.1.8. The following design criteria were used in the selection of plant instrumentation:

A. Provide continuous monitoring of process parameters required by the operator;

B. Provide a permanent record of those parameters for which trend information is useful, from a safety standpoint;

C. Provide display information to the operator that is reliable, comprehensible, and timely;

D. Provide multiple channels of indication for the RPS and ESFAS process parameters to allow cross-checking of channels; and

E. Provide instrumentation display that adequately monitors the parameters over the ranges required for various conditions.

The information provided is sufficient to allow the operator to accurately assess the conditions within the reactor systems, and in a timely manner perform those appropriate actions to maintain the reactor systems within the conditions assumed by

the safety analysis in Chapter 15. In addition, the information allows the operator to perform the cross-checking of measurement channels to assure operational availability of these channels as discussed in section 7.2.1.1.9 and 7.3.1.1.8.

7.5.2.2 Analysis of Reactor Trip System Monitoring

Sufficient information is provided to the operator to allow confirmation that a trip has occurred and to determine the process parameter that has provided a trip input.

CEA insertion information can be determined by the operator after a trip by visual display bar chart information and CEA Limit Indication (refer to section 7.5.1.1.4).

Indication of neutron levels in the reactor core as well as other reactor and Reactor Coolant System information are provided for the operator.

The following design criteria were used in the selection of information that is provided to the operator:

A. System conditions requiring operator attention during routine plant operations and at the time of reactor trip are available in the control room;

B. Annunciation in the control room of all operations performed at the RPS cabinet affecting the function of the system;

C. Indication of any selected plant variables that are manually bypassed; and

D. Indication of automatic removal of a bypass.

7.5.2.3 Analysis of Engineered Safety Features Monitoring

Information is provided to the operator so that he may monitor the status of the Engineered Safety Features Systems. The following design criteria were used in the selection of information that is provided to the operator:

A. System conditions requiring operator attention or action during routine plant operators are displayed and/or controlled in the control room;

B. Annunciation is provided in the control room of all operations performed at the ESFAS cabinet affecting the function of the system;

C. Indication of any selected plant variable that is manually blocked or bypassed is provided; and

D. Indication of automatic removal of block or bypass status is provided.

Consistent with the above criteria, the information shown in Table 7.5-1 is provided for the operator's use. The information is provided to aid the operator in determining that manual actuation of an Engineered Safety Features System is required (which he may then perform) and to aid him in confirming proper system operation after automatic initiation. Input parameters used for actuation are indicated in the control room as are positive indications that pump and valves have actuated and that flows have been established.

BOP ESFAS. Information is provided to the operator to allow monitoring of the status of the one-out-of-two ESF systems. The design criteria provided in CESSAR Section 7.5.2.3 were used in the selection of information that is provided to the operator.

Consistent with these criteria, the information shown in table 7.5-1 is provided for operator use.

The display instrumentation for the containment combustible gas control system is supplied in such a manner that the operator has time to make reasoned judgment before his action is essential. Consistent with this criterion, the information shown on table 7.5-1 is provided for operator use.

The ESFAS actuation parameter displays provide information to enable the operator to assess accident conditions and to perform the necessary operation of the containment combustible gas control system. Containment hydrogen concentration monitors provide information necessary for manual combustible gas control through the use of the containment hydrogen recombiners. Refer to Table 1.8-1 and subsections 6.2.5 and 18.II.F.1.6 for further information.

7.5.2.4 Analysis of CEA Position Indication

CEA Position Indication allows the operator to easily determine the position of all of the CEAs within the reactor core. The information is presented in a form that can be assessed by the operator to easily determine that the CEAs are in the required position, that a CEA has dropped into the core, or that the CEA positions are as required after a reactor trip.

The following design criteria were used in selection of the CEA position indication:

A. Position readouts of all CEAs may be obtained.

B. Continuous position indication of all CEAs is available.

C. A means is provided to alert the operator to deviation of CEAs within a group.

D. A permanent record may be made of the position of any or all CEAs.

E. Separate "full-in" and "full-out" indications are provided for each CEA.

F. Redundant and diverse means of indicating CEA position are provided.

7.5.2.5 Analysis of Post-Accident Monitoring Instrumentation

The Post-Accident Monitoring (PAM) instrumentation which is identified in table 1.8-1 is provided for remote monitoring of post-accident conditions within the Reactor Coolant System, steam generating system and the containment. Post-accident conditions are defined as those conditions which exist after the NSSS has reached a stable configuration following an accident.

The extensive instrumentation and controls required by table 1.8-1 provide the plant operator with long-term monitoring and surveillance capabilities and provide redundancy and appropriate wide-range indication of post-accident conditions within the primary containment.

The requirements of IEEE 279-1971 "Criteria for Protections System for Nuclear Power Generating Station" are not completely applicable to the design of the post-accident monitoring instrumentation in that this instrumentation is not part of a protection system. However, the intent of some of the design criteria contained therein will be applied to the design of those systems used to monitor post-accident conditions to the

extent appropriate as follows (heading numbers correspond to the Section numbers in IEEE 279-1971):

4.1 General Functional Requirement:

The PAM instrumentation is not designed to limit reactor fuel, fuel cladding and coolant conditions to levels within plant and fuel design limits. Each instrument's performance characteristic, response time and accuracy have been selected for compatibility with the design goal of providing the operator with long-term monitoring and surveillance capabilities after the plant has reached a stable condition.

4.2 Single Failure Criterion:

The PAM instrumentation is designed so that any single failure shall not result in the loss of the surveillance function on the system level after an incident. The wiring is arranged so that no single fault or failure, including either an open or shorted circuit will result in the loss of surveillance capability at the system level.

4.3 Quality Control of Components and Modules:

The Quality Assurance program is described in Topical Report CENPD 210A "Description of the C-E Nuclear Steam Supply System Quality Assurance Program" (Reference 1). This program includes appropriate requirements for design review, procurement, inspection and testing to ensure that PAM components shall be of a quality consistent with minimum maintenance requirements and low failure rates.

4.4 Equipment Qualifications:

The PAM instrumentation meets the equipment qualification requirements described in Section 3.10 and 3.11.

4.5 Channel Integrity:

Type testing of components, separation of sensors and channels, and qualification of cabling are utilized to ensure that the channels will maintain the functional capability required under applicable extreme conditions.

4.6 Channel Independence:

The locations of the sensors and the points at which the sensing lines are connected to the process loop have been selected to provide physical separation of the channels to the maximum extent practicable, thereby precluding a situation in which a single event could fail both PAM channels. See section 8.3.1.4 for cable routing.

4.7 Control and Protection System Interaction:

Where PAM instrumentation is also used for control purposes an isolation device shall be used to prevent any credible failure in the control portion from affecting the PAM readout.

4.8 Derivation of System Inputs:

All system inputs are derived from signals that are direct measures of the desired variables.

4.9 Capability for Sensor Checks:

Performance of the surveillance instrumentation will be verified during reactor operation subject to the following:

a. Testing will not adversely affect the safety or operability of the plant;

b. Normal system operation will be considered an acceptable method of verifying surveillance instrumentation performance if system operating

parameters are similar to those anticipated following a LOCA:

c. In the event that the surveillance instrument performance cannot be verified under the conditions of a and b above, periodic testing will be performed during reactor shutdown periods.

4.10 Capability for Test and Calibration:

The PAM instrumentation can be checked from the sensor signal through the indication located in the main control room. Many of the sensors used for PAM are also used in the PPS and therefore will be tested during PPS testing. For those sensors that are not part of the PPS, testing will be performed on a periodic basis.

4.11 Channel Bypass or Removal from Operation:

Any one of the two PAM channels may be tested, calibrated or repaired without detrimental effects on the other channel. The limitations specified in Technical Specifications should be adhered to.

4.12 Operating Bypasses:

This Section is not applicable to PAM instrumentation.

4.13 Indication of Bypasses:

This section is not applicable to PAM instrumentation.

4.14 Access to Means for Bypassing:

This section is not applicable to PAM instrumentation.

4.15 Multiple Set Points:

This section is not applicable to PAM instrumentation.

4.16 Completion of Protective Action Once it is Initiated:

This section is not applicable to PAM instrumentation.

4.17 Manual Initiation:

This section is not applicable to PAM instrumentation.

4.18 Access to Set Point Adjustments, Calibration and Test Points:

See section 13.5 for a discussion of administrative control for access to setpoint adjustments.

4.19 Identification of Protective Actions:

This section is not applicable to PAM instrumentation.

4.20 Information Readout:

Indicators capable of displaying both current reading and historical trend information are provided for each redundant post-accident monitoring (PAM) channel. Outputs are provided for continuously recording one channel of each analog variable.

4.21 System Repair:

A defective PAM channel can be detected by testing as previously discussed. Replacement or repair of one PAM channel will not affect the other channel. (Refer to Technical Specifications for limitations).

4.22 Identification:

The PAM instrumentation channels will not be uniquely identified as such. The channels will be identified to distinguish between redundant channels for the same variable. Refer to section 1.8 for a discussion of Regulatory Guide 1.97, Post Accident Monitoring Instrumentation.

7.5.2.6 Analysis of Automatic Bypass Indication on a System Level

The automatic bypass/inoperable indication status panel provides a means for the operator to easily determine the availability of ESF and ESF-supporting systems. The following design criteria were used in the design to conform to Regulatory Guide 1.47 and Branch Technical Position ICSB-21.

A. The system consists of two portions; one reporting the status of safety train A equipment, the other reporting the status of safety train B equipment. The system accepts channelized (channel A, B, C, or D) Class 1E inputs. The system is nonsafety-related, but since inputs are Class 1E, the system is powered from Class 1E 125 V-dc power supplies.

B. Status contacts continuously monitor the availability of control power and the position of circuit breakers of all automatically actuated ESF devices. A loss of control power or deliberate racking out of a breaker automatically initiates a system level indication with audible alarm, except for the containment purge refueling mode isolation valves. The circuit breakers for these valves are locked open during normal operation. An alarm is not initiated when the valve circuit breakers are locked open and the valve is in the safe position (closed). An alarm will be initiated if the valve is not in a safe position and a loss of power develops, or the valve is not in a safe position and its circuit breaker is open.

C. The capability for initiating a manual bypass indication and alarm is provided via a system level manual bypass switch used to indicate the bypass condition to the operator for those manual valves and other components which are not automatically monitored. The initiation and removal of manual bypass indication will be under administrative control.

D. All systems affected by the bypassing/inoperability of a given component that are shared by multiple systems automatically generate a bypass/inoperable audible and visual alarm in each system affected.

E. Indication and annunciation test capability is provided by simulating a trouble contact condition when the test button is depressed. The test feature generates the audible alarm and causes all windows to flash in unison. The test feature is independent for each channel.

7.5.3 REFERENCES

1. CENPD 210A "Description of the C-E Nuclear Steam Supply System Quality Assurance Program" Combustion Engineering, Inc.

7.6 ALL OTHER INSTRUMENTATION SYSTEMS REQUIRED FOR SAFETY

7.6.1 INTRODUCTION

This section describes the Shutdown Cooling System Suction Line Valve Interlocks and the Safety Injection Tank Isolation Valve Interlocks. The Shutdown Cooling System (SCS) is discussed in section 5.4.7; the Safety Injection System (SIS) is discussed in section 6.3.

The interlocks on the SCS and on the Safety Injection Tanks (SIT) are designed to act as permissives. The Shutdown Cooling System Suction Line Valve Interlocks permit the isolation valves to be opened below a certain pressure and automatically close them above a certain pressure. The Safety Injection Tank Isolation Valve Interlocks are designed to permit the operator to isolate the SITs at low pressure and automatically open them above a certain pressure. This allows the SITs to be maintained at a given pressure when the balance of the RCS is depressurized.

Since there are no reactor coolant loop isolation valves, there will always be some flow in an idle loop so that there is no need for a cold water interlock.

The refueling interlocks are discussed in section 9.1.4.

The Shutdown Cooling System Suction Line Valve Interlocks and the Safety Injection Tank Isolation Valve Interlocks are automatically connected to the emergency busses if there should be a loss of all AC power. This is to assure that the interlocks and valves will be able to operate under all operating conditions.

Instrumentation utilized to mitigate the consequences of fuel handling accidents are discussed in sections 9.4 and 15.7.

7.6.1.1 System Descriptions

7.6.1.1.1 Shutdown Cooling System Suction Line Valve Interlocks

The SCS is a low temperature, low pressure system used to remove decay heat from the RCS. Cooldown of the RCS is accomplished via the steam generator down to about 350°F and about 400 psia. Below these values the SCS is used to cool the RCS to refueling temperatures and to maintain these conditions for extended periods of time.

To preclude overpressurization, there are redundant, motor driven, interlocked, isolation valves on each suction line. The interlocks prevent the suction line isolation valves from being opened if RCS pressure has not decreased below 410 psia.

These interlocks are redundant so that any single failure will not cause a suction line and heat exchanger to be subjected to pressures greater than design pressure. The interlock cannot be overridden so that operator action cannot inadvertently subject the SCS to RCS pressure. In addition, no single failure can prevent the operator from aligning the valves, on at least one suction line, for shutdown cooling after RCS pressure requirements are satisfied.

Redundant relief valves are provided on the suction lines to prevent or mitigate overpressurization from pressure transients. These transients can be caused by inadvertent starting of HPSI pumps, charging pumps, inadvertent energizing of pressurizer backup heaters, or a combination of these. The relief valves are set at 467 psig to insure the system stays below its design limits.

7.6.1.1.2 Safety Injection Tank Isolation Valve Interlocks

The SIS is designed to inject borated water into the RCS upon receipt of an SIAS (refer to Section 7.3) and to provide long term cooling in conjunction with other systems following an accident. The Safety Injection Tanks (SIT) inject borated water if system pressure drops below their internal pressure. During normal operation each tank has a motor operated isolation valve that is open and power to its motor circuit is removed to eliminate the possibility of spurious actuation. As the RCS pressure is reduced during plant shutdown, the low pressurizer pressure trip setpoint is reduced to avoid inadvertent initiation of Safety Injection, the SITs are depressurized to a value below the SCS design pressure, and the valves have their power restored and are closed.

The SIT interlocks are used to prevent the SITs from inadvertently pressurizing the SCS while maintaining SIT availability in case of a LOCA. Refer to Figure 7.6-2 for the interlock logic. The isolation valves are manually closed when RCS pressure drops below the value shown on Table 7.6-1 so that the SITs cannot cause overpressurization of the SCS, and also so that the SITs can be maintained at some pressure above atmospheric. The valves will automatically reopen when RCS pressure exceeds 515 psia; this is not a problem for the SCS since SIT pressure is less than SCS design pressure at this time. This opening of the SIT isolation valves insures that the SITs are available for injection during plant startup. If the isolation valves are closed and an SIAS is initiated, the isolation valves will automatically open. The SIAS overrides the interlock or any manual signal.

There is an alarm associated with the SITs. The alarm will sound if the RCS pressure is increased to 700 psig and the SITs have not been repressurized. This insures that the SITs will be available for injection at the RCS pressure specified in the ECCS analysis (See section 6.3.3).

7.6.1.1.3 Class 1E Alarm System

A Class 1E alarm system is provided for a limited number of operational occurrences for which no specific automatic actuation of a safety system is required. The Class 1E alarm system alerts the operator to keep the plant operating within technical specification limits and prevent equipment damage.

The 1E alarm system consists of individual visual status indicators dedicated to each instrument channel. An audible alarm is provided for each alarm channel. The alarmed condition requires manual reset, once initiated.

The 1E alarm system is independent of the normal plant annunciation system and the redundant channels are powered from separate 1E power trains.

Operator acknowledgment of 1E alarms follows the same procedure used for the normal plant annunciator, with the exception that the audible alarms for each channel can be "silenced" with the use of a keylock switch (see 7.6.2.1.3).

7.6.1.1.3.1 <u>Reactor Coolant Pump Cooling Water Supply Monitoring</u>. Safety grade instrumentation is provided to detect the loss of cooling water to the reactor coolant pumps in order to ensure

that the operator will have sufficient time to initiate manual tripping of the pumps to protect the pumps from seal failure. The cooling water flowrate to each pump is monitored by two redundant flow transmitters. If the cooling water flowrate is reduced below the minimum required for pump operation, a low flow signal will be initiated in each flow channel for the affected pump. The low flow signals will independently actuate their respective Class 1E redundant alarm system channels in the control room. The setpoint for alarming will be selected with sufficient margin to assure that proper operator notification is given. The alarm system utilizes a one-out-of-one logic for each channel.

7.6.1.1.3.2 Safety Injection Tank Pressure Monitoring. Safety grade instrumentation is provided to alert the operator of the unavailability of the safety injection tanks (SITs) to perform their core flooding function in the event of a LOCA.

The pressure in each SIT is independently monitored by a pressure sensor.

Reactor coolant system pressure is monitored by pressurizer pressure sensors.

If SIT pressure is reduced below that required for core flooding, a low-pressure signal will be initiated in the respective pressure channel for the affected tank.

The low-pressure signal will independently actuate its respective Class 1E redundant alarm system for channel B (tanks 1 and 2) or for channel A (tanks 3 and 4) in the control room.

The alarm for low SIT pressure is based upon an indication of pressurizer pressure above 715 psia coincident with SIT

pressure below 600 psig. The alarm system utilizes a one-out-of-one logic for each SIT pressure sensor, with a one-out-of-two logic for each visual alarm window.

7.6.1.1.3.3 Auxiliary Building ESF Pump Room Level Monitoring. Safety grade instrumentation is provided to alert the operator of a leak in an auxiliary building ESF pump room (containment spray, high-pressure safety injection, and low-pressure safety injection). The level in each ESF pump room is independently monitored by a level switch mounted in the drain basin of each room. A high level signal, from the level switch, will independently actuate the respective Class 1E alarm in the control room.

7.6.1.1.4 Other Systems

7.6.1.1.4.1 Fire Protection Instrumentation and Detection System. The instrumentation utilized to detect, alarm, or mitigate the consequences of fires is discussed in subsection 9.5.1.

Table 7.6-1
SHUTDOWN COOLING (SDC) SYSTEM AND SAFETY INJECTION TANK (SIT) INTERLOCKS
(Page 1 of 3)

SYSTEM	SETPOINT[a]	FUNCTION and Value[b]
Shutdown Cooling System		
SDC Suction Line Valves	≤ 385 psia	Open Permissive Interlock: prevents SDC isolation valves from opening until RCS pressure is less than the setpoint value and allows operator to open valves only when pressure is < 410 psia. Technical Specifications (TS): Verify SDC System open permissive interlock prevents the valves from being opened every 18 months with a simulated or actual RCS pressure signal ≥ 410 psia (S.R. 3.4.15.2). Test description in UFSAR section 7.6.2.2.1; 4.10
Shutdown Cooling Relief Valves	467 psig	Prevents or mitigates over-pressurization of the SCS; an LTOP design feature.
Safety Injection Tank SIT Isolation Valves	≥ 410 psia	Auto-Open Interlocks: SIT isolation valves automatically open prior to exceeding RCS pressure of 515 psia OR on a SIAS, if the valves are closed. Sends an open signal if valves are open, or closed, and overrides a closing signal.[d]

Table 7.6-1
SHUTDOWN COOLING (SDC) SYSTEM AND SAFETY INJECTION TANK (SIT) INTERLOCKS
(Page 2 of 3)

SYSTEM	SETPOINT[a]	FUNCTION and Value[b]
Shutdown Cooling System		
Safety Injection Tank SIT Isolation Valves (continued)		Technical Requirements Manual (TRM): Verify that each SIT MOV opens automatically prior to actual or simulated RCS pressure exceeding 515 PSIA and upon receipt of a SIAS test signal; every 18 months. (TRM TSR 3.5.200.4) (SIAS Variable Setpoint: see Table 7.2-1 & Table 7.3-11A) Test description in USFAR section 7.6.2.2.2; 4.10
	≤ 420 psia[c]	SIT Valves must be fully open when PZR pressure is ≥ 430 psia. Power to the MOVs must be removed when PZR pressure is ≥ 1500 psia. (LCO 3.5.2)
	< 405 psia	SIT Valve Closure Permissive: allows valves to be closed by the operator only when RCS pressure is less than 430 psia. (T.S. Basis for LCOs 3.5.1 and 3.5.2) With RCS pressure less than the setpoint, the SIT motor operated isolation valves may be closed to isolate the SITs from the RCS but must remain energized. This allows RCS cooldown and depressurization without discharging the SITs into the RCS or requiring depressurization of the SITs. Test description in UFSAR section 7.6.2.2.2; 4.10

Table 7.6-1
SHUTDOWN COOLING (SDC) SYSTEM AND SAFETY INJECTION TANK (SIT) INTERLOCKS
(Page 3 of 3)

SYSTEM	SETPOINT[a]	FUNCTION and Value[b]
Shutdown Cooling System		
Safety Injection Tank SIT Isolation Valves (continued)		TS: Verify SIT MOV power is removed every 31 days from each required SIT isolation valve operator when RCS pressure is ≥ 1500 psia. (SRs 3.5.1.5 and 3.5.2.5).[c]
		TS: Verify each required SIT isolation MOV is fully open every 12 hours when RCS pressure is ≥ 430 psia. (SRs 3.5.1.1 and 3.5.2.1).[c]
SIT - RCS 1E Differential Alarm	RCS > 690 psia AND SIT < 610 psig	SIT-RCS Differential pressure alarm. 1E alarm if RCS pressure is greater than 715 psia with SIT pressure less than 600 psig. (TSR 3.5.200.5)

(a) Setpoint values listed are the presently installed values determined by the applicable design calculation.

(b) Values listed with the function are from License documents such as the TRM or Technical Specifications.

(c) Acceptance criteria of ≤ 420 psia is used for valves open and power to MOVs removed with breakers locked open, before exceeding 430 psia.

(d) Above the SIT isolation valves auto-open interlock, the maximum pressure at which the SIAS open signal will open a closed valve is limited by the valve operator differential pressure design capability.

7.6.1.2 Design Bases

7.6.1.2.1 Shutdown Cooling System Suction Line Valve Interlocks

The SCS interlocks conform to the following design criteria:

A. Each suction line shall have at least two valves in series to provide isolation between the RCS and the SCS;

B. The isolation valves shall have interlocks to prevent opening the isolation valves while the RCS pressure is above that which would result in the allowable SCS pressure being exceeded;

C. The interlocks shall operate even after a single failure;

D. The interlocks shall not prevent achieving cold shutdown from the control room after a single failure;

E. Pressurizer pressure shall be used to provide the interlock functions;

F. Separate, physically independent sensors, located on separate pressurizer sensing nozzles, shall be provided; and

G. The interlocks must not fail so as to preclude opening of at least one SCS path (if RCS pressure permits), or closing of both suction paths after a LOCA.

7.6.1.2.2 Safety Injection Tank Isolation Valve Interlocks

The SIT Isolation Valve Interlocks are designed consistent with the balance of the SIS. Because the SIS is an ESF System, the ESF criteria take precedence over any applied to the

interlocks. The interlocks conform, generally, to the SIS criteria specified in Section 6.3. The SIT interlocks meet the following criteria:

A. The SITs shall not be isolated from the RCS when RCS pressure exceeds a preset value; the interlocks shall function to automatically open the isolation valves when RCS pressure exceeds a preset value;

B. Pressurizer pressure shall provide the required function;

C. Separate, physically independent, sensors, located on separate pressurizer sensing nozzles, shall be provided;

D. Operating procedures, administrative controls, and the interlocks all insure that the isolation valves are open when pressure in the RCS is greater than a preset value;

E. When system pressure exceeds the setpoint the interlock opens the valve; the SITs must be repressurized prior to RCS pressure reaching 700 psig.

7.6.1.3 Final System Drawings

Refer to section 1.7 for a list of figures applicable to this section and figure 7.6-2.

7.6.2 ANALYSIS

7.6.2.1 Analysis of Design Criteria

7.6.2.1.1 Shutdown Cooling System Suction Line Valve Interlocks

A. The isolation valve interlocks are redundant in that there are two trains; train A has three valves, two receiving their signal from one pressure sensor and the third valve receives its signal from an independent sensor; train B also has three valves but using two different pressure sensors. Each path to each valve will be physically independent and separate from the others. With this degree of redundancy and independence, the interlocks can sustain a single failure and can still isolate both heat exchangers or make one available when required.

B. The interlocks and valves can be tested in accordance with General Design Criteria 1 and 21; Regulatory Guides 1.22, 1.47 and 1.68; and the appropriate sections of IEEE standards 279-1971, 336-1971 and 338-1971.

C. The method for identifying power and signal cables and cable trays dedicated to the instrumentation, control, and electrical equipment associated with the isolation valves will be as discussed in Section 7.1.3.16 and will conform to R.G 1.75 as discussed in Section 7.1.2.10.

D. The instrumentation, control, and electrical equipment associated with the SCS interlocks are seismically and environmentally qualified to operate under all required

design basis events in accordance with the requirements stated in Section 3.10 and 3.11.

7.6.2.1.2 Safety Injection Tank Isolation Valve Interlocks

Because the SIS is an ESF System, the requirements of the General Design Criteria, Regulatory Guides, and IEEE standards appropriate for ESF Systems are used for all of the instrumentation and controls. The interlocks are designed to be consistent with the balance of the system and its requirements. Refer to Section 6.3 for a discussion of the SIS and Section 7.3 for a discussion of the ESFAS.

7.6.2.1.3 Class 1E Alarm System

The Class 1E alarm system utilizes two independent alarm systems, one for each channel. There are no operating bypasses for the 1E alarm system or inputs. An input signal will sound an audible alarm that can be acknowledged (muted) with a switch in the control room. Additionally, the audible alarms for each channel can be "silenced" with the use of a key which is under administrative control. The silence function disables the 1E annunciator system audible alarm which will prevent it from sounding for any new input signal until it is reset.

The instrumentation and input signals are provided in compliance with the requirements of IEEE Standard 279-1971.

7.6.2.1.3.1 <u>Reactor Coolant Pump Cooling Water Supply Monitoring</u>. Monitoring the cooling water flowrate to the reactor coolant pumps with two visual status alarms for each pump on low cooling water flow provides sufficient information to the operator to determine if cooling water is available to each pump

and to take appropriate action in less than 30 minutes to protect the reactor coolant pump affected.

The instrumentation is provided in compliance with the requirements of IEEE Standard 279-1971.

7.6.2.1.3.2 Safety Injection Tank Pressure Monitoring. Monitoring the SIT pressure with two visual status alarms for each channel on low SIT pressure provides information to the operator to determine the unavailability of the SITs to perform their core flooding function in the event of a LOCA. The instrumentation is provided in compliance with the requirements of IEEE 279-1971.

7.6.2.1.3.3 Auxiliary Building ESF Pump Room Level Monitoring. Monitoring each ESF pump room level with one visual status alarm for each room provides sufficient information and 30 minutes of time for the operator to take appropriate action to prevent equipment flooding at a leakage rate of 50 gallons per minute. The instrumentation is provided in compliance with the requirements of IEEE 279-1971, except for the redundancy requirements. These level switches are not required to be environmentally qualified since flooding of these pump rooms will not occur as a result of an initiating event considered by the PVNGS EQ program.

7.6.2.2 Analysis of Equipment Design Criteria

7.6.2.2.1 Shutdown Cooling System Suction Line Valve Interlocks

This description is only of the interlocks. The valves and piping are discussed in Section 5.4.7. The requirements of IEEE 279-1971 are written expressly for protection systems; as

such, they are not directly applicable to these interlocks. However, a discussion of the extent to which these interlocks comply with Section 4 of this standard is provided below:

4.1 General Functional Requirement:

The interlocks are designed to operate during accident environmental conditions.

4.2 Single Failure Criterion:

Any single failure leading to loss of one channel will not result in opening of all of the isolation valves installed in series in one SCS suction line. Loss of two selective interlock channels (both part of one SCS suction line) and violation of administrative controls and procedures is required to open all three isolation valves.

4.3 Quality Control of Components:

The sensors for these interlocks meet the same quality requirements imposed on the protection system sensors.

4.4 Equipment Qualification:

Type tests will be performed on the instrumentation to ensure its operation during expected environmental conditions.

4.5 Channel Integrity:

The interlocks are designed to maintain functional capability during accident environments. Failure of an interlock will not preclude opening a path or closing both paths of the SCS.

4.6 Channel Independence:

The pressure transmitters are located on separate pressurizer nozzles. Separation is maintained between channels.

4.7 Control and Protection System Interaction:

The interlocks have no non-safety control function.

4.8 Derivation of System Inputs:

Pressurizer pressure is the sensed parameter.

4.9 Capability for Sensor Check:

The operational availability of the four pressure sensing channels can be determined by comparing their outputs once pressurizer pressure has come within the range of the sensors.

4.10 Capability for Test and Calibration:

Complete testing capability of the SCS isolation valve interlock exists. The tests will be performed in conjunction with periodic in-service testing and inspection of the valves. The test will include testing of the logic, valve control circuits, and actuation of the individual valves. This testability will be equivalent to the testability required for ESF circuits. A simplified diagram of the logic circuit is shown on Figure 7.6-1.

Testing may be accomplished sequentially for each series valve by inserting a test signal to the bistables, simulating a decreased pressure condition, while holding the control switch in the open position, to the point where the valve partially opens, manually reclosing the valve, simulating an increased pressure condition and observing that the valve does not open when the hand switch is moved to open position.

4.11 Capability for Bypass or Removal from Operation:

Removal of one channel for test does not compromise system reliability. Failure of one of the remaining channels during a test outage would not create an unacceptable situation, since

administrative controls (key locks) effectively preclude inadvertent opening of the valves by the operator.

4.12 through 4.14 Bypassing:

There are no bypasses.

4.15 Multiple Setpoints:

This requirement is not applicable.

4.16 Completion of Protective Action Once it is Initiated:

This requirement is not applicable.

4.17 Manual Initiation:

This requirement is not applicable.

4.18 Access to Setpoint Adjustments, Calibration and Test Points:

Access is controlled by administrative procedures.

4.19 Identification of the Protective Action:

Indication of isolation is provided by redundant valve position indication.

4.20 Information Readout:

The readout consists of four pressure indicators and position indication for four of the six valves.

4.21 System Repair:

Components are accessible for repair, one channel can be placed out of service for maintenance without jeopardizing the isolation of the SCS.

4.22 Identification:

The instrumentation and cables associated with the SCS interlocks will not be uniquely identified as such. The channels will be identified to distinguish between redundant channels of safety-related equipment (See Section 7.1.3.16).

7.6.2.2.2 Safety Injection Tank Isolation Valve Interlocks

The SIS and its design requirements are discussed in Section 6.3. The requirements of IEEE 279-1971 are written expressly for protection systems, and as such, they are not directly applicable to these interlocks. The following discussion refers to the requirements set forth in the respective items of Section 4 of IEEE 279-1971 as they relate to the SIT isolation valve interlocks:

4.1 General Function Requirement:

The interlocks have been designed to operate during accident environmental conditions.

4.2 Single Failure Criterion:

Loss of an interlock channel, at operating pressure, will not cause a valve to close since the valve motor circuit breaker is racked out. At low pressure, if the interlock should fail and an SIT starts to pressurize the RCS, the SCS is protected since the SITs are depressurized to 400 psia prior to initiation of shutdown cooling to prevent an interlock failure from causing such a problem.

4.3 Quality Control of Components:

The sensors for these interlocks meet the same quality requirements imposed on the protection system sensors.

4.4 Equipment Qualification:

Type tests will be performed on the instrumentation to ensure its operation during expected environmental conditions.

4.5 Channel Integrity:

The interlocks have been designed to maintain functional capability when exposed to accident environments. They will not preclude Safety Injection during accident conditions.

4.6 Channel Independence:

The pressure transmitters are located on separate pressurizer nozzles. Separation is maintained between channels.

4.7 Control and Protection System Interaction:

4.8 Derivation of System Inputs:

Pressurizer pressure is the sensed parameter.

4.9 Capability for Sensor Checks:

The operational availability of the two pressure sensing channels can be determined by comparing their outputs.

4.10 Capability for Test and Calibration:

Complete testing capability of the SIT isolation valve interlocks exists. The tests will be performed in conjunction with periodic in-service testing and inspection of the valves. The tests will include testing of the logic, valve control circuits, and actuation of the individual valves. A simplified diagram of the logic circuit is shown on Figure 7.6-1.

Testing may be accomplished sequentially for each valve by inserting a test signal to the bistables, simulating a decreased pressure condition while holding the control switch in the close position, to the point where the valve partially

closes, and then simulating an increased pressure condition to the point where the interlock circuit causes the valve to return to the fully open position. This procedure will then be repeated to allow testing of the SIAS signal to the valve.

4.11 Capability for Bypass or Removal from Operation:

Removal of one channel for test does not compromise system reliability. Failure of one of the remaining channels during a test outage would not create an unacceptable situation, since administrative controls (key locks, racked out breakers, locked open breakers) preclude inadvertent closing of the valves by the operator.

4.12 through 4.14 bypassing:

There are no bypasses.

4.15 Multiple Set Points:

This requirement is not applicable.

4.16 Completion of Protective Action Once Initiated:

This requirement is not applicable.

4.17 Manual Initiation:

This requirement is not applicable.

4.18 Access to Setpoint Adjustments, Calibration and Test Points:

Access is controlled by administrative procedures.

4.19 Identification of the Protective Action:

Identification of isolation is provided by redundant valve position indication.

4.20 Information Readout:

The readout consists of two pressure indicators and position indication for each valve. This provides the operator with clear, concise information.

4.21 System Repair:

The components are accessible for repair. One channel can be placed out of service without jeopardizing the availability of the SITs.

4.22 Identification:

The instrumentation and cables associated with the SIT isolation valve interlocks will not be uniquely identified as such. The channels will be identified to distinguish between channels of safety related equipment (See Section 7.1.3.16).

In addition, for periodic testing requirements, see the Technical Specifications and Technical Requirements Manual (TRM); for access procedures for setpoint adjustments, calibration, and test points, see section 13.5.

7.6.2.3 Fire Protection Instrumentation and Detection System

An analysis of the fire protection system is discussed in subsection 9.5.1.

This page intentionally blank

7.7 CONTROL SYSTEMS NOT REQUIRED FOR SAFETY

Refer to paragraph 7.2.2.4.1 for additional discussion of control systems not required for safety.

7.7.1 DESCRIPTION

The control and instrumentation systems, whose functions are not essential for the safety of the plant, include plant instrumentation and control equipment not addressed in Section 7.2 through 7.6. The general description given below permits an understanding of the reactor and important subsystem control methodology.

The design reactivity feedback properties of the NSSS will inherently cause reactor power to match the total NSSS load. The resulting reactor coolant temperature at which this occurs is a controlled parameter and is adjusted by changes in total reactivity as implemented through CEA position changes or through boric acid concentration changes in the primary coolant.

The ability of the NSSS to follow turbine load changes is dependent on the ability of the control systems or operator to adjust reactivity, feedwater flow, bypass steam flow, reactor coolant inventory, and energy content of the pressurizer such that NSSS conditions remain within normal operating limits.

Except as limited by Xenon conditions, the major control systems described below provide the capability to automatically follow limited load changes. Additionally, these automatic systems provide the capability to accommodate load rejections of any magnitude or the loss of one of two operating feedwater pumps.

7.7.1.1 Control Systems

7.7.1.1.1 Reactivity Control Systems

The reactor's reactivity is controlled by adjustments of CEAs for rapid reactivity changes or by adjustment of boric acid concentration for slow reactivity changes. The boric acid is used to compensate for such long term effects as fuel burnup and changes in fission product concentration. The boric acid concentration can be used to do some load following. Since these long term changes occur slowly, operator action is suitable for boric acid concentration control. The CEAs can either be controlled manually by the operator or automatically to maintain the programmed reactor coolant temperature and power level during boric acid concentration changes, within the limits of CEA travel.

The Reactor Regulating System (RRS) is used to automatically adjust reactor power and reactor coolant temperature to follow turbine load transients within established limits. The RRS receives a turbine load index signal (linear indication of load) and reactor coolant temperature signals (see Figure 7.7-5). The turbine load index is supplied to a reference temperature (T_{REF}) program which establishes the desired average temperature. The hot leg and cold leg temperature signals are averaged (T_{AVG}) in the RRS. The T_{REF} signal is then subtracted from the T_{AVG}, signal to provide a temperature error signal. Power range neutron flux is subtracted from the turbine load index to provide compensation to the T_{AVG} - T_{REF} error signal generated.

This resulting error signal is fed to a CEA rate program, to determine whether the CEAs are to be moved at a high or low

rate, and to a CEA status program which determines if the CEAs are to be withdrawn, inserted or held. The outputs of the rate and status programs are sent to the Control Element Drive Mechanism Control System (CEDMCS).

If the temperature error signal is very high, that is T_{AVG} is much higher than T_{REF}, an Automatic Withdrawal Prohibit (AWP) signal will be sent to the CEDMCS. Since the withdrawal of CEAs causes T_{AVG} to increase, prohibiting a withdrawal prevents an increase in the error signal.

The Control Element Drive Mechanism Control System (CEDMCS) accepts automatic CEA motion demand signals from the Reactor Regulating System or manual motion signals from the CEDMCS Operators Module and converts these signals to direct current pulses that are transmitted to the CEDM coils to cause CEA motion.

A reactor trip initiated by the Reactor Protective System causes the input motive power to be removed from the CEDMCS by the trip switchgear, which in turn causes all CEAs to be inserted by gravity. The CEDMCS is thus not required for safety. (See Figure 7.7-6).

There are four different modes of control; sequential group movement in manual and automatic control, manual group movement and manual individual CEA movement. Sequential group movement functions such that, when the moving group reaches a programmed low (high) position, the next group begins inserting (withdrawing), thus providing for overlapping motion of the regulating groups. The initial group stops upon reaching its lower (upper) limit. Applied successively to all regulating groups, the procedure allows a smooth continuous rate of change

of reactivity. The CEDMCS accepts signals from the Plant Monitoring System (PMS) to effect this sequencing of regulating CEA group motion. The CEDMCS utilizes sequencing signals from the PMS that are derived from the CEDMCS up-down pulse counters. The shutdown CEAs are moved in the manual control mode only, with either individual or group-movement. A selector switch permits withdrawal of no more than one shutdown group at any time.

The part-strength CEAs may be moved manually, with either individual or group movement.

During plant startup and shutdown, and all cases where power is below 15%, manual control is used. Automatic control of the regulating CEAs by the RRS may be selected by the operator only when above 15% power. Manual control may be used to override automatic control at any time.

7.7.1.1.2 Reactor Coolant System Pressure Control System

The Pressurizer Pressure Control System (PPCS) maintains the Reactor Coolant System pressure within specified limits by the use of pressurizer heaters and spray valves. The pressurizer provides a water/steam surge volume to minimize pressure variations due to density changes in the coolant. The pressurizer is described in Section 5.4.10.

A pressurizer pressure signal is used in a proportional controller to control the proportional heaters (see Figure 7.7-7). The heaters will be operated to maintain the pressurizer pressure as required. The operator can take manual control to regulate the pressure.

The pressurizer pressure signal is also sent to a spray valve controller. This provides a signal to the spray valves to control their opening. Since reactor coolant is somewhat cooler than the water/steam mixture, reactor coolant sprayed in will cause some steam to condense and thereby reduce the system pressure. The operator can take manual control of the spray valves to control the pressure.

If the proportional heaters are being used, and system pressure is still decreasing, the backup heaters would be automatically energized. The operator can also manually energize these backup heaters.

The control system has a low level interlock and a high pressure interlock. The low level interlock shuts off the heaters when the level falls below a setpoint.

If the pressurizer pressure reaches a high setpoint, all heaters will be deenergized; this is to ensure that the heaters will not cause the pressure to increase further.

7.7.1.1.3 Pressurizer Level Control System

The Pressurizer Level Control System (PLCS) minimizes changes in RCS coolant inventory by using the charging pumps and letdown control valves in the Chemical and Volume Control System (CVCS) discussed in Section 9.3.4. It also maintains a vapor volume in the pressurizer to accommodate surges during transients. Figure 7.7-8 shows the PLCS diagram.

During normal operations the level is programmed as a function of reactor coolant average temperature (T_{AVG}) in order to minimize charging and letdown flow requirements. The T_{AVG} goes through a level setpoint program and the setpoint program

signal is compared to the actual level signal. The level error signal is sent to a level error program which is used to control the charging pumps.

If the level error program shows that the level is very high it will deenergize a normally running pump leaving only one pump (the always running pump) running. If the level is very low the level error program will cause the standby pump to start, thereby having three pumps charging the system.

The level error signal is sent to a Proportional plus Integral plus Derivative (PID) controller which generates an error signal. This signal is passed through a lag circuit which prevents rapid changes in the letdown flow. The output of the lag circuit is passed to the selected letdown valve via the auto-manual control and the letdown valve selector. The auto-manual control allows the operator to control level manually by controlling the letdown valve. The letdown valve selector switch allows the operator to select which valve will be operated by the PLCS.

7.7.1.1.4 Feedwater Control System

The Digital Feedwater Control System (DFWCS) has a separate compound, or software control strategy, for each steam generator. The discussion of the FWCS will refer to only one steam generator. Refer to Figure 7.7-1 for the FWCS block diagram.

The DFWCS is based on a two-mode control strategy. At low power levels, the DFWCS is designed to automatically control the steam generator downcomer water level in a Single-Element mode. The DFWCS performs dynamic compensation on the level

signal to generate an output signal indicative of the required feedwater flow. The output signal is used to generate the downcomer valve position demand signal. When in this control mode the economizer valve will be closed and the pump speed setpoint will be at its minimum value. Steam generator level will be controlled during 1% per minute turbine load ramps in this mode (assuming that all other control systems are operating in automatic).

The DFWCS is designed to automatically control the steam generator downcomer water level at higher levels in a Three-Element mode. The Three-Element mode continuously solves the steam generator mass balance equation to keep the feedwater input equal to the steam flow output. The level measurement acts as a trim on this mass balance and assures that the level is reset to its proper setpoint value following any system disturbances. Thus, the three modes are level, feedwater flow, and steam flow. The gain and reset control settings are adaptively adjusted by reactor power and feedwater temperature to adjust control response for the "shrink/swell" phenomenon. Steam generator level will be controlled during the following conditions (assuming that all other control systems are operating in automatic):

A. Steady state operations;

B. 5% per minute turbine load ramps between 15 and 100% NSSS power;

C. 10% turbine load steps;

D. Loss of one of two operating feedwater pumps; and

E. Load rejection of any magnitude.

Transfer from Single-Element to Three-Element control, and back, is performed bumplessly without any need for operator balancing or other intervention. The transfer occurs automatically and is based on NSSS power. The transfer to Three-Element control occurs as soon as the stability of the steam and feedwater measurement will allow.

Panel Display Stations provide the operator interface with the DFWCS. The operator may use either interface to provide the steam generator level setpoint at the master control station or manually control the economizer and downcomer valve positions.

The signal from the master control station also goes to a high select circuit which selects the higher of the total feedwater demand signals from both feedwater systems and passes it to the pump program. The pump program generates a pump speed setpoint signal. A panel display station provides the operator with access to the pump speed bias to allow balancing of the pumps. The operator can also manually control the pump speed at this station.

7.7.1.1.5 Steam Bypass Control System

The Turbine Bypass System consists primarily of the turbine bypass valves and the Steam Bypass Control System (SBCS). The SBCS controls the positioning of the turbine bypass valves, through which steam is bypassed around the turbine into the unit condenser, with exception of two valves which dump steam to atmosphere. These two valves are the last to open and first to close during steam bypass operation.

The system is designed to increase plant availability by making full utilization of turbine bypass capacity to remove excess NSSS thermal energy following turbine load rejections with condenser available. This is achieved by the selective use of turbine bypass valves and the controlled release of steam. This avoids unnecessary reactor trips, and prevents the opening of pressurizer or secondary safety valves.

Refer to Figure 7.7-2 for the SBCS block diagram. The Reactor Power Cutback System, discussed below, is used in conjunction with the SBCS to reduce the required turbine bypass valve capacity. Additionally, the SBCS is used during turbine loading to provide an even load on the reactor as the turbine is brought up to load. The system is also used during reactor heatup and cooldown to remove excess NSSS energy, and control the rate of temperature change.

The following three types of valve signals are generated for each turbine bypass valve a modulation signal which controls the flow rate through the valve; a quick opening signal which causes the valve to fully open in a short time; and a valve permissive signal which is required for the preceding two signals to operate the bypass valve.

In the modulation mode a steam flow signal is sent to a program which develops a main steam header pressure program signal. At the same time the pressurizer pressure is used to generate a pressurizer pressure bias program. The two program signals and the measured main steam header pressure are compared to provide an error signal which goes to the controller. The controller demand, or a manual signal provided by the operator, is passed to an electro-pneumatic converter on each turbine bypass valve. This converts the electrical signal to an air signal which is

passed through the first solenoid valve to the air actuated turbine bypass valve shown on Figure 7.7-2.

In the quick opening mode the pressurizer pressure and steam flow signals are compared and the difference signal produced is sent to a change detector. The change detector output is compared to a threshold value; if the change signal exceeds the threshold a quick opening signal is produced. The quick opening signal energizes the solenoid which then blocks the modulated air signal and applies the full air system pressure, to quick open the valve.

A permissive signal is also produced by the SBCS. This signal is provided by circuitry identical to that described above except that the output of the permissive controller is converted to a binary signal and fed into an OR gate with the permissive quick opening signal. If a permissive signal is present it will open the second solenoid valve and allow either the modulated or the quick open air signal to be applied to the pneumatically operated bypass valves. When the permissive signal is removed the control air is vented to atmosphere and the valve closes. When turbine condenser pressure exceeds a present value, the turbine bypass valves are prevented from opening.

Reactor Power Cutback demand signals are generated by the same circuitry that produces the valve quick opening signals. These redundant signals are sent to the Reactor Power Cutback System (RPCS).

7.7.1.1.6 Reactor Power Cutback System

The NSSS normally operates with minor perturbations in power and flow. These can be handled by the control systems discussed above. Certain large plant imbalances can occur however, such as a large turbine load rejection, turbine trip or loss of one of two main feedwater pumps. Under these conditions maintaining the NSSS within the control band ranges can be accomplished by rapid reduction of NSSS power at a rate which is greater than that provided by the normal high speed CEA insertion. Refer to Figure 7.7-4 for the block diagram of the Reactor Power Cutback System (RPCS).

The RPCS is a control system designed to accommodate certain types of imbalances by providing a "step" reduction in reactor power. The step reduction in reactor power is accomplished by the simultaneous dropping of one or more preselected groups of full strength regulating CEAs into the core. The CEA groups are dropped in their normal sequence of insertion. The RPCS also provides control signals to the turbine to rebalance turbine and reactor power following the initial reduction in reactor power as well as to restore steam generator water level and pressure to their normal controlled values. The system is designed to accommodate either large load rejections or the loss of one feedwater pump.

The RPCS receives two of each of the following signals; loss of feedwater pump 1, loss of feedwater pump 2 and two cutback demand signals from the SBCS. A two-out-of-two logic is required to actuate the system. The operator has the capability to manually actuate the system.

The operator inputs the CEA group drop selection through the RPCS operator's console. Input indication is provided for selection of all CEA subgroups. However, only CEA groups 4 and/or 5 (subgroups 22, 5 and/or 4) are capable of selection for drop.

The RPCS is actuated upon receiving coincident two-out-of-two sensor logic signals indicating either large turbine load rejection or loss of one main feedwater pump. The actuation initiates the dropping of the preselected pattern of CEAs. There are inhibits in the Control Element Drive Mechanisms Control System (CEDMCS) to prevent the possibility of the RPCS dropping CEA groups which are not intended to drop for a reactor power cutback (e.g., Part-Strength groups, Shutdown Groups, etc.). Subsequent insertion of other groups either automatically by the Reactor Regulating System (RRS) or manually by the operator occurs as necessary. The actuation logic also temporarily changes plant control to a turbine follow mode by first initiating a rapid turbine power reduction to approximately 60% power, followed by a further reduction if necessary to balance turbine power with reactor power.

7.7.1.1.7 Boron Control System

Boron Concentration, via regular sampling of the reactor coolant is supplied to the operator to allow regulation and monitoring of the boron concentration in the reactor coolant. The means by which RCS boron control is accomplished is by dilution and boration. Refer to Section 9.3.4 for a discussion of the Chemical and Volume Control System (CVCS). To allow the operator to maintain the required boron concentration in the

reactor coolant, the Volume Control Tank contents may be maintained at a prescribed boron concentration either manually or automatically. Additional recorders indicate reactor makeup water flow and boric acid makeup flow, which can be used to determine whether boration or dilution is occurring.

At power, the boron concentration, in addition to CEA position determines reactor coolant temperature. Because of the long time required to change the boron concentration, the boron is used for long term effects such as fuel burnup and fission product build up. Boron concentration control can also be used for load following. By adjusting the boron concentration, the CEAs can be withdrawn to provide an adequate shutdown margin.

7.7.1.1.8 Loose Parts Monitoring System

Refer to Section 4.2.5.H.2.

A loose parts monitoring system (LPMS) is installed at PVNGS. The LPMS is designed to detect and record signals resulting from impacts occurring within the reactor coolant system. Eight transducers will be located in the areas where loose parts are most likely to become entrapped. These are:

A. Two redundant transducers clamp-mounted on the incore instrument guide tubes on the reactor vessel lower head, diametrically opposed.

B. Two redundant transducers mounted diametrically opposed on the reactor head.

C. Two redundant transducers on each steam generator. The transducers are mounted on the outer diameter in the tube sheet region.

Experience has shown that the exact location of the accelerometers is not critical since the acoustic wave that results from an impact propagates throughout the entire head. The transducers will be high temperature piezoelectric accelerometers.

A high temperature, low noise, radiation hardened, flame-retardant coaxial cable will connect the accelerometer to a preamplifier located in a junction box outside of the biological shield. From the preamplifier the signals are sent via suitable wires, such as a twisted shielded pair, to the data acquisition panel in the control room. Cabling between redundant sensor channels from the sensor to the preamplifier located outside the secondary shield wall will be physically separated from each other.

A data acquisition panel located in the control room area contains alarm modules that continually monitor the incoming signals from the preamplifier for the presence of impacting.

The alarm level for each accelerometer is determined by a setpoint adjustment. Alarm levels were initially set above background levels established during baseline "signature" testing. Further baseline testing will be conducted from time to time and alarm levels may be adjusted to compensate for age-related noise generation at 100% power. The system sensitivity is better than 0.05 ft-lb at the sensors. Initial alarm setting is 0.5 $\pm$0.25 ft-lb. The occurrence of a loose part impacting on the inside of the structure causes bursts of signals that exceed the alarm setpoint and trigger the alarm. The data acquisition panel includes signal recording with playback and an audio monitor of live signal.

7.7.1.1.8.1 Recording. A digital recording system is provided, which includes an event analysis computer for analyzing the collected data. Signals from all channels are continually sampled. Storage time intervals are dependent upon the sampling rate and memory capacity of the analysis computer. This computer performs data acquisition and recording and provides alarm indication on a control room annunciator to indicate a loose part event. It is capable of real-time analysis, spectrum analysis, and produces X-Y plot displays including an amplitude and frequency cursor with digital readout on an oscilloscope-type display.

7.7.1.1.8.2 Audio Monitoring. The audio monitoring shall consist of a speaker, independent volume control, and a selector switch for monitoring the loose parts channels.

7.7.1.1.8.3 Sensor Channel Operability and Functional Test. A preoperational calibration and functional test will be performed. Baseline "signatures" of each channel will be obtained to establish background levels. Provision is made for channel operability tests and for channel functional tests. System calibration shall be performed at least once each 18 months. Diagnostic procedures to confirm the presence of loose parts will make use of the baseline "signatures" to verify that recorded impact signals are above background.

7.7.1.1.8.4 Operability for Seismic Conditions. The loose part detection system has been shown to be adequate for the OBE by test. Power is supplied from a 120 V-ac normal (nonseismically qualified) instrument bus, which has a Class 1E backup source.

All components of the system are high reliability items. They are to remain operable under normal environmental conditions of the plant and are readily accessible for servicing (except sensors). Replacement of components, if any, at full power operation would be limited to the channel preamplifiers located outside the secondary shield wall. The preamplifiers are replaceable during full power operation. The only other components of the loose parts monitoring system located in containment are cables and the sensors. Equipment located in the control room is not subject to the environment of the containment and is readily accessible and repairable at all times.

7.7.1.1.8.5 Training Program for Plant Personnel. See paragraph 13.2.1.

7.7.1.1.9 In-Core Instrumentation System

The in-core instrumentation system is used to monitor the core power distribution.

There are 50 in-core monitoring assemblies with five self-powered Rhodium detectors in each location. The 50 assemblies are strategically distributed about the reactor core, and the five detectors are axially distributed along the length of the core at 10, 30, 50, 70 and 90% of core height. This permits representative three dimensional flux mapping of the core. The Rhodium detectors produce a delayed beta current proportional to the neutron activation of the detectors which is proportional to the neutron flux in the detector region.

The signals from the in-core detectors are converted to usable voltage signals by the In-Core Amplifier System which sends

these signals to the Plant Monitoring Systems (PMS) by way of multiplexers. The PMS converts these analog voltages to equivalent digital signals and performs the background, beta decay delay and Rhodium depletion compensation using digital signal processing routines.

The fixed in-core instrumentation system is designed to perform the following functions:

A. To determine the gross power distribution in the core during different operating conditions from 20% to 100% power;

B. To provide data to estimate fuel burn-up in each fuel assembly;

C. To provide data for the evaluation of thermal margins in the core;

The fixed in-core detectors can be used to assist in the calibration of the ex-core detectors by providing azimuthal and axial power distribution information. The ex-core system is used to provide indication of the flux power and axial distribution for the Reactor Protective System.

7.7.1.1.10 Excore Neutron Flux Monitoring System (Non-Safety Channels)

The ex-core neutron flux monitoring system includes neutron detectors located around the reactor core and signal conditioning equipment located in the control room area. Neutron flux is monitored from source levels through full power operation and signal outputs are provided for reactor control and for information display.

Two startup channels provide source level neutron flux information to the reactor operator for use during extended shutdown periods, initial reactor startup, startups after extended shutdown periods, and following reactor refueling operations. Each channel consists of a dual section proportional counter assembly, with each section having multiple BF_3 proportional counters, one preamplifier located outside the reactor shield, and a signal processing drawer containing power supplies, a logarithmic amplifier, and test circuitry. High voltage power to the proportional counters is terminated several decades of neutron flux above the source level to extend detector life. These channels provide readout and audio count rate information but have no direct control or protective functions.

Two control channels provide neutron flux information, in the power operating range of 1% to 125%, to the Reactor Regulating System for use during automatic turbine load-following operation (see Section 7.7.1.1.1). Each control channel consists of a dual section uncompensated ionization chamber detector and a signal conditioning drawer containing power supplies, a linear amplifier, and test circuitry. The detector is operated in the current mode only. These channels are completely independent of the safety channels.

7.7.1.1.11 Boron Dilution Alarm System

Reactivity control in the reactor core is effected, in part, by soluble boron in reactor coolant system. The Boron Dilution Alarm System (Figure 7.7-11) utilizes the startup channel nuclear instrumentation signals to detect a possible inadvertent boron dilution event while in Modes 3-6. There are

two redundant and independent channels in the Boron Dilution Alarm System (BDAS) to ensure detection and alarming of the event.

The BDAS contains logic which will detect a possible inadvertent boron dilution event by monitoring the startup channel neutron flux indications. When these neutron flux signals increase (during shutdown) to equal or greater than the calculated alarm setpoint, alarm signals are initiated to the Plant Annunciation System. The alarm setpoint is periodically, automatically lowered to be a fixed amount above the current neutron flux signal. The alarm setpoint will only follow decreasing or steady flux levels, not an increasing signal. The current neutron flux indication and alarm setpoint (per channel) are displayed. There is also a reset capability to allow the operator to acknowledge the alarm and initialize the system.

7.7.1.2 Design Comparison

The functional design of the following, non-safety, control systems was performed by Combustion Engineering. The design differences between the control systems in the CESSAR Licensing scope and the control systems provided for the reference plant (Arkansas Nuclear One - Unit 2 - (ANO-2) NRC Docket No. 50-368) are discussed in this section.

7.7.1.2.1 Reactivity Control Systems

The RRS is functionally identical to that of the reference plant with the following changes:

A. It does not use pressurizer pressure for compensation;

B. An AMI signal is produced to prevent CEA motion whenever there is a deviation between any pair of redundant input signals; and

C. There is only one RRS instead of two.

The CEDMCS is functionally identically to that of the reference plant with the following changes:

A. The CEDMs can be deenergized in groups, by signals from the RPCS;

B. The two power buses are tied together within the CEDMCS cabinets;

C. System has a four coil, double-step CEDM instead of a five coil, single step;

D. Only one subgroup can be transferred to the hold bus at any one time;

E. The CWP is effective in all modes, and CWP can be bypassed at the Operator's Module;

F. UCL and LCL are replaced with UGS and LGS for the PLCEA; and

G. System can handle up to 97 CEAs as opposed to 81.

None of the design differences in the RRS or CEDMCS have been taken credit for in the safety analysis since they have no safety significance.

7.7.1.2.2 Reactor Coolant Pressure Control System

The PPCS is functionally identical to that used in the reference plant.

7.7.1.2.3 Pressurizer Level Control System

The PLCS is functionally identical to that used in the reference plant.

7.7.1.2.4 Feedwater Control System

The FWCS is functionally identical to the reference plant with the following exceptions:

A. This system is designed for a U-tube steam generator with an integral economizer, the reference system's U-tube steam generators do not have an economizer;

B. This system controls feedwater to the upper (downcomer) and lower (economizer) steam generator nozzles; and

C. Each nozzle has one valve to control instead of a main and bypass valve for a single nozzle.

None of these design differences discussed above have been taken credit for in the safety analysis since they have no safety significance.

7.7.1.2.5 Steam Bypass Control System

The SBCS has the following design differences from the Steam Dump and Bypass Control System (SDBCS) of the reference plant.

A. This system controls eight turbine bypass valves, the SDBCS controls three turbine bypass valves and four atmospheric dump valves;

B. Signals are provided to the RPCS upon a major load rejection.

Neither of these design differences have been taken credit for in the safety analysis since they have no safety significance.

7.7.1.2.6 Reactor Power Cutback System

The RPCS did not exist in the reference plant. It has not been taken credit for in the Safety Analysis.

7.7.1.2.7 Boron Control System

The BCS is functionally identical to that used in the reference plant.

7.7.1.2.8 In-Core Instrumentation System

The in-core instrumentation system is functionally identical to that of the reference plant with the following changes:

A. There are 50 in-core instrument assemblies being credited rather than 44; and

B. The in-core instrumentation system is designed for bottom rather than top entry.

None of these design differences have been taken credit for in the safety analysis since they have no safety significance.

7.7.1.2.9 Ex-Core Neutron Flux Monitoring System

The ex-core monitoring system is identical to the reference plant except that it uses uncompensated ion chambers instead of fission chambers for the control channel detectors. This difference has no impact on the functioning of the system and has no safety significance.

7.7.1.2.10 Boron Dilution Alarm System

The Boron Dilution Alarm System is an addition to the CESSAR design. There is no functional comparison to the reference plant.

7.7.1.3 Monitoring Systems

7.7.1.3.1 Core Operating Limit Supervisory System (COLSS)

7.7.1.3.1.1. General. The core operating limit supervisory system (COLSS) consists of process instrumentation and algorithms used to continually monitor the limiting conditions for operation on:

- Linear heat rate margin
- DNBR margin
- Total core power
- Azimuthal tilt
- Axial shape index

The COLSS continually calculates DNBR margin, linear heat rate margin, total core power, core average axial shape index, and azimuthal tilt magnitude, and compares the calculated values to the limiting condition for operation on these parameters. If a limiting condition for operation is exceeded for any of these parameters, COLSS alarms are initiated and operator action is taken as required by Technical Specifications.

The limiting safety system settings, core power operating limits, axial shape index, and the azimuthal tilt operating limit are specified such that the following criteria are met:

- No safety limit will be exceeded as a result of anticipated operational occurrences (AOOs).
- The consequences of postulated accidents will be acceptable.

The reactor protective system functions to initiate a reactor trip at the specified limiting safety system settings. The COLSS is not required for plant safety since it does not initiate any direct safety-related function during AOOs or postulated accidents. The Technical Specifications define the limiting conditions for operation (LCO) required to ensure that reactor core conditions during operation are no more severe than the initial conditions assumed in the safety analyses and in the design of the low DNBR and high LPD trips. The COLSS serves to monitor reactor core conditions in an efficient manner and provides indication and alarm functions to aid the operator in maintenance of core conditions within the LCOs given in the Technical Specifications.

The COLSS algorithms are executed in the plant monitoring system (PMS). The calculational speed and capacity of the PMS computer enable numerous separate plant operating parameters to be integrated into three easily monitored parameters: (1) margin to core power limit (based upon DNBR, linear heat rate, and power limits), (2) azimuthal tilt, and (3) axial shape index. If COLSS were not provided, maintenance of reactor core parameters within the LCOs, as defined by the Technical Specifications, would be accomplished by monitoring and alarming based on the separate nonsafety-related process parameters used in the COLSS calculations. Therefore, the essential difference in using COLSS in lieu of previous

monitoring concepts is the integration of many separate process parameters into a few easily monitored parameters. The conciseness of the COLSS displays has distinct operational advantages, since the number of parameters that must be monitored by the operator is reduced.

Detailed process testing of COLSS is conducted to ensure proper system performance as described below:

A. After installation of revised COLSS software algorithms in the PMS computer, appropriate test cases are run on the computer to verify the COLSS implementation; the number of test cases may vary from 1 to approximately 43 depending on the software change(s) made. In test tests, COLSS is off-line (in the TEST mode) and sets of stored constants are substituted for live sensor inputs. These test cases are designed to test the functionality of the module(s) containing the algorithm(s). Agreement of test case results to within round-off errors indicates that the COLSS software is functioning and implemented properly.

B. Just prior to startup from a refueling outage, new constants from a Quality Assured analysis are installed in the PMS.

C. When COLSS is on-line (in the SCHEDULED mode), a detailed report of the COLSS inputs, intermediate calculated values, and results may be printed upon request. Comparison of this information with intermediate calculated values and results from an off-line COLSS program using the same input values can

provide additional assurance of proper operability of the COLSS program. Testing can be performed on an as needed basis under administrative control to assure proper performance of COLSS. Since COLSS is not required for plant safety, COLSS testing requirements are not included in the Technical Specifications (however, the Technical Specifications do include verification of certain COLSS alarms).

7.7.1.3.1.2 System Description. Sensor validity checks are performed by COLSS on those measured input parameters used in the COLSS calculations. The validity checks consist of checking sensor inputs for the following conditions:

- Sensor out-of-range
- Excessive deviation between like sensors

One of the following actions is taken for out of range sensors:

A. Automatic replacement of the failed sensor by an equivalent sensor (when available).

B. Automatic function termination when adequate process information is not available.

C. Substitution of constants for selected COLSS inputs (performed under administrative control).

If an out-of-range sensor is detected, an alarm to the operator is actuated and corrective action is automatically initiated.

A more detailed discussion of sensor validity checks is included in CEN-312, Revision 01-P.[1]

The core power distribution is continually monitored by COLSS, and the core average axial shape index is computed. Operation of the reactor with the calculated ASI within the specified axial shape index limits assures that the actual value of core average axial shape index is within the range of values used in the safety analysis. A core power operating limit based on linear heat rate is computed from the core power distribution. Operation of the reactor at or below this power operating limit assures that the peak linear heat rate is never more adverse than that postulated in the loss of coolant analyses.

Core parameters affecting the DNBR margin are continually monitored by COLSS, and a core power operating limit based on DNBR is computed. Operation of the reactor at or below this operating limit power level ensures that the most limiting DNB transient that can result from an AOO does not result in a DNBR reduction to a value less than the DNBR SAFDL.

A core power operating limit based on licensed power level is also monitored by COLSS. When the COLSS-auctioneered reactor power exceeds the license power limit setpoint (COLSS addressable constant NKLPL), an alarm is generated. Due to normal fluctuations in the process variables used to calculate reactor power from COLSS, normal full power operation without alarm actuation requires an NKLPL setpoint > 100%. The NKLPL setpoint is determined by station procedures using a statistical analysis of COLSS calculated plant powers, with the objective to avoid nuisance alarms and still provide early warning to the operators of the need to reduce power. As required by station procedures, the Licensed Operators have the responsibility to ensure that steady state reactor power is maintained less than or equal to the licensed power limit.

Operation of the reactor at or below 100% power ensures that the total core power is never greater than that assumed as an initial condition in the safety analysis.

Axial shape index, core power, and the core power operating limits based on peak linear heat rate and DNBR are continually indicated on the control board. The margin between the core power and the lowest core power operating limit is also displayed on the control board indicator. An alarm is initiated if the COLSS calculated core power level exceeds a COLSS calculated core power operating limit or if the calculated axial shape index exceeds its limits.

In addition to the above calculations, the azimuthal flux tilt is calculated in COLSS. The azimuthal flux is not directly monitored by the plant protection system; rather an azimuthal flux tilt allowance, based on the maximum tilt anticipated to exist during normal operation, is provided as an addressable constant in the protection system. This tilt allowance is used in the low DNBR and high local power density trip calculations. The azimuthal flux tilt is continually monitored by COLSS and an alarm initiated in the event that the azimuthal flux tilt exceeds the azimuthal flux tilt allowance setting in the plant protection system.

The following are calculated by COLSS:

- Reactor coolant volumetric flowrate
- Core power as determined by:

  Reactor coolant ΔT

  Secondary system calorimetric

  Turbine first stage pressure
- Axial shape index
- Azimuthal tilt
- Linear heat rate core power operating limit
- DNBR core power operating limit
- Margin to each core power operating limit

Control board indication of the following COLSS parameters is continually available to the operator.

- Linear heat rate core power operating limit
- DNBR core power operating limit
- Total core power
- Margin between core power and lowest core power operating limit
- Axial shape index

The algorithms are executed in the PMS. Technical Specifications for the reactor core provide an alternate means of monitoring the limiting conditions for operation in the event that the PMS is out of service.

COLSS alarms are initiated if:

- Core power exceeds a core power operating limit
- Axial shape index exceeds its limits
- Azimuthal flux tilt exceeds azimuthal flux tilt limit

A description of COLSS algorithms and a discussion of the treatment of COLSS input information are included in reference 1. Table 7.7-1 provides a listing of the types, quantities, and ranges of sensors that provide input information for the COLSS algorithms.

A functional block diagram of the core operating limit supervisory system is presented in Figure 7.7-3.

7.7.1.3.1.3 Description of COLSS Algorithms.

7.7.1.3.1.3.1 Reactor Coolant Volumetric Flowrate. The DNBR margin is a function of the reactor coolant volumetric flowrate. The four reactor coolant pump rotational speed signals and four RCP differential pressure instruments are monitored by COLSS and used to calculate the volumetric flowrate. The pump characteristics are determined from testing conducted at the pump manufacturer's test facility and correlations between the pump rotational speed, pump differential pressure, and the volumetric flowrate are developed. Measurement uncertainties in the pump testing and COLSS measurement channel uncertainties are factored into the calculation of the margin to a power operating limit. The four pump volumetric flowrates are summed to obtain the reactor vessel volumetric flowrate. Necessary allowances for core bypass flow, flow factors, reactor coolant temperature, etc.,

are factored into the value of flow used in the DNBR calculation.

7.7.1.3.1.3.2 Core Power Calculation. The reactor coolant ΔT power, turbine power, and the secondary calorimetric power are computed in COLSS. The reactor coolant ΔT power and turbine power are less complex algorithms than the secondary calorimetric power and are performed at a more frequent interval. The secondary calorimetric power is used as a standard against which reactor coolant ΔT power and turbine power are continually calibrated.

Table 7.7-1

COLSS MONITORED PLANT VARIABLES

Monitored Parameters	COLSS Sensors	Number of Sensors	Sensor Range
Core volumetric flow	RCP rotational speed	2 per pump	0 to 1,320 rpm
	RCP differential pressure	2 per pump	0 to 150 psid
Core power			
Primary calorimetric	Cold leg temperature	1 per cold leg	Narrow range (2) 500 to 650F Wide range (2) 0 to 600F
	Hot leg temperature	1 per hot leg	500 to 650F
Secondary calorimetric	Feedwater flow	1 per generator	0 to 10.0×10^6 lbm/hr
	Steam flow	2 per generator	0 to 5.0×10^6 lbm/hr
	Feedwater temperature	1 per generator	0 to 500F
	Steam pressure	1 per generator	900 to 1,300 psia
Core power distribution	In-core monitoring system	50 in-core assemblies each containing 5 axial stacked detectors	NA[a]
	CEA group position	1 per CEA group	0 to 150 inches
Reactor coolant pressure	Pressurizer pressure	2 (on pressurizer)	1,500 to 2,500 psia
Turbine power	Turbine first stage pressure	1 (on turbine)	0 to 800 psig

a. Core power distribution is provided in a graphic format.

This arrangement provides the benefits of the secondary calorimetric accuracy and the faster dynamic response characteristics of the reactor coolant ΔT power and turbine power.

The reactor coolant ΔT power is calculated based on the reactor coolant volumetric flowrate, the reactor coolant cold leg temperature, and the reactor coolant hot leg temperature. ΔT power provides a leading indication of core power changes in response to reactivity changes.

The turbine power is calculated based on turbine first stage pressure. Turbine power provides a leading indication of core power changes in response to load changes.

The secondary calorimetric power is based on measurements of feedwater flowrate, feedwater temperature, steam flow, and steam pressure. A detailed energy balance is performed for each steam generator. The energy output of the two steam generators is summed and allowances made for reactor coolant pump heat, pressurizer heaters, and primary and secondary system energy losses.

7.7.1.3.1.3.3 COLSS Determination of Power Distribution. The determination of the 3-D peaking factor, the integrated radial peaking factor, the power shape in the hottest channel, and the azimuthal tilt magnitude is performed based on in-core measurements of the flux distribution, processed by pre-programmed algorithms and stored constants. A brief description is given here of the data processing approach employed by COLSS to yield the desired power distribution

information. This analysis is repeated at least once per minute, and thus represents continual on-line monitoring.

The dynamic response characteristic of the self-powered rhodium in-core detectors is a function of both prompt and delayed components of electrical current generated in the detector and cabling. The delayed portion of the current signal is governed by the decay of isotopes of rhodium having half-lives of 0.7 minutes and 4.4 minutes. To provide the capability to compensate for the delayed portion of the signal, the COLSS power distribution determination includes a compensation algorithm for the in-core signals used as input to COLSS. The algorithm approximately represents the inverse of the in-core detector dynamic response, such that the combination of detector response and dynamic compensation produces a signal representative of the actual neutron flux response.

The capability for signal filtering is provided through selection of algorithm constants. With the capability for dynamic compensation and filtering on the in-core signals, changes in local flux level during operational load follow transients are adequately represented by the COLSS power distribution determination.

Following correction of the fixed detector signals for background and burnup, five axially distinct region-average power integrals corresponding to the five rhodium detector segments are constructed, taking into account signal-to-power conversion factors which are a function of burnup in the surrounding fuel. The five power integrals are expanded into a forty node core average axial power distribution using a Fourier series technique.

Employing tables of factors relating power in the hot pin to the core average, the axial power profile in the hot pin is computed.

Malpositioning of a CEA or CEA group, the uncontrolled insertion or withdrawal of a CEA or CEA group, or a dropped CEA will be detected by COLSS with inputs received from the pulse-counting CEA position indicating system. Should these deviations occur, adjustments to the planar radial peaking factors are performed to ensure that the COLSS DNBR and peak linear heat rate calculations remain conservative. It is noted that COLSS only provides a monitoring function and therefore has only the function of informing the operator of such deviations. Any protective action required for the CEA-related events is provided by the RPS.

Flux tilts are detected by comparison of signals from symmetrically located sets of fixed in-core detectors, at various levels in the core. The flux tilts are included in the computation of margin to the power operating limit. In this way, postulated nonseparable asymmetric xenon shifts are identified and reflected in the power distribution assessment. Alarms are provided by COLSS when the xenon tilt exceeds the allowances for these effects carried in the core protection calculators as a penalty, or when it exceeds an absolute limit (imposed by the Technical Specifications) indicating possible power distribution abnormality.

The possibility of inoperable fixed in-core detectors is allowed for by provision of redundant detector strings within each region of the core. If an inoperable fixed in-core detector is identified during internal consistency checks of

the data, that detector is dropped from COLSS calculations prior to replacement, e.g., at a subsequent refueling.

After the inception of operation, periodic confirmation of the COLSS assessment of the power distribution, including the suitability of any updated stored constants, is obtained by comparison with a more detailed, off-line processing of an extensive in-core flux map produced by the fixed in-core instrument systems. One means of analyzing the detailed flux map is to compare it with detailed calculations of the power distribution which include computations of the flux at the instrument location. Folding this together with other analyses of the ability of the detailed calculation to estimate the local pin-by-pin power distribution enables an overall assessment of the COLSS power distribution error.

7.7.1.3.1.3.4 Core Power Operating Limit Based on Linear Heat Rate. The core power operating limit based on linear heat rate is calculated as a function of the core power distribution. The power level that results from this calculation corresponds to the limiting condition for operation of peak linear heat rate margin.

7.7.1.3.1.3.5 Core Power Operating Limit Based on DNBR. The core power operating limit based on DNBR is calculated as a function of the reactor coolant volumetric flowrate, the core power distribution, the maximum value of the four reactor coolant cold leg temperatures, and the reactor coolant system pressure. The CE-1 correlation is used in conjunction with an iterative scheme to compute the operating limit power level. (See section 4.4 for a detailed discussion of the CE-1

correlation). The power level that results from this calculation corresponds to the limiting conditions for operation on DNBR margin.

7.7.1.3.1.4 Calculation and Measurement Uncertainties. Three uncertainty penalty factors are calculated for COLSS, one which is used in calculating the linear heat rate power operating limit and two which are used in calculating the DNBR power operating limit.

The LHR adjustment accounts for the composite modeling uncertainty in the COLSS determination of the 3-D peak and for the various engineering factors. This modeling error is determined from a set of several thousand comparison cases between COLSS and design codes covering suitable ranges of power level, core burnup, CEA position, and primary system fluid properties. The overall adjustment factor accounts for the effects of fuel rod bow, poison rod bow, design code modeling uncertainty, COLSS power algorithm uncertainty, CECOR measurement uncertainty, and computer processing uncertainties.

Similarly, the DNBR adjustments account for the composite modeling uncertainty in the COLSS calculation of the power distribution and DNBR. This composite modeling error is based on the same set of comparison cases between COLSS and design codes used for the LHR uncertainty calculation. The overall adjustment factors include the effects of fuel rod bow, poison rod bow, design code modeling uncertainty, CECOR measurement uncertainty, COLSS DNB algorithm uncertainty, and computer processing uncertainties.

7.7.1.3.2 Plant Monitoring System (PMS)

The PMS is designed and configured as a general purpose facility for plant monitoring, alarming, and reporting purposes. It includes the capability of direct interaction with plant control systems to provide permissive or control inputs to these systems based upon calculational determination of plant conditions.

7.7.1.3.2.1 Application Programs. The PMS application programs, exclusive of COLSS, that provide either a reactor monitoring or Plant Protection System monitoring function are described below:

A. Power Dependent Insertion Limits (PDILs) are operating limits on allowable insertion of full-strength CEAs as a function of reactor power, PDILs are used to maintain operation consistent with shutdown margin (when the reactor is critical) and ejected CEA worth (when the reactor is critical) constraints. PDILs utilize reactor power and CEA position signals.

B. Isolated output signals from each DNBR/LPD Calculator System channel (including calibrated ex-core neutron flux power and margin to DNBR and local power density trip setpoints) are sent to the computer. The difference between the maximum and minimum values of the four channels for each parameter is compared to a predetermined constant. An alarm is initiated if the constant is exceeded.

C. The post-trip review program monitors pre-selected process inputs at selected intervals before and after

a reactor trip. This program provides a means of monitoring events before and after a plant trip.

D. The sequence-of-events program monitors PPS bistable trip units and records status of changes (channel trips) with a resolution of several milliseconds as a means of monitoring events before and after plant trip.

Each of these PMS functions is intended to assist the plant operator in supervision or analysis of plant conditions. None of these functions is required to ensure plant safety or permit plant operation.

7.7.1.3.2.2 NSSS Programs. The NSSS programs which utilize the PMS that provide input to plant control systems are described below:

A. The CEA group sequencing program provides input to the Control Element Drive Mechanism Control System (CEDMCS) in the form of permissive signals. These signals permit sequential insertion and withdrawal of regulating CEA groups by the CEDMCS, with a pre-programmed overlap between consecutive groups during Automatic Sequential and Manual Sequential modes of operation.

The PMS monitors the following functions during sequential modes of CEA group operation:
(1) withdrawal sequence which starts with group 1 and ends with the last regulating group in consecutively increasing numbers, and (2) the insertion sequence starts with the last regulating group and ends with group 1 in consecutively decreasing numbers. Proper

sequencing of the group necessitates that the preceding group reach a specified limit before the next group is permitted to move. One sequential permissive contact output is initiated for each regulating group when the permissive conditions for that group have been met. In addition to sequential permissive outputs for each regulating group, one contact output for out-of-sequence alarming is provided, which does not pass through the CEDMCS Auxiliary Cabinets.

B. The PMS also provides normal CEA control limits for all FSCEAs/PSCEAs. These limits include the Upper (Lower) Group Stops for full-strength CEAs and the Upper (Lower) Group Stops for the PSCEAs. These control limits are provided to the CEDMCS to automatically terminate CEA motion upon reaching the CEA limits of travel.

C. The movable in-core detector system program provided monitoring and control of the movable in-core detector drive and transfer machines. Detector processing is described in Section 7.7.1.1.8.

Each of these functions is intended to enhance flexibility of plant operation. None are required to ensure plant safety or permit plant operation.

All other functions presently implemented in the PMS are solely for operator and administrative convenience and involve neither the Plant Protection System nor plant control. None of the PMS functions are required to ensure plant safety or permit plant operation.

7.7.1.3.2.3 Pulse Counting CEA Position Indication System. The pulse counting CEA position indication system infers each CEA position by maintaining a record of the "raise" and "lower" control pulses sent to each magnetic jack Control Element Drive Mechanism (CEDM). The pulse counting CEA position signal associated with each CEA is reset to zero whenever the rod drop contact (located within the reed switch position transmitter housing) is closed. This permits the pulse counting system to automatically reset the position to zero, whenever a reactor trip occurs or whenever a CEA is dropped into the core. This system is incorporated in the Plant Monitoring System (PMS) which feeds control board digital displays. One digital display provides CEA group information. A second digital display provides individual CEA position information. The position of each CEA is periodically printed out for a permanent record. A printout is available, on operator demand, of selected CEA positions.

The pulse counting CEA position indication system provides position information to CEA related alarm programs and the Core Operating Limit Supervisory System (COLSS) contained in the PMS. The PMS CEA and COLSS alarms are indicated on an alarm display, which contains both audible and visible indication, and by hard copy printout on the printer. The alarms are included in the system design to provide information to the operator to assist in maintaining proper CEA control and to aid in the monitoring of CEA limits. The following alarms are provided by the pulse counting CEA position indication system:

A. Power Dependent Insertion Limits (PDILs) Alarms

An alarm is provided on PC and CMC COLSS after CMC/COLSS upgrade, in the event CEA insertion exceeds

predetermined limits required to maintain adequate shutdown margin and to ensure CEA insertion consistent with the CEA ejection analysis. Further definition of the PDIL function is provided in Paragraph 7.7.1.3.2.1.

B. Pre-Power Dependent Insertion Limits (PPDILs) Alarm

This alarm is provided to advise the operator of an impending approach to PDILs.

C. Out of Sequence Alarm

An alarm is provided to alert the operator in the event the CEA groups are inserted in a sequence other than the pre-determined acceptable sequence.

D. CEA Deviation Alarm

An alarm is provided to alert the operator in the event the deviation in position between the highest and lowest CEA in any group exceeds a predetermined allowable deviation.

E. Core Operating Limit Supervisory System Alarms

The pulse counting CEA position indication system provides input data to COLSS. These data are used in the COLSS power distribution calculations, and alarms are initiated in the event the affected COLSS limits are reached. The basis for the COLSS alarms and the use of the pulse count CEA position information is discussed in Section 7.7.1.3.1.

7.7.2 ANALYSIS

The plant control system and equipment are designed to provide high reliability during steady state operation and anticipated transient conditions. The RPS analysis of Section 7.2.2 encompasses the failure modes of these control systems and demonstrates that these systems are not required for safety.

The safety analyses of Chapter 15.0 do not require these systems to remain functional.

7.7.3 REFERENCES

1. "Overview Description of the Core Operating Limit Supervisory System," CEN-312, Revision 01-P, November 1986

APPENDIX 7A

RESPONSES TO NRC REQUESTS FOR INFORMATION

APPENDIX 7A

CONTENTS

	Page
Question 7A.1 (NRC Question 222.01)	7A-1
Question 7A.2 (NRC Question 222.02)	7A-2
Question 7A.3 (NRC Question 222.03)	7A-3
Question 7A.4 (NRC Question 222.04)	7A-4
Question 7A.5 (NRC Question 492.3)	7A-5
Question 7A.6 (NRC Question 492.4)	7A-7

APPENDIX 7A

QUESTION 7A.1 (NRC Question 222.01)

Loss of Non-Class 1E Instrumentation and Control Power System Bus During Power Operation (IE Bulletin 79-27)

If reactor controls and vital instruments derive power from common electrical distribution systems, the failure of such electrical distribution systems may result in an event requiring operator action concurrent with failure of important instrumentation upon which these operator actions should be based. This concern was addressed in IE Bulletin 79-27. On November 30, 1979, IE Bulletin 79-27 was sent to operating license (OL) holders, the near term OL applicants (North Anna 2, Diablo Canyon, McGuire, Salem 2, Sequoyah, and Zimmer), and other holders of construction permits (CPs), including Palo Verde. Of these recipients, the CP holders were not given explicit direction for making a submittal as part of the licensing review. However, they were informed that the issue would be addressed later.

You are requested to address this issue by taking IE Bulletin 79-27 Actions 1 through 3 under "Actions to be Taken by Licensees". Within the response time called for in the attached transmittal letter, complete the review and evaluation required by Actions 1 through 3 and provide a written response describing your reviews and actions. This report should be in the form of an amendment to your FSAR and submitted to the NRC Office of Nuclear Reactor Regulations as a licensing submittal.

RESPONSE:

The response is given in amended paragraph 7.1.2.33.

QUESTION 7A.2 (NRC Question 222.02)

If safety equipment does not remain in its emergency mode upon reset of an engineered safeguards actuation signal, system modification, design change or other protective action of the affected equipment is not compromised once the associated actuation signal is reset. This issue was addressed in IE Bulletin 80-06 (enclosed). For facilities with operating licenses as of March 13, 1980, IE Bulletin 80-06 required that reviews be conducted by the licensees to determine which, if any, safety functions might be unavailable after reset, and what changes could be implemented to correct the problem.

For facilities with a construction permit, including OL applicants, Bulletin 80-06 was issued for information only.

The NRC staff has determined that all CP holders, as a part of the OL review process are to be requested to address this issue. Accordingly, you are requested to take the actions called for in Bulletin 80-06 Actions 1 through 4 under "Actions to be Taken by Licensees". Within the response time called for in the attached transmittal letter, complete the review verifications and descriptions of corrective actions taken or planned as stated in Actions 1 through 3 and submit the report called for in Action Item 4. The report should be submitted to the NRC Office of Nuclear Regulation as a licensing submittal in the form of an FSAR amendment.

RESPONSE:

The response is given in amended paragraph 7.1.2.34.

QUESTION 7A.3 (NRC Question 222.03)

Operating reactor licensees were informed by IE Information Notice 79-22, issued September 19, 1979, that certain non-safety grade or control equipment, if subjected to the adverse environment of a high energy line break, could impact the safety analyses and the adequacy of the protection functions performed by the safety grade equipment. Enclosed is a copy of IE Information Notice 79-22, and reprinted copies of an August 20, 1979, Westinghouse letter and a September 10, 1979, Public Service Electric and Gas Company letter which address this matter. Operating reactor licensees conducted reviews to determine whether such problems could exist at operating facilities.

We are concerned that a similar potential may exist at light water facilities now under construction. You are, therefore, requested to perform a review to determine what, if any, design changes or operator actions would be necessary to assure that high energy line breaks will not cause system failures to complicate the event beyond your FSAR analysis. Provide the results of your reviews including all identified problems and the manner in which you have resolved them to NRR.

The specific "scenarios" discussed in the above referenced Westinghouse letter are to be considered as examples of the kind of interactions which might occur. Your review should include those scenarios, where applicable, but should not necessarily be limited to them. Applicants with other LWR designs should consider analogous interactions as relevant to their designs.

RESPONSE:

The response is given in amended paragraph 7.1.2.35.

QUESTION 7A.4 (NRC Question 222.04)

The analysis reported in chapter 15 of the FSAR are intended to demonstrate the adequacy of safety systems in mitigating anticipated operational occurrences and accidents.

Based on the conservative assumptions made in defining these design basis events and the detailed review of the analyses by the staff, it is likely that they adequately bound the consequences of single control system failures.

To provide assurance that the design basis event analyses adequately bound other more fundamental credible failures, you are requested to provide the following information:

1. Identify those control systems whose failure or malfunction could seriously impact plant safety.
2. Indicate which, if any, of the control systems identified in (1) receive power from common power sources. The power sources considered should include all power sources whose failure or malfunction could lead to failure or malfunction of more than one control system and should extend to the effects of cascading power losses due to the failure of higher level distribution panels and load centers.
3. Indicate which, if any, of the control systems identified in (1) receive input signals from common sensors. The sensors considered should include, but should not necessarily be limited to, common hydraulic headers or impulse lines feeding pressure, temperature, level or other signals to two or more control systems.

4. Provide justification that any simultaneous malfunctions of the control systems identified in (2) and (3) resulting from failures or malfunctions of the applicable common power source or sensor are bounded by the analyses in chapter 15 and would not require action or response beyond the capability of operators or safety systems.

RESPONSE: Refer to Section 7.2.2.4.1 for a detailed response.

QUESTION 7A.5 (NRC Question 492.3)[a]

CEN-251(V)-P, Revision 00 - "PVNGS-1 Cycle 1 CPC and CEAC Data Base Listing," June 1983 provides data base values for the Palo Verde, Unit 1, CPC and CEAC.

The data base document states that - "the purpose of this document is to specify the CPC and CEAC data base constants applicable to the PVNGS-1 Cycle 1 software described in Reference 1, the CPC Functional Design Specification, and Reference 2, the CEAC Calculator Functional Design Specification."

References 1 and 2 are the functional specifications for a CPC and CEAC for San Onofre. In addition, Reference 3 is a software modification for Waterford, although not mentioned in the text.

(a) Are the referenced data base constants for San Onofre applicable to Palo Verde?

a. Submitted by NRC as Question 492.1

(b) Why is a reference given for a Waterford modification? Does this apply to Palo Verde?

RESPONSE:

A. The references listed in CEN-251(V)-P have been reviewed, and none of the four references relates to San Onofre data base constants. Furthermore, the San Onofre data base constants are not applicable to Palo Verde.

B. The reference to a document defining the Waterford modifications was incorrect. The referenced document applies only to Waterford CPC/CEAC software. The correct Reference 3 to CEN-251(V)-P should be Reference 7A-1 to this response. Reference 7A-1 incorporates the Waterford modifications and defines additional changes that were made specifically for Palo Verde. The last complete versions of the CPC and CEAC functional descriptions submitted to the NRC were References 7A-2 and 7A-3. References 7A-1 through 7A-3 completely define the functional design for the Palo Verde CPC/CEAC software. Therefore, the first paragraph of Section 1.2 in CEN-251(V)-P should read as follows:

"The CPC/CEAC system, as functionally described in References 1 and 2 and as modified by Reference 3, is implemented in assembly language and also exists as a FORTRAN simulation. This document provides..."

In addition, Subparagraph (1) of Section 1.3 in CEN-251(V)-P should read as follows:

"(1) The CPC and CEAC protection systems described in References 1, 2, and 3."

References

7A-1 CPC/CEAC Software Modifications for System 80, Enclosure 1-P to LD-82-039, March 1982.

7A-2 Functional Design Specification for a Core Protection Calculator, CEN-147(S)-P, January 1981.

7A-3 Functional Design Specification for a Control Element Assembly Calculator, CEN-148(S)-P, January 1981.

QUESTION 7A.6 (NRC Question 492.4)[a]

CEN-251(V)-P, revision 00 - "PVNGS-1 Cycle 1 and CEAC Data Base Listing," June 1983 provides data base values for CPC and CEAC. However, the BERR values (addressable constants) are not consistent with the approved CESSAR-80 values described in Enclosure 1-P to LD-83-010, "Statistical Combination of Uncertainties Part V," January 1983. Specifically, a comparison is shown in the following table for BERR values given for Palo Verde and CESSAR-80:

	Palo Verde	CESSAR-80
BERR0	8.5	9.0
BERR1	1.065	1.099
BERR2	8.5	7.48
BERR3	1.074	1.139
BERR4	8.5	12.48

(a) Explain why the Palo Verde BERRs differ from the CESSAR-80 values and justify their acceptability.

a. Submitted by NRC as Question 492.2

RESPONSE:

The Palo Verde BERRs do not differ from the CESSAR-80 values. The BERR values are calculated toward the end of the CPC software testing and, therefore, are not available at the time the CPC/CEAC data base is generated. The BERR values given in CEN-251(V)-P are preliminary values. These preliminary values are required in order to generate and certify a data base for use in phase I and phase II testing. In addition, certain outputs of the CPC/CEAC software testing are required as inputs to the uncertainty analysis which determines the correct BERR values for plant power operations. Since the BERR values are addressable constants, the final values can be loaded when the software is loaded.

The BERR values given for Palo Verde are not the correct values. The values certified for power operations are the same as those given for CESSAR-80. The letter (Reference 7A-4) which transmitted the CPC/CEAC disks and software documentation also transmitted the correct BERR values. These values are listed in Attachment 3 of the letter, which is a table of correct addressable constant values. The letter also transmitted comments on the addressable constants which include the following guidance:

> "Attachment (3) lists the addressable constants and their values. The values of some of the addressable constants in Attachment (3) are different than the values for the equivalent constants contained in the data base listing and the software data base . . . The values listed in Attachment (3) supersede those

values listed in the data base and are to be implemented when the software is loaded."

Reference

7A-4 Letter from C. Ferguson (C-E) to G.C. Andognini (APS), V-CE-18963, dated September 7, 1983.

Intentionally Left Blank