Table of Contents

7.0 Instrumentation and Controls
7.1 Introduction
7.1.1 Identification of Safety-Related Systems
7.1.1.1 Reactor Trip System
7.1.1.2 Engineered Safety Features Actuation System
7.1.1.3 Systems Required for Safe Shutdown
7.1.1.4 Safety-Related Display Instrumentation
7.1.1.5 Other Systems Required for Safety
7.1.2 Identification of Safety Criteria
7.1.2.1 Design Bases
7.1.2.1.1 Reactor Trip System
7.1.2.1.2 Engineered Safety Features Actuation System
7.1.2.1.3 Interlocks
7.1.2.1.4 Bypasses
7.1.2.1.5 Equipment Protection
7.1.2.1.6 Diversity
7.1.2.1.7 Bistable Trip Setpoints
7.1.2.1.8 Emergency Power
7.1.2.2 Independence of Redundant Systems
7.1.2.3 Physical Identification of Safety-Related Equipment
7.1.2.4 Design Criteria
7.1.2.4.1 General Design Criteria
7.1.2.4.2 NRC Regulatory Guides
7.1.2.4.3 NRC IE Bulletin 90-01 and Supplement 1
7.1.2.4.4 Industry Standards
7.1.3 References

7.2 Reactor Trip System
7.2.1 Description
7.2.1.1 System Description
7.2.1.1.1 Functional Performance Requirements
7.2.1.1.2 Reactor Trips
7.2.1.1.3 Reactor Trip System Interlocks
7.2.1.1.4 Reactor Coolant Temperature Sensor Arrangement
7.2.1.1.5 Pressurizer Water Level Reference Leg Arrangement
7.2.1.1.6 Analog System
7.2.1.1.7 Solid State Logic Protection System
7.2.1.1.8 Isolation Amplifiers
7.2.1.1.9 Energy Supply and Environmental Variations
7.2.1.1.10 Setpoints
7.2.1.1.11 Seismic Design
7.2.1.2 Design Bases Information
7.2.1.2.1 Generating Station Conditions
7.2.1.2.2 Generating Station Variables
7.2.1.2.3 Spatially Dependent Variables
7.2.1.2.4 Limits, Margins, and Set Points
7.2.1.2.5 Abnormal Events
7.2.1.2.6 Minimum Performance Requirements
7.2.1.3 Final Systems Drawings
7.2.2 Analyses
7.2.2.1 Failure Mode and Effects Analyses
7.2.2.2 Evaluation of Design Limits

7.2.2.2.1 Trip Setpoint Discussion
7.2.2.2.2 Reactor Coolant Flow Measurement
7.2.2.2.3 Evaluation of Compliance to Applicable Codes and Standards
7.2.2.3 Specific Control and Protection Interactions
7.2.2.3.1 Neutron Flux
7.2.2.3.2 Reactor Coolant Temperature
7.2.2.3.3 Pressurizer Pressure
7.2.2.3.4 Pressurizer Water Level
7.2.2.3.5 Steam Generator Water Level
7.2.2.4 Additional Postulated Accidents
7.2.3 Tests and Inspections
7.2.4 References

7.3 Engineered Safety Features Actuation System
7.3.1 Description
7.3.1.1 System Description
7.3.1.1.1 Function Initiation
7.3.1.1.2 Analog Circuitry
7.3.1.1.3 Digital Circuitry
7.3.1.1.4 Final Actuation Circuitry
7.3.1.1.5 Support Systems
7.3.1.2 Design Bases Information
7.3.1.2.1 Generating Station Conditions
7.3.1.2.2 Generating Station Variables
7.3.1.2.3 Spatially Dependent Variables
7.3.1.2.4 Limits, Margins and Levels
7.3.1.2.5 Abnormal Events
7.3.1.2.6 Minimum Performance Requirements
7.3.2 Analysis
7.3.2.1 Failure Mode and Effects Analyses
7.3.2.2 Compliance With Standards and Design Criteria
7.3.2.2.1 Single Failure Criteria
7.3.2.2.2 Equipment Qualification
7.3.2.2.3 Independence
7.3.2.2.4 Control and Protection System Interaction
7.3.2.2.5 Capability for Sensor Checks and Equipment Test and Calibration
7.3.2.2.6 Manual Blocking Features
7.3.2.2.7 Manual Initiation of Protective Actions (Regulatory Guide 1 .62)
7.3.2.3 Further Considerations
7.3.2.4 Summary
7.3.2.4.1 Loss of Coolant Protection
7.3.2.4.2 Steam Line Break Protection
7.3.3 References

7.4 Systems Required for Safe Shutdown
7.4.1 Auxiliary Feedwater System Instrumentation and Control
7.4.1.1 Description
7.4.1.2 Design Bases
7.4.1.3 Analysis
7.4.1.3.1 General Functional Requirement
7.4.1.3.2 Single Failure Criterion
7.4.1.3.3 Quality of Components
7.4.1.3.4 Equipment Qualification
7.4.1.3.5 Channel Integrity
7.4.1.3.6 Channel Independence
7.4.1.3.7 Control and Protection System Interaction

7.4.1.3.8 Derivation of System Inputs
7.4.1.3.9 Capability for Test and Calibration
7.4.1.3.10 Channel Bypass or Removal From Operation
7.4.1.3.11 Operating Bypasses
7.4.1.3.12 Indication of Bypasses
7.4.1.3.13 Access to Means for Bypassing
7.4.1.3.14 Multiple Setpoints
7.4.1.3.15 Completion of Protective Action Once it is Initiated
7.4.1.3.16 Manual Initiation
7.4.1.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.4.1.3.18 Identification of Protective Action
7.4.1.3.19 Information Read-Out
7.4.1.3.20 System Repair
7.4.1.3.21 Identification
7.4.2 Nuclear Service Water System Instrumentation and Control
7.4.2.1 Description
7.4.2.2 Design Bases
7.4.2.3 Analysis
7.4.2.3.1 General Functional Requirements
7.4.2.3.2 Single Failure Criterion
7.4.2.3.3 Quality of Components and Modules
7.4.2.3.4 Equipment Qualification
7.4.2.3.5 Channel Integrity
7.4.2.3.6 Channel Independence
7.4.2.3.7 Control and Protection System Interaction
7.4.2.3.8 Derivation of System Inputs
7.4.2.3.9 Capability for Test and Calibration
7.4.2.3.10 Channel Bypass or Removal From Operation
7.4.2.3.11 Operating Bypasses
7.4.2.3.12 Indication of Bypasses
7.4.2.3.13 Access to Means for Bypassing
7.4.2.3.14 Multiple Setpoints
7.4.2.3.15 Completion of Protective Action Once it is Initiated
7.4.2.3.16 Manual Initiation
7.4.2.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.4.2.3.18 Identification of Protective Action
7.4.2.3.19 Information Read-Out
7.4.2.3.20 System Repair
7.4.2.3.21 Identification
7.4.3 Component Cooling Water System Instrumentaton and Control
7.4.3.1 Description
7.4.3.2 Design Bases
7.4.3.3 Analysis
7.4.3.3.1 General Functional Requirements
7.4.3.3.2 Single Failure Criterion
7.4.3.3.3 Quality of Components and Modules
7.4.3.3.4 Equipment Qualification
7.4.3.3.5 Channel Integrity
7.4.3.3.6 Channel Independence
7.4.3.3.7 Control and Protection System Interaction
7.4.3.3.8 Derivation of System Inputs
7.4.3.3.9 Capability for Test, and Calibration
7.4.3.3.10 Channel Bypass or Removal From Operation
7.4.3.3.11 Operating Bypasses
7.4.3.3.12 Indication of Bypasses
7.4.3.3.13 Access to Means for Bypassing

7.4.3.3.14 Multiple Setpoints
7.4.3.3.15 Completion of Protective Action Once it is Initiated
7.4.3.3.16 Manual Initiation
7.4.3.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.4.3.3.18 Identification of Protective Action
7.4.3.3.19 Information Read-Out
7.4.3.3.20 System Repair
7.4.3.3.21 Identification
7.4.4 Chemical and Volume Control System Instrumentation and Control
7.4.4.1 Description
7.4.4.2 Design Bases
7.4.4.3 Analysis
7.4.4.3.1 General Functional Requirements
7.4.4.3.2 Single Failure Criterion
7.4.4.3.3 Quality of Components and Modules
7.4.4.3.4 Equipment Qualification
7.4.4.3.5 Channel Integrity
7.4.4.3.6 Channel Independence
7.4.4.3.7 Control and Protection System Interaction
7.4.4.3.8 Derivation of System Inputs
7.4.4.3.9 Capability for Test and Calibration
7.4.4.3.10 Channel Bypass or Removal From Operation
7.4.4.3.11 Operating Bypasses
7.4.4.3.12 Indication of Bypasses
7.4.4.3.13 Access to Means for Bypassing
7.4.4.3.14 Multiple Setpoints
7.4.4.3.15 Completion of Protective Action Once it is Initiated
7.4.4.3.16 Manual Initiation
7.4.4.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.4.4.3.18 Identification of Protective Action
7.4.4.3.19 Information Read-Out
7.4.4.3.20 System Repair
7.4.4.3.21 Identification
7.4.5 Residual Heat Removal System Instrumentation and Controls
7.4.5.1 Description
7.4.5.2 Design Bases
7.4.5.3 Analysis
7.4.5.3.1 General Functional Requirements
7.4.5.3.2 Single Failure Criterion
7.4.5.3.3 Quality of Components and Modules
7.4.5.3.4 Equipment Qualification
7.4.5.3.5 Channel Integrity
7.4.5.3.6 Channel Independence
7.4.5.3.7 Control and Protection System Interaction
7.4.5.3.8 Derivation of System Inputs
7.4.5.3.9 Capability for Test, Calibration, and Sensor Checks
7.4.5.3.10 Channel Bypass or Removal From Operation
7.4.5.3.11 Operating Bypasses
7.4.5.3.12 Indication of Bypasses
7.4.5.3.13 Access to Means for Bypassing
7.4.5.3.14 Multiple Setpoints
7.4.5.3.15 Completion of Protective Action Once it is Initiated
7.4.5.3.16 Manual Initiation
7.4.5.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.4.5.3.18 Identification of Protective Action
7.4.5.3.19 Information Read-Out

7.4.5.3.20 System Repair
7.4.5.3.21 Identification
7.4.6 Emergency Core Cooling System Instrumentation and Control
7.4.7 Auxiliary Shutdown Control
7.4.7.1 Description
7.4.7.2 Analysis

7.5 Safety-Related Display Instrumentation
7.5.1 Description
7.5.2 Inadequate Core Cooling Instrumentation
7.5.2.1 Core Exit Thermocouples (CET)
7.5.2.2 Subcooling Monitor
7.5.2.3 Reactor Vessel Level Instrumentation System (RVLIS)

7.6 All Other Systems Required for Safety
7.6.1 Instrumentation and Control Power Supply System
7.6.2 Deleted Per 2012 Update
7.6.3 Cold-Leg Accumulator Motor-Operated Isolation Valves
7.6.3.1 Description
7.6.3.2 Design Bases
7.6.3.3 Analysis
7.6.3.3.1 General Functional Requirements
7.6.3.3.2 Single Failure Criterion
7.6.3.3.3 Quality of Components and Modules
7.6.3.3.4 Equipment Qualification
7.6.3.3.5 Channel Integrity
7.6.3.3.6 Channel Independence
7.6.3.3.7 Control and Protection System Interaction
7.6.3.3.8 Derivation of System Inputs
7.6.3.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.3.3.10 Channel Bypass or Removal From Operation
7.6.3.3.11 Operating Bypasses
7.6.3.3.12 Indication of Bypasses
7.6.3.3.13 Access to Means for Bypassing
7.6.3.3.14 Multiple Setpoints
7.6.3.3.15 Completion of Protective Action Once it is Initiated
7.6.3.3.16 Manual Initiation
7.6.3.3.17 Access to Setpoint Adjustments, Calibration, and Test Point s
7.6.3.3.18 Identification of Protective Action
7.6.3.3.19 Information Read-Out
7.6.3.3.20 System Repair
7.6.3.3.21 Identification
7.6.4 Containment Pressure Control System
7.6.4.1 Description
7.6.4.2 Design Bases
7.6.4.3 Analysis
7.6.4.3.1 General Functional Requirement
7.6.4.3.2 Single Failure Criterion
7.6.4.3.3 Quality of Components
7.6.4.3.4 Equipment Qualification
7.6.4.3.5 Channel Integrity
7.6.4.3.6 Channel Independence
7.6.4.3.7 Control and Protection System Interaction
7.6.4.3.8 Derivation of System Inputs
7.6.4.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.4.3.10 Channel Bypass or Removal From Operation

7.6.4.3.11 Operating Bypasses
7.6.4.3.12 Indication of Bypass
7.6.4.3.13 Access to Means for Bypassing
7.6.4.3.14 Multiple Setpoints
7.6.4.3.15 Completion of Protective Action Once it is Initiated
7.6.4.3.16 Manual Initiation
7.6.4.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.4.3.18 Identification of Protective Action
7.6.4.3.19 Information Read-Out
7.6.4.3.20 System Repair
7.6.4.3.21 Identification
7.6.5 Refueling Water System Instrumentation and Switchover From Safety Injection to Recirculation Mode
7.6.5.1 Description
7.6.5.2 Design Bases
7.6.5.3 Analysis
7.6.5.3.1 General Functional Requirements
7.6.5.3.2 Single Failure Criterion
7.6.5.3.3 Quality of Components and Modules
7.6.5.3.4 Equipment Qualification
7.6.5.3.5 Channel Integrity
7.6.5.3.6 Channel Independence
7.6.5.3.7 Control and Protection System Interaction
7.6.5.3.8 Derivation of Inputs
7.6.5.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.5.3.10 Channel Bypass or Removal From Operation
7.6.5.3.11 Operating Bypasses
7.6.5.3.12 Indication of Bypass
7.6.5.3.13 Access to Means for Bypassing
7.6.5.3.14 Multiple Setpoints
7.6.5.3.15 Completion of Protective Action Once it is Initiated
7.6.5.3.16 Manual Initiation
7.6.5.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.5.3.18 Identification of Protective Action
7.6.5.3.19 Information Read-Out
7.6.5.3.20 System Repair
7.6.5.3.21 Identification
7.6.6 Liquid Radwaste System
7.6.6.1 Description
7.6.6.2 Design Bases
7.6.6.3 Analysis
7.6.6.3.1 General Functional Requirements
7.6.6.3.2 Single Failure Criterion
7.6.6.3.3 Quality of Components and Modules
7.6.6.3.4 Equipment Qualification
7.6.6.3.5 Channel Integrity
7.6.6.3.6 Channel Independence
7.6.6.3.7 Control and Protection System Interaction
7.6.6.3.8 Derivation of System Inputs
7.6.6.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.6.3.10 Channel Bypass or Removal From Operation
7.6.6.3.11 Operating Bypasses
7.6.6.3.12 Indication of Bypass
7.6.6.3.13 Access to Means for Bypassing
7.6.6.3.14 Multiple Setpoints
7.6.6.3.15 Completion of Protective Action Once it is Initiated

7.6.6.3.16 Manual Initiation
7.6.6.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.6.3.18 Identification of Protective Action
7.6.6.3.19 Information Read-Out
7.6.6.3.20 System Repair
7.6.6.3.21 Identification
7.6.7 Diesel Generator Room Sump Pump System
7.6.7.1 Description
7.6.7.2 Design Bases
7.6.7.3 Analysis
7.6.7.3.1 General Functional Requirements
7.6.7.3.2 Single Failure Criterion
7.6.7.3.3 Quality of Components and Modules
7.6.7.3.4 Equipment Qualification
7.6.7.3.5 Channel Integrity
7.6.7.3.6 Channel Independence
7.6.7.3.7 Control and Protection System Interaction
7.6.7.3.8 Derivation of System Inputs
7.6.7.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.7.3.10 Channel Bypass or Removal From Operation
7.6.7.3.11 Operating Bypasses
7.6.7.3.12 Indication of Bypass
7.6.7.3.13 Access to Means for Bypassing
7.6.7.3.14 Multiple Setpoints
7.6.7.3.15 Completion of Protective Action Once it is Initiated
7.6.7.3.16 Manual Initiation
7.6.7.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.7.3.18 Identification of Protective Action
7.6.7.3.19 Information Read-Out
7.6.7.3.20 System Repair
7.6.7.3.21 Identification
7.6.8 Diesel Building Ventilation System Instrumentation and Controls
7.6.8.1 Description
7.6.8.2 Design Bases
7.6.8.3 Analysis
7.6.8.3.1 General Functional Requirements
7.6.8.3.2 Single Failure Criterion
7.6.8.3.3 Quality of Components and Modules
7.6.8.3.4 Equipment Qualification
7.6.8.3.5 Channel Integrity
7.6.8.3.6 Channel Independence
7.6.8.3.7 Control and Protection System Interaction
7.6.8.3.8 Derivation of System Inputs
7.6.8.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.8.3.10 Channel Bypass or Removal From Operation
7.6.8.3.11 Operating Bypasses
7.6.8.3.12 Indication of Bypass
7.6.8.3.13 Access to Means for Bypassing
7.6.8.3.14 Multiple Setpoints
7.6.8.3.15 Completion of Protective Action Once it is Initiated
7.6.8.3.16 Manual Initiation
7.6.8.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.8.3.18 Identification of Protective Action
7.6.8.3.19 Information Read-Out Temperature
7.6.8.3.20 System Repair
7.6.8.3.21 Identification

7.6.9 Groundwater Drainage System Instrumentation and Control
7.6.9.1 Description
7.6.9.2 Design Bases
7.6.9.3 Analysis
7.6.9.3.1 General Functional Requirements
7.6.9.3.2 Single Failure Criterion
7.6.9.3.3 Quality of Components and Modules
7.6.9.3.4 Equipment Qualification
7.6.9.3.5 Channel Integrity
7.6.9.3.6 Channel Independence
7.6.9.3.7 Control and Protection System Interaction
7.6.9.3.8 Derivation of System Inputs
7.6.9.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.9.3.10 Channel Bypass or Removal From Operation
7.6.9.3.11 Operating Bypasses
7.6.9.3.12 Indication of Bypass
7.6.9.3.13 Access to Means for Bypassing
7.6.9.3.14 Multiple Setpoints
7.6.9.3.15 Completion of Protective Action Once it is Initiated
7.6.9.3.16 Manual Initiation
7.6.9.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.9.3.18 Identification of Protective Action
7.6.9.3.19 Information Read-Out
7.6.9.3.20 System Repair
7.6.9.3.21 Identification
7.6.10 Containment Air Return, Hydrogen Skimmer and Hydrogen Recombiner System
7.6.10.1 Description
7.6.10.2 Design Bases
7.6.10.3 Analysis
7.6.10.3.1 General Functional Requirements
7.6.10.3.2 Single Failure Criterion
7.6.10.3.3 Quality of Components and Modules
7.6.10.3.4 Equipment Qualification
7.6.10.3.5 Channel Integrity
7.6.10.3.6 Channel Independence
7.6.10.3.7 Control and Protection System Interaction
7.6.10.3.8 Derivation of System Inputs
7.6.10.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.10.3.10 Channel Bypass or Removal From Operation
7.6.10.3.11 Operating Bypasses
7.6.10.3.12 Indication of Bypasses
7.6.10.3.13 Access to Means for Bypassing
7.6.10.3.14 Multiple Setpoints
7.6.10.3.15 Completion of Protective Action Once it is Initiated
7.6.10.3.16 Manual Initiation
7.6.10.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.10.3.18 Identification of Protective Action
7.6.10.3.19 Information Read-Out
7.6.10.3.20 System Repair
7.6.10.3.21 Identification
7.6.11 Spent Fuel Pool Cooling System
7.6.11.1 Description
7.6.11.2 Design Bases
7.6.11.3 Analysis
7.6.11.3.1 General Functional Requirements
7.6.11.3.2 Single Failure Criterion

7.6.11.3.3 Quality of Components and Modules
7.6.11.3.4 Equipment Qualification
7.6.11.3.5 Channel Integrity
7.6.11.3.6 Channel Independence
7.6.11.3.7 Control and Protection System Interaction
7.6.11.3.8 Derivation of System Inputs
7.6.11.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.11.3.10 Channel Bypass or Removal From Operation
7.6.11.3.11 Operating Bypasses
7.6.11.3.12 Indication of Bypass
7.6.11.3.13 Access to Means for Bypassing
7.6.11.3.14 Multiple Setpoints
7.6.11.3.15 Completion of Protective Action Once it is Initiated
7.6.11.3.16 Manual Initiation
7.6.11.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.11.3.18 Identification of Protective Action
7.6.11.3.19 Information Read-Out
7.6.11.3.20 System Repair
7.6.11.3.21 Identification
7.6.12 Auxiliary Building Ventilation System
7.6.12.1 Description
7.6.12.2 Design Bases
7.6.12.3 Analysis
7.6.12.3.1 General Functional Requirements
7.6.12.3.2 Single Failure Criterion
7.6.12.3.3 Quality of Components and Modules
7.6.12.3.4 Equipment Qualification
7.6.12.3.5 Channel Integrity
7.6.12.3.6 Channel Independence
7.6.12.3.7 Control and Protection System Interaction
7.6.12.3.8 Derivation of System Inputs
7.6.12.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.12.3.10 Channel Bypass or Removal From Operation
7.6.12.3.11 Operating Bypasses
7.6.12.3.12 Indication of Bypass
7.6.12.3.13 Access to Means for Bypassing
7.6.12.3.14 Multiple Setpoints
7.6.12.3.15 Completion of Protective Action Once it is Initiated
7.6.12.3.16 Manual Initiation
7.6.12.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.12.3.18 Identification of Protective Action
7.6.12.3.19 Information Read-Out
7.6.12.3.20 System Repair
7.6.12.3.21 Identification
7.6.13 Control Room Area Heating, Ventilation and Air Conditioning Instrumentation and Control
7.6.13.1 Description
7.6.13.2 Design Bases
7.6.13.3 Analysis
7.6.13.3.1 General Functional Requirements
7.6.13.3.2 Single Failure Criterion
7.6.13.3.3 Quality of Components and Modules
7.6.13.3.4 Equipment Qualification
7.6.13.3.5 Channel Integrity
7.6.13.3.6 Channel Independence
7.6.13.3.7 Control and Protection System Interaction

7.6.13.3.8 Derivation of System Inputs
7.6.13.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.13.3.10 Channel Bypass or Removal From Operation
7.6.13.3.11 Operating Bypasses
7.6.13.3.12 Indication of Bypass
7.6.13.3.13 Access to Means for Bypassing
7.6.13.3.14 Multiple Setpoints
7.6.13.3.15 Completion of Protective Action Once it is Initiated
7.6.13.3.16 Manual Initiation
7.6.13.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.13.3.18 Identification of Protective Action
7.6.13.3.19 Information Read-Out
7.6.13.3.20 System Repair
7.6.13.3.21 Identification
7.6.14 Annulus Ventilation System Instrumentation and Control
7.6.14.1 Description
7.6.14.2 Design Bases
7.6.14.3 Analysis
7.6.14.3.1 General Functional Requirements
7.6.14.3.2 Single Failure Criterion
7.6.14.3.3 Quality of Components
7.6.14.3.4 Equipment Qualification
7.6.14.3.5 Channel Integrity
7.6.14.3.6 Channel Independence
7.6.14.3.7 Control and Protection System Interaction
7.6.14.3.8 Derivation of System Inputs
7.6.14.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.14.3.10 Channel Bypass or Removal From Operation
7.6.14.3.11 Operating Bypasses
7.6.14.3.12 Indication of Bypass
7.6.14.3.13 Access to Means for Bypassing
7.6.14.3.14 Multiple Setpoints
7.6.14.3.15 Completion of Protective Action Once it is Initiated
7.6.14.3.16 Manual Initiation
7.6.14.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.14.3.18 Identification of Protective Action
7.6.14.3.19 Information Read-Out
7.6.14.3.20 System Repair
7.6.14.3.21 Identification
7.6.15 Diesel Generator Fuel Oil System Instrumentation and Controls
7.6.15.1 Description
7.6.15.2 Design Bases
7.6.15.3 Analysis
7.6.15.3.1 General Functional Requirements
7.6.15.3.2 Single Failure Criterion
7.6.15.3.3 Quality of Components and Modules
7.6.15.3.4 Equipment Qualification
7.6.15.3.5 Channel Integrity
7.6.15.3.6 Channel Independence
7.6.15.3.7 Control and Protection System Interaction
7.6.15.3.8 Derivation of System Inputs
7.6.15.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.15.3.10 Channel Bypass or Removal From Operation
7.6.15.3.11 Operating Bypasses
7.6.15.3.12 Indication of Bypass
7.6.15.3.13 Access to Means for Bypassing

7.6.15.3.14 Multiple Setpoints
7.6.15.3.15 Completion of Protective Action Once it is Initiated
7.6.15.3.16 Manual Initiation
7.6.15.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.15.3.18 Identification of Protective Action
7.6.15.3.19 Information Read-Out
7.6.15.3.20 System Repair
7.6.15.3.21 Identification
7.6.16 Diesel Generator Cooling Water System Instrumentation and Control
7.6.16.1 Description
7.6.16.2 Design Bases
7.6.16.3 Analysis
7.6.16.3.1 General Functional Requirements
7.6.16.3.2 Single Failure Criterion
7.6.16.3.3 Quality of Components
7.6.16.3.4 Equipment Qualification
7.6.16.3.5 Channel Integrity
7.6.16.3.6 Channel Independence
7.6.16.3.7 Control and Protection System Interaction
7.6.16.3.8 Derivation of System Inputs
7.6.16.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.16.3.10 Channel Bypass or Removal From Operation
7.6.16.3.11 Operating Bypasses
7.6.16.3.12 Indication of Bypass
7.6.16.3.13 Access to Means for Bypassing
7.6.16.3.14 Multiple Setpoints
7.6.16.3.15 Completion of Protective Action Once it is Initiated
7.6.16.3.16 Manual Initiation
7.6.16.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.16.3.18 Identification of Protective Action
7.6.16.3.19 Information Read-Out
7.6.16.3.20 System Repair
7.6.16.3.21 Identification
7.6.17 Diesel Generator Starting Air System Instrumentation and Control
7.6.17.1 Description
7.6.17.2 Design Bases
7.6.17.3 Analysis
7.6.17.3.1 General Functional Requirements
7.6.17.3.2 Single Failure Criterion
7.6.17.3.3 Quality of Components and Modules
7.6.17.3.4 Equipment Qualification
7.6.17.3.5 Channel Integrity
7.6.17.3.6 Channel Independence
7.6.17.3.7 Control and Protection System Interaction
7.6.17.3.8 Derivation of System Inputs
7.6.17.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.17.3.10 Channel Bypass or Removal From Operation
7.6.17.3.11 Operating Bypasses
7.6.17.3.12 Indication of Bypass
7.6.17.3.13 Access to Means for Bypassing
7.6.17.3.14 Multiple Setpoints
7.6.17.3.15 Completion of Protective Action Once it is Initiated
7.6.17.3.16 Manual Initiation
7.6.17.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.17.3.18 Identification of Protective Action
7.6.17.3.19 Information Read-Out

7.6.17.3.20 System Repair
7.6.17.3.21 Identification
7.6.18 Diesel Generator Lubricating Oil System Instrumentation and Control
7.6.18.1 Description
7.6.18.2 Design Bases
7.6.18.3 Analysis
7.6.18.3.1 General Functional Requirements
7.6.18.3.2 Single Failure Criterion
7.6.18.3.3 Quality of Components
7.6.18.3.4 Equipment Qualification
7.6.18.3.5 Channel Integrity
7.6.18.3.6 Channel Independence
7.6.18.3.7 Control and Protection System Interaction
7.6.18.3.8 Derivation of System Inputs
7.6.18.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.18.3.10 Channel Bypass or Removal From Operation
7.6.18.3.11 Operating Bypasses
7.6.18.3.12 Indication of Bypass
7.6.18.3.13 Access to Means for Bypassing
7.6.18.3.14 Multiple Setpoints
7.6.18.3.15 Completion of Protective Action Once it is Initiated
7.6.18.3.16 Manual Initiation
7.6.18.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.18.3.18 Identification of Protective Action
7.6.18.3.19 Information Read-Out
7.6.18.3.20 System Repair
7.6.18.3.21 Identification
7.6.19 Fuel Handling Area Ventilation System Instrumentation and Control
7.6.19.1 Description
7.6.19.2 Design Bases
7.6.19.3 Analysis
7.6.19.3.1 General Functional Requirements
7.6.19.3.2 Single Failure Criterion
7.6.19.3.3 Quality of Components and Modules
7.6.19.3.4 Equipment Qualification
7.6.19.3.5 Channel Integrity
7.6.19.3.6 Channel Independence
7.6.19.3.7 Control and Protection System Interaction
7.6.19.3.8 Derivation of System Inputs
7.6.19.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.19.3.10 Channel Bypass or Removal From Operation
7.6.19.3.11 Operating Bypasses
7.6.19.3.12 Indication of Bypass
7.6.19.3.13 Access to Means for Bypassing
7.6.19.3.14 Multiple Setpoints
7.6.19.3.15 Completion of Protective Action Once it is Initiated
7.6.19.3.16 Manual Initiation
7.6.19.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.19.3.18 Identification of Protective Action
7.6.19.3.19 Information Read-Out
7.6.19.3.20 System Repair
7.6.19.3.21 Identification
7.6.20 Reactor Coolant System Overpressure Protection System for Low Pressure/Temperature, Water Solid Conditions
7.6.20.1 Description
7.6.20.2 Design Bases

7.6.20.3 Analysis
7.6.20.3.1 General Functional Requirements
7.6.20.3.2 Single Failure Criterion
7.6.20.3.3 Quality of Components and Modules
7.6.20.3.4 Equipment Qualification
7.6.20.3.5 Channel Integrity
7.6.20.3.6 Channel Independence
7.6.20.3.7 Control and Protection System Interaction
7.6.20.3.8 Derivation of System Inputs
7.6.20.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.20.3.10 Channel Bypass or Removal From Operation
7.6.20.3.11 Operating Bypasses
7.6.20.3.12 Indication of Bypass
7.6.20.3.13 Access to Means for Bypassing
7.6.20.3.14 Multiple Setpoints
7.6.20.3.15 Completion of Protective Action Once it is Initiated
7.6.20.3.16 Manual Initiation
7.6.20.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.20.3.18 Identification of Protective Action
7.6.20.3.19 Information Read-Out
7.6.20.3.20 System Repair
7.6.20.3.21 Identification
7.6.21 Nuclear Service Water Pump Structure Ventilation System
7.6.21.1 Description
7.6.21.2 Design Basis
7.6.21.3 Analysis
7.6.21.3.1 General Functional Requirement
7.6.21.3.2 Single Failure
7.6.21.3.3 Quality of Components and Modules
7.6.21.3.4 Equipment Qualification
7.6.21.3.5 Channel Integrity
7.6.21.3.6 Channel Independence
7.6.21.3.7 Control and Protection System Interaction
7.6.21.3.8 Derivation of System Inputs
7.6.21.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.21.3.10 Channel Bypass or Removal From Operation
7.6.21.3.11 Operating Bypasses
7.6.21.3.12 Indication of Bypass
7.6.21.3.13 Access to Means for Bypassing
7.6.21.3.14 Multiple Setpoints
7.6.21.3.15 Completion of Protective Action Once it is Initiated
7.6.21.3.16 Manual Initiation
7.6.21.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.21.3.18 Identification of Protective Action
7.6.21.3.19 Information Read-Out
7.6.21.3.20 System Repair
7.6.21.3.21 Identification
7.6.22 Main Feedwater Flow Isolation on High Doghouse Water Level Instrumentation
7.6.22.1 Description
7.6.22.2 Design Bases
7.6.22.3 Analysis
7.6.22.3.1 General Functional Requirements
7.6.22.3.2 Single Failure Criterion
7.6.22.3.3 Quality of Components and Modules
7.6.22.3.4 Equipment Qualification
7.6.22.3.5 Channel Integrity

7.6.22.3.6 Channel Independence
7.6.22.3.7 Control and Protection System Interaction
7.6.22.3.8 Derivation of System Inputs
7.6.22.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.22.3.10 Channel Bypass or Removal From Operation
7.6.22.3.11 Operating Bypasses
7.6.22.3.12 Indication of Bypass
7.6.22.3.13 Access to Means for Bypassing
7.6.22.3.14 Multiple Setpoints
7.6.22.3.15 Completion of Protection Action Once it is Initiated
7.6.22.3.16 Manual Initiation
7.6.22.3.17 Access to Setpoint Adjustments, Calibration, and Test Points
7.6.22.3.18 Identification of Protective Action
7.6.22.3.19 Information Read-Out
7.6.22.3.20 System Repair
7.6.22.3.21 Identification
7.6.23 Boron Dilution Mitigation System
7.6.23.1 Description
7.6.23.2 Design Bases
7.6.23.3 Analysis
7.6.23.3.1 General Functional Requirement
7.6.23.3.2 Single Failure Criterion
7.6.23.3.3 Quality of Components
7.6.23.3.4 Equipment Qualification
7.6.23.3.5 Channel Integrity
7.6.23.3.6 Channel Independence
7.6.23.3.7 Control and Protection System Interaction
7.6.23.3.8 Derivation of System Inputs
7.6.23.3.9 Capability for Test, Calibration, and Sensor Checks
7.6.23.3.10 Channel Bypass or Removal From Operation
7.6.23.3.11 Operating Bypasses
7.6.23.3.12 Indication of Bypass
7.6.23.3.13 Access to Means for Bypassing
7.6.23.3.14 Multiple Setpoints
7.6.23.3.15 Completion of Protection Action Once it is Initiated
7.6.23.3.16 Manual Initiation
7.6.23.3.17 Access to Setpoint Adjustments, Calibration, and Test Point
7.6.23.3.18 Identification of Protective Action
7.6.23.3.19 Information Read-Out
7.6.23.3.20 System Repair
7.6.23.3.21 Identification
7.6.24 References

7.7 Control Systems Not Required for Safety
7.7.1 Description
7.7.1.1 Reactor Control System
7.7.1.2 Rod Control System
7.7.1.2.1 Full Length Rod Control System
7.7.1.2.2 Rod Control System Failures
7.7.1.3 Plant Control Signals for Monitoring and Indicating
7.7.1.3.1 Monitoring Functions Provided by the Nuclear Instrumentation System
7.7.1.3.2 Rod Position Monitoring of Full Length Rods
7.7.1.3.3 Control Bank Rod Insertion Monitoring
7.7.1.3.4 Rod Deviation Alarm
7.7.1.3.5 Rod Bottom Alarm
7.7.1.4 Plant Control System Interlocks

7.7.1.4.1 Rod Stops
7.7.1.4.2 Automatic Turbine Load Runback
7.7.1.4.3 Turbine Loading Stop
7.7.1.5 Pressurizer Pressure Control
7.7.1.6 Pressurizer Water Level Control
7.7.1.7 Steam Generator Water Level Control
7.7.1.8 Steam Dump Control
7.7.1.8.1 Load Rejection Steam Dump Controller
7.7.1.8.2 Plant Trip Steam Dump Controller
7.7.1.8.3 Steam Header Pressure Controller
7.7.1.9 Incore Instrumentation
7.7.1.9.1 Thermocouples
7.7.1.9.2 Movable Neutron Flux Detector Drive System
7.7.1.9.3 Control and Readout Description
7.7.1.10 Boron Concentration Measurement System
7.7.1.11 ATWS Mitigation Actuation Circuitry
7.7.2 Analysis
7.7.2.1 Separation of Protection and Control System
7.7.2.2 Response Considerations of Reactivity
7.7.2.3 Step Load Changes Without Steam Dump
7.7.2.4 Loading and Unloading
7.7.2.5 Load Rejection Furnished By Steam Dump System
7.7.2.6 Reactor Trip
7.7.3 References

7.8 Operating Control Stations
7.8.1 General Layout
7.8.2 Monitor Light Panels
7.8.3 ESF Bypass Indication
7.8.4 Summary of Alarms
7.8.5 Auxiliary Control Stations
7.8.6 Safety Features
7.8.7 Occupancy
7.8.8 Loose Parts Monitoring System

THIS PAGE LEFT BLANK INTENTIONALLY.

List of Tables

Table 7-1. List of Reactor Trips

Table 7-2. Protection System Interlocks

Table 7-3. Reactor Trip System Instrumentation

Table 7-4. Reactor Trip Correlation

Table 7-5. Instrumentation Operating Condition for Engineered Safety Features

Table 7-6. Instrument Operating Conditions for Isolation Functions

Table 7-7. Interlocks for Engineered Safety Features Actuation System

Table 7-8. Auxiliary Shutdown Panel A Instrumentation And Controls Available For Hot Shutdown

Table 7-9. Auxiliary Shutdown Panel B Instrumentation And Controls Available For Hot Shutdown

Table 7-10. Auxiliary Feedwater Pump Turbine Control Panel Instrumentation And Controls Available For Hot Shutdown

Table 7-11. Control Room Indicators and/or Recorders Available to the Operator to Monitor Significant Plant Parameters During Normal Operation

Table 7-12. Plant Control System Interlocks

Table 7-13. Deleted Per 1990 Update

Table 7-14. ESF Bypass Indication

Table 7-15. ESF Response Times

Table 7-16. Main Control Board Indicators and/or Recorders Available to the Operator (Condition II, III, and IV Events)

THIS PAGE LEFT BLANK INTENTIONALLY.

List of Figures

Figure 7-1. Protection System Block Diagram

Figure 7-2. Instrumentation and Control System Diagrams - Index and Symbols
Instrumentation and Control System Diagrams - Index and Symbols

Figure 7-3. Setpoint Reduction Function for Overpower and Overtemperature □T Trips

Figure 7-4. Typical ESF Test Circuits

Figure 7-5. Engineered Safeguards Test Cabinet Index, Notes, and Legend

Figure 7-6. Motor-Driven Auxiliary Feedwater Pump Alignment to NSW Logic Diagram

Figure 7-7. Turbine-Driven Auxiliary Feedwater Pump Alignment to NSW Logic Diagram

Figure 7-8. Component Cooling Water System Logic Diagram

Figure 7-9. Chemical and Volume Control System Logic Diagram

Figure 7-10. Residual Heat Removal Pump Logic Diagram

Figure 7-11. Deleted Per 1991 Update

Figure 7-12. Deleted Per 1993 Update

Figure 7-13. Cold Leg Accumulator Isolation Valves Control and Alarm Logic

Figure 7-14. Containment Pressure Control System Logic

Figure 7-15. RWST Level Signal for Safety Injection System Recirculation Sump Isolation Valves

Figure 7-16. Safety Injection System Recirculation Sump Isolation Valves

Figure 7-17. Reactor Coolant System Overpressure Protection System for Low Pressure/Temperature Water Solid Conditions Logic Diagram

Figure 7-18. Rod Control System Block Diagram

Figure 7-19. Control Bank Rod Insertion Monitor Block Diagram

Figure 7-20. Rod Deviation Comparator

Figure 7-21. Pressurizer Pressure Control

Figure 7-22. Pressurizer Level Control System Block Diagram

Figure 7-23. Steam Generator Level Control
Steam Generator Level Control

Figure 7-24. Main Feedwater Pump Speed Control System Block Diagram

Figure 7-25. Steam Dump Control System

Figure 7-26. Basic Flux-Mapping System

Figure 7-27. Deleted Per 1990 Update

Figure 7-28. Deleted Per 1990 Update

Figure 7-29. Deleted Per 1990 Update

Figure 7-30. Deleted Per 2000 Update

Figure 7-31. Rod Control System Simplified Block Diagram

Figure 7-32. Control Bank D Power Cabinets 1BD and 2BD Partial Schematic Diagram

Figure 7-33. Deleted Per 1995 Update

7.0 Instrumentation and Controls

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.0.

THIS PAGE LEFT BLANK INTENTIONALLY.

7.1 Introduction

This chapter presents the various plant instrumentation and control systems by relating the functional performance requirements, design bases, system descriptions, design evaluations, and tests and inspections for each. The information provided in this chapter emphasizes these instruments and associated equipment which constitute the protection system as defined in IEEE 279-1971 "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations".

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

It is shown that the applicable criteria and codes, such as General Design Criteria and IEEE Standards, concerned with the safe generation of nuclear power are met by these systems. (See Section 7.1.2.4 for a discussion of applicable design criteria).

Definitions

Terminology used in this chapter is based on the definitions given in IEEE 279-1971. In addition, the following definitions apply:

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

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

Cold Shutdown Condition - When the reactor is subcritical by at least 1 percent $\Delta k/k$ and T_{avg} is $\leq 200°F$.

Hot Shutdown Condition - When the reactor is subcritical, by an amount greater than or equal to the margin to be specified in the applicable Technical Specification, and T_{avg} is greater than the temperature to be specified in the applicable Technical Specification.

Phase A Containment Isolation - Closure of all non-essential process lines which penetrate the containment initiated by the safety injection signal.

Phase B Containment Isolation - Closure of remaining process lines, initiated by containment Hi-Hi pressure signal (process lines do not include Engineered Safety Features lines).

System Response Times:

Reactor Trip System Response Time

The time delays are defined as the time required for the reactor trip (i.e., the time the rods are free and begin to fall) to be initiated following a step change in the variable being monitored from 5 percent below (or above) to 5 percent above (or below) the trip setpoint.

Engineered Safety Features Actuation System Response Time

The interval required for the Engineered Safety Features sequence to be initiated subsequent to the point in time that the appropriate variable (s) exceed setpoints. The response time includes sensor/process (analog) and logic (digital) delay.

Reproducibility - This definition is taken from Scientific Apparatus Manufactures Association (SAMA) Standard PMC-20.2-1973, Process Measurement and Control Terminology: "the closeness of agreement among repeated measurements of the output for the same value of input, under normal operating conditions over a period of time, approaching from both directions." It includes drift due to environmental effects, hysteresis, long-term drift, and repeatability. Long-term drift (aging of components, etc.) is not an important factor in accuracy requirements since, in general, the drift is not significant with respect to the time elapsed between testing. Therefore, long-term drift may be eliminated from this definition. Reproducibility, in most cases, is a part of the definition of accuracy (see below).

Accuracy - This definition is derived from Scientific Apparatus Manufactures Association (SAMA) Standard PMC-20.1-1973, Process Measurement and Control Terminology. An accuracy statement for a device falls under Note 2 of the SAMA definition of accuracy, which means reference accuracy or the accuracy of that device at reference operating conditions: "Reference accuracy includes conformity, hysteresis and repeatability." To adequately define the accuracy of a system, the term reproducibility is useful as it covers normal operating conditions. The following terms, "trip accuracy" and "indicated accuracy" etc., will then include conformity and reproducibility under normal operating conditions. Where the final result does not have to conform to an actual process variable but is related to another value established by testing, conformity may be eliminated, and the term reproducibility may be substituted for accuracy.

Normal Operating Conditions - For this document, these conditions cover all normal process temperature and pressure changes. Also included are ambient temperature changes around the transmitter and racks. This document does not include any accuracies under "post-accident" conditions.

Readout Devices - For consistency the final device of a complete channel is considered a readout device. This includes indicators, recorders, isolators (nonadjustable), and controllers.

Channel Accuracy - This definition includes accuracy of primary elements, transmitter and rack modules. It does not include readout devices or rack environmental effects, but does include process and environmental effects on field-mounted hardware. Rack environmental effects are included in the next two definitions to avoid duplication due to dual inputs.

Indicated and/or Recorded Accuracy - This definition includes channel accuracy, accuracy of readout devices, and rack environmental effects.

Trip Accuracy - This definition includes comparator accuracy, channel accuracy for each input, and rack environmental effects. This is the tolerance expressed in process terms (or percent of span) within which the complete channel must perform its intended trip function. This includes all instrument errors but no process effects such as streaming. The term "actuation accuracy" may be used where the word "trip" might cause confusion (for example, when starting pumps and other equipment).

Control Accuracy - This definition includes channel accuracy, accuracy of readout devices (isolator, controller), and rack environmental effects. Where an isolator separates control and protection signals, the isolator accuracy is added to the channel accuracy to determine control accuracy, but credit is taken for tuning beyond this point; i.e., the accuracy of these modules (excluding controllers) is included in the original channel accuracy. It is simply defined as the accuracy of the control signal in percent of the span of that signal. This will then include gain

changes where the control span is different from the span of the measured variable. Where controllers are involved, the control span is the input span of the controller. No error is included for the time in which the system is in a non-steady state condition.

7.1.1 Identification of Safety-Related Systems

The instrumentation and control systems and supporting systems required to function to achieve the system responses assumed in the safety evaluations and those needed to shutdown the plant safely are given in this Section.

These systems have definitive functional requirements developed on the bases of the Westinghouse NSSS design. Figure 7-2 defines the scope interface. Regardless of the supplier, the functional requirements necessary to assure plant safety and proper control are clearly defined.

System functions for the safety-related systems identified below are similar to those of the McGuire Nuclear Station (See Section 1.3 for a comparison table).

7.1.1.1 Reactor Trip System

The Reactor Trip System is a functionally defined system described in Section 7.2. The equipment that provides the trip functions is also identified and discussed in Section 7.2. The design bases for the Reactor Trip System are given in Section 7.1.2.1. Figure 7-2, page 3 shows a single-line diagram of this system.

7.1.1.2 Engineered Safety Features Actuation System

The Engineered Safety Features Actuation System (ESFAS) is a functionally defined system described in Section 7.3. The equipment that provides the actuation functions is identified and discussed in Section 7.3. Design bases for the ESFAS are given in Section 7.1.2.1.

7.1.1.3 Systems Required for Safe Shutdown

The systems required for safe shutdown are described in Section 7.4. The design bases for each of these systems are given in the discussion of the system.

7.1.1.4 Safety-Related Display Instrumentation

The safety-related display instrumentation that provides the operator with information to enable him to monitor the results of Engineered Safety Features actions following a Condition II, III, or IV event is described in Section 7.5.

7.1.1.5 Other Systems Required for Safety

Other systems required for safety that are not included in Sections 7.1.1.1, 7.1.1.2, 7.1.1.3, and 7.1.1.4 are described in Section 7.6. The design bases for each of these systems are given in the discussion of the system.

7.1.2 Identification of Safety Criteria

Section 7.1.2.1 gives design bases for the systems given in Section 7.1.1.1 and 7.1.1.2.

The electrical control circuits of all safety-related equipment have been reviewed and it has been determined that the disabling of one component will not inadvertently render other components inoperable for engineered safety features operation.

Conservative considerations for instrument errors are included in the accident analyses presented in Chapter 15. Functional requirements, developed on the basis of the results of the accident analyses, which have utilized conservative assumptions and parameters are used in designing these systems and a preoperational testing program verifies the adequacy of the design. Accuracies are given in Sections 7.2, 7.3 and 7.5.

The documents discussed in Section 7.1.2.4 were considered in the design of the systems given in Section 7.1.1. In general, the scope of these documents is given in the document itself. This determines the systems or parts of systems to which the document is applicable.

7.1.2.1 Design Bases

7.1.2.1.1 Reactor Trip System

The Reactor Trip System acts to limit the consequences of Condition II events (faults of moderate frequency, such as loss of feedwater flow) by, at most, a shutdown of the reactor and turbine with the plant capable of returning to operation after corrective action. The Reactor Trip System features impose a limiting boundary region to plant operation which ensures that the reactor safety limits are not exceeded during Condition II events and that these events can be accommodated without developing into more severe conditions. Reactor trip setpoints are given in the Technical Specifications.

The design requirements for the Reactor Trip System are derived by analyses of plant operating and fault conditions where automatic rapid control rod insertion is necessary in order to prevent or limit core or reactor coolant boundary damage. The design bases addressed in IEEE 279-1971 are discussed in Section 7.2.1. The design limits specified by Westinghouse for the Reactor Trip System are:

1. Minimum DNBR shall not be less than the minimum allowable DNBR as a result of any anticipated transient or malfunction (Condition II faults).
2. Power density shall not exceed the rated linear power density for Condition II faults. See Chapter 4 for fuel design limits.
3. The stress limit of the Reactor Coolant System for the various conditions shall be as specified in Chapter 5.
4. Release of radioactive material shall not be sufficient to interrupt or restrict public use of those areas beyond the exclusion radius as a result of any Condition III fault.
5. For any Condition IV fault, release of radioactive material shall not result in an undue risk to public health and safety.

7.1.2.1.2 Engineered Safety Features Actuation System

The Engineered Safety Features Actuation System acts to limit the consequences of Condition III events (infrequent faults such as primary coolant spillage from a small rupture which exceeds normal charging system makeup and requires actuation of the Safety Injection System). The Engineered Safety Features Actuation System acts to mitigate Condition IV events (limiting faults, which include the potential for significant release of radioactive material).

The design bases for the Engineered Safety Features Actuation System are derived from the design bases given in Chapter 6 for the Engineered Safety Features. Design bases requirements of IEEE 279-1971 are addressed in Section 7.3.1.2. General design requirements are given below.

1. Automatic Actuation Requirements

   The primary requirement of the Engineered Safety Features Actuation System is to receive input signals (information) from the various on-going processes within the reactor plant and containment and automatically provide, as output, timely and effective signals to actuate the various components and subsystems comprising the Engineered Safety Features System.

2. Manual Actuation Requirements

   The Engineered Safety Features Actuation System has provisions in the control room for manually initiating the functions of the Engineered Safety Features System.

7.1.2.1.3 Interlocks

Interlocks are discussed in Sections 7.2, 7.3, 7.6 and 7.7. The protection (P) interlocks are given on Table 7-2 and Table 7-7. The safety analyses demonstrates that even under conservative critical conditions for either postulated or hypothetical accidents, the protective systems ensure that the NSSS will be put into and maintained in a safe state following an ANS Condition II, III or IV accident commensurate with applicable Technical Specifications and pertinent ANS Criteria. Therefore the protective systems are entirely redundant and separate, including all permissives and blocks and have been designed to meet General Design Criteria 20, 21 and 22. In addition, all blocks/bypasses of a protective function, as listed in Table 7-2 and Table 7-7, are automatically cleared whenever the permissives conditions are not met, in accordance with paragraph 4.12 of IEEE 279-1971. Control interlocks (C) are identified on Table 7-12. Because control interlocks are not safety-related, they have not been specifically designed to meet the requirements of IEEE Protection System Standards.

7.1.2.1.4 Bypasses

Bypasses are designed to meet the requirements of IEEE 279-1971, paragraphs 4.11, 4.12, 4.13 and 4.14. A discussion of bypasses provided is given in Sections 7.2 and 7.3.

7.1.2.1.5 Equipment Protection

The criteria for equipment protection are given in Chapter 3. Equipment related to safe operation of the plant is designed, constructed, and installed to protect it from complete destruction by fire, missiles, or other natural hazards.

7.1.2.1.6 Diversity

Functional diversity has been designed into the Reactor Protection System. Functional diversity is discussed in Reference 10. The extent of diverse system variables has been evaluated for a wide variety of postulated accidents. Generally, two or more diverse protection functions would automatically terminate an accident before unacceptable consequences could occur.

For example, there are automatic reactor trips based upon neutron flux measurements, reactor coolant loop temperature measurements, pressurizer pressure and level measurements, and reactor coolant pump underfrequency and undervoltage measurements, as well as a manual trip, and a trip initiated by a safety injection signal.

Regarding the Engineered Safety Features Actuation System, for a loss of coolant accident, a safety injection signal can be obtained manually or by automatic initiation from two diverse parameter measurements.

1. Low pressurizer pressure

2. High containment pressure

For a steam break accident, safety injection signal actuation is provided by:

1. Low pressurizer pressure
2. For a steam break inside containment, high containment pressure (Hi-Hi) provides an additional parameter for generation of the signal.

All of the above sets of signals are redundant and physically separated and meet the requirements of IEEE 279-1971.

7.1.2.1.7 Bistable Trip Setpoints

Three bistable trip setpoint values are specified which are applicable to reactor trip and engineered safety features actuation:

1. Safety limit setpoint
2. Limiting value
3. Nominal setpoint

The safety limit is the value assumed in the accident analysis and is the least conservative value.

The limiting value is the Technical Specification value and is obtained by subtracting a safety margin from the safety limit. The safety margin accounts for instrument error, process uncertainties such as flow stratification and transport factor effects, etc.

The nominal setpoint is the value set into the equipment and is obtained by subtracting allowances for instrument drift from the limiting value. The nominal setpoint allows for the normal expected instrument setpoint drifts such that the Technical Specification limits will not be exceeded under normal operation.

The setpoints that require trip action are given in the Technical Specifications. A further discussion on setpoints is found in Section 7.2.2.2.1.

The trip setpoint is determined by factors other than the most accurate portion of the instrument's range. The safety limit value is determined only by the accident analysis. As described above, allowance is then made for process uncertainties, instrument error, instrument drift, and calibration uncertainty to obtain the nominal setpoint value which is actually set into the equipment. The only requirement on the instrument's accuracy value is that over the instrument span, the error must always be less than or equal to the error value allowed in the accident analysis. The instrument does not need to be the most accurate at the setpoint value as long as it meets the minimum accuracy requirement. The accident analysis accounts for the expected errors at the actual setpoint.

Range selection for the instrumentation covers the expected range of the process variable being monitored consistent with its application. The design of the Reactor Protection and Engineered Safety Features Systems is such that the bistable trip setpoints do not require process transmitters to operate within 5 percent of the high and low end of their calibrated span or range. Functional requirements established for every channel in the Reactor Protection and Engineered Safety Features Systems stipulate the maximum allowable errors for accuracy. The protection channels have the capability for, and are tested to ascertain that the characteristics throughout the entire span in all aspects are acceptable and meet functional requirement specifications. As a result, no protection channel normally operates within 5 percent of the limits of its specified span.

In this regard, it should be noted that the specific functional requirements for response time, setpoint, and operating span will be finalized contingent on the results and evaluation of safety studies to be carried out using data pertinent to the plant. Emphasis is placed on establishing adequate performance requirements under both normal and faulted conditions. This will include consideration of process transmitters margins such that even under a highly improbable situation of full power operation at the limits of the operating map (as defined by the high and low pressure reactor trip, δT overpower and overtemperature trip lines (DNB protection), and the steam generator safety valve pressure setpoint) that adequate instrument response is available to ensure plant safety.

As Found/As Left Tolerance

Several RPS/ESFAS functions have requirements stated n the Technical Specifications that operation of the channels will be gauged against the As-Found and As-Left Tolerances in accordance with TSTF-493 Rev. 4 (Ref. 11). For those specific functions, a methodology is used to determine the allowable calibration tolerances to further assure that the instrument channels are operating within the bounds defined in the Safety Analysis.

"As Found" is the condition in which a channel, or portion of a channel, is found after a period of operation and before recalibration, if necessary. The As-Found Tolerance is the allowance that the channel, or portion thereof, is expected to be within based on uncertainty calculations which ensure the channel is capable of producing a trip prior to reaching the Safety Analysis Analytical Limit. Values recorded during a channel As-Found surveillance which are within the As-Found Tolerance would clearly indicate a channel is operating as intended. Values recorded duirng a channel As-Found surveillance which exceed the As-Found Tolerance would be assessed to determine if the channel can continue to perform after adjustment within the bounds defined in the Safety Analysis.

Normally, the As-Found Tolerance would be equivalent to the errors verified during the surveillance. Therefore, the uncertainty terms which make up the As-Found Tolerance for the portion of the channel under surveillance would typically include the square root sum of squares combination of reference accuracy, drift and measurement and test equipment uncertainty effects (e.g. M&TE Uncertainty and M&TE Reading Resolution). Inclusion of additional uncertainty terms (e.g. normal radiation effect, tubing error effects) may be included but must be justified. Additionally, the uncertainty terms may be treated as bias if a random, independent correlation of the terms cannot be assured. As-Found Tolerance more conservative than the value calculated by this method may be used with appropriate justification.

"As-Left" is the condition in which a channel, or portion of a channel, is left after calibration or final setpoint device setpoint verification. The As-Left Tolerance is the acceptable setting variation about the setpoint that the technician may leave the setting following calibration.

Uncertainty terms which make up the As-Left Tolerance for the portion of the channel under surveillance would typically include the square root sum of squares combination of reference accuracy and measurement and test equipment uncertainty effects (e.g. M&TE Uncertainty and M&TE Reading Resolution). Inclusion of additional uncertainty terms (e.g. normal radiation effect, tubing error effects) may be included but must be justified. Additionally, the uncertainty terms may be treated as bias if a random, independent correlation of the terms cannot be assured. As-Left Tolerances more conservative than the value calculated by this method may be used without further justification. See Reference 11 for additional information.

7.1.2.1.8 Emergency Power

The design bases for the instrumentation and controls emergency power supply is given in Sections 8.3.2.1.2.1 and 8.3.2.2.

7.1.2.2 Independence of Redundant Systems

The safety-related systems in Section 7.1.1 are designed to meet the independence and separation requirements of Criterion 22 of the 1971 General Design Criteria and paragraph 4.6 of IEEE 279-1971.

The electrical power supply, instrumentation, and control conductors for redundant circuits of a nuclear plant have physical separation to preserve the redundancy and to ensure that no single credible event will prevent operation of the associated function due to electrical conductor damage. Critical circuits and functions include power, control, and analog instrumentation associated with the operation of the Reactor Trip System or Engineered Safety Features Actuation System. Credible events include, but are not limited to, the effects of short circuits, pipe rupture, missiles, and fire and are considered in the basic plant design.

The protection system uses redundant instrumentation channels and actuation trains and incorporates physical and electrical separation to prevent faults in one channel from degrading any other protection channel. The Westinghouse design of protection systems incorporates overcurrent devices to prevent malfunctions in one circuit from causing unacceptable influences on the functioning of the protection system.

Westinghouse test programs have demonstrated that the Class 1E protection systems (Nuclear Instrumentation System, Solid State Protection System, and the 7300 Process Control System) are not degraded by Non-Class 1E circuits sharing the same enclosure. Tests conducted on the as-built designs of the NIS and SSPS were reported and accepted by the NRC in support of the Diablo Canyon Application (Docket No.'s 50-275 and 50-323). Westinghouse considers these programs applicable to all plants, including Catawba. Westinghouse tests on the 7300 PCS were covered in a report titled "7300 Series Process Control System Noise Tests" subsequently reissued as WCAP-8892. In a letter dated April 20, 1977, R. Tedesco to C. Eicheldinger, the NRC accepted this report in which its applicability to Catawba is established.

In the NIS, PCS, and SSPS input cabinets where redundant channel instrumentation are physically adjacent, there are no wire ways or cable penetrations which would permit, for example, a fire resulting from electrical failure in one channel to propagate into redundant channels in the logic racks. Other redundant analog channels are separated by locating modules in different cabinets.

Electrical isolation in the BOP circuit design is achieved by the use of optical isolation devices. The isolation devices are designed and successfully tested for maintaining a minimum of 2300 vrms isolation between the input and output circuitry.

A description of criterion used for physical separation of Class 1E circuits is provided in Section 8.3.1.4.

7.1.2.3 Physical Identification of Safety-Related Equipment

There are four separate protection sets identifiable with process equipment associated with the Reactor Trip and Engineered Safeguards Actuation Systems. A protection set may be comprised of more than a single process equipment cabinet. The color coding of each process equipment rack nameplate coincides with the color code established for the protection set of which it is a part. Redundant channels are separated by locating them in different equipment

cabinets. Separation of redundant channels begins at the process sensors and is maintained in the field wiring, containment penetrations and equipment cabinets to the redundant trains in the logic racks. At the logic racks the protection set color coding for redundant channels is clearly maintained until the channel loses its identity in the redundant logic trains. The color coded nameplates described below provide identification of equipment associated with protective functions and their channel set association:

PROTECTION SET	COLOR CODING
I	RED
II	WHITE
III	BLUE
IV	YELLOW

Red is used to identify Train A, and yellow is used to identify Train B.

All non-cabinet mounted protective equipment and components are provided with channel or train identification. Small electrical components such as relays have channel or train identification on the enclosures which house them.

For additional information regarding the physical identification of Class 1E equipment, refer to Section 8.3.1.3.

7.1.2.4 Design Criteria

The design criteria, including the General Design Criteria, NRC Regulatory Guides, and IEEE Standards, that are considered in the design of the safety-related instrumentation and controls are presented and discussed below.

7.1.2.4.1 General Design Criteria

The General Design Criteria of 10CFR 50, Appendix A, are discussed in Section 3.1.

7.1.2.4.2 NRC Regulatory Guides

Regulatory Guide 1.11 (Safety Guide 11, Dated 3/10/71)

Instrument lines that penetrate the Containment are sized and provided with isolation valves in compliance with the recommendations of Regulatory Guide 1.11 as discussed in Section 6.2.4.1.

Regulatory Guide 1.22 (Safety Guide 22, Dated 2/17/72)

Periodic testing of the Reactor Trip and Engineered Safety Features Actuation Systems, as described in Sections 7.2.2 and 7.3.2, complies with Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions."

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

The actuation logic for the Reactor Trip and Engineered Safety Features Actuation System is tested as described in Sections 7.2 and 7.3. As recommended by Regulatory Guide 1.22, where actuated equipment is not tested during reactor operation it has been determined that:

1. There is no practicable system design that would permit operation of the equipment without adversely affecting the safety or operability of the plant;
2. The probability that the protection system will fail to initiate the operation of the equipment is, and can be maintained, acceptably low without testing the equipment during reactor operation; and
3. The equipment can routinely be tested when the reactor is shut down.

The equipment that cannot be tested at full power so as not to damage equipment or upset plant operation is as follows:

1. Manual actuation switches
2. Turbine
3. Main steam line isolation valves (close)
4. Main feedwater isolation valves (close)
5. Feedwater control valves (close)
6. Main feedwater pumps
7. Reactor coolant pump component cooling water isolation valves (close)
8. Reactor coolant pump seal water return valves (close)
9. Residual Heat Removal Pumps Containment Sump Suction Valves (NI-184B and NI-185A)
10. Centrifugal charging Pump Cold Leg Injection Isolation Valves (NI-9 and NI-10)
11. Certain valves in the Chemical Volume and Control (NV-10A, 11A, 13A, 15B, 312A, 314B, 188A, 189B, 252A, and 253B)
12. Reactor Coolant Drain Tank Heat Exchanger Component Cooling Isolation Valves (KC-320A, KC-332B, and KC-333A)
13. Fire Suppression Containment Isolation Valves (RF-389B and RF-447B)
14. Nuclear Service Water Valves RN-484A, RN-437B, and RN-487B
15. Instrument Air Valve VI-77B
16. Blowdown Valves BB-8A, BB-10B, BB-19A, BB-21B, BB-56A, BB-57B, BB-60A, and BB-61B.

The justifications for not testing the above sixteen items at full power are discussed below.

1. Manual Actuation Switches - These would cause initiation of their protection system function at power causing plant upset and/or reactor trip. It should be noted that the reactor trip function that is derived from the automatic safety injection signal is tested at power as follows:

   The analog signals, from which the automatic safety injection signal is derived, is tested at power in the same manner as the other analog signals and as described in Section 7.2.2.2.3 (10). The processing of these signals in the Solid State Protection System (SSPS) wherein their channel orientation converts to a logic train orientation is tested at power by the built-in

semi-automatic test provisions of the SSPS. The reactor trip breakers are tested at power as discussed in Section 7.2.2.2.3 (10).

2. Turbine

   A discussion of the turbine is provided in Section 10.2.2.

3. Closing the Main Steam Line Stop Valves

   Main steam isolation valves are routinely tested during refueling outages. Testing of main steam isolation valve closure at power is not practical. As the plant power is increased, the coolant average temperature is programmed to increase. If the valves are closed under these elevated temperature conditions, the steam pressure transient would unnecessarily operate the steam generator relief valves and possibly the steam generator safety valves. The steam pressure transient produced would cause shrinkage in steam generator level, which would cause the reactor to trip on low-low steam generator water level. Testing during operation will decrease the operating life of the valve.

   Based on the above identified problems incurred with periodic testing of the main steam line isolation valves at power and since, 1) no-practical system design will permit operation of the valves without adversely affecting the safety or operability of the plant, 2) the probability that the protection system will fail to initiate the actuated equipment is acceptably low due to test up to final actuation, and 3) these valves will be routinely tested during refueling outages, the proposed resolution meets the guidelines of Section D.4 of Regulatory Guide 1.22.

4. Closing the Feedwater Isolation Valve

   The feedwater isolation valves are routinely tested during refueling outages. Periodic testing of these feedwater isolation valves by closing them completely, or partially, at power would induce steam generator water level transients and oscillations which would trip the reactor. These transient conditions would be caused by perturbing the feedwater flow and pressure conditions necessary for proper operation of the variable-speed feedwater pump control system and the steam generator water level control system.

   Based on these identified problems incurred with periodic testing of the feedwater isolation valves at power and since 1) no practical system design will permit operation of these valves without adversely affecting the safety or operability of the plant, 2) the probability that the protection system will fail to initiate the activated equipment is acceptably low due to testing up to final actuation, and 3) these valves will be routinely tested during refueling outages, the proposed resolution meets the guidelines of Section D.4 of Regulatory Guide 1.22.

5. Closing the Feedwater Control Valves

   These valves are routinely tested during refueling outages. To close them at power would adversely affect the operability of the plant. The verification of operability of feedwater control valves at power is assured by confirmation of proper operation of the steam generator water level system. Testing of the solenoids which provide the closing function for these valves is periodically performed at power as discussed in Section 7.3.2.2.5. The operability of the slave relays which actuate the solenoid is verified during this test. Although the actual closing of these control valves is blocked when the slave relay is tested, all functions are tested to assure that no electrical malfunctions have occurred which could defeat the protective function. It is noted that the solenoids work on the de-energize-to-actuate principle, so that the feedwater control valves will fail close upon either the loss of electrical power to the solenoids or loss of air pressure.

Based on the above, the testing of the isolating function of feedwater control valves meets the guidelines of Section D.4 of Regulatory Guide 1.22.

6. Main Feedwater Pumps

   The containment integrity analyses do not assume tripping of the feed-water pumps; therefore, the main feedwater pump trip solenoids are not considered safety-related and require no periodic testing. These functions are routinely tested during refueling outages. One out of three solenoid trip testing can be performed on-line without a CF pump trip.

   Some accidents in Chapter 15.1 do credit the CF pump trip in conjunction with closing of the feedwater control valves and feedwater isolation valves. The CF Pump trip is a third means of terminating feedwater flow to the steam generators in the event of a control valve malfunction that initiates excessive feedwater accident and single failure of a feedwater isolation valve to close. this accident is described in section 15.1.2 of the FSAR. The 15.1.2 accident is a condition II event. Condition II events do not cause fuel failure or risk secondary over-pressurization.

7. RCP Component Cooling Water Isolation Valves (Close)

   Component cooling water supply and return containment isolation valves are routinely tested during refueling outages. Testing of these valves while the reactor coolant pumps are operating introduces an unnecessary risk of costly damage to all the reactor coolant pumps. Loss of component cooling water to these pumps is of economic consideration only, as the reactor coolant pumps are not required to perform any safety-related function.

   The reactor coolant pumps will not seize due to complete loss of component cooling. Information from the pump manufacturer indicates that the bearing babbitt would eventually break down but not so rapidly as to overcome the inertia of the flywheel. If the pumps are not stopped within 3 to 10 minutes after component cooling water is isolated, pump damage could be incurred.

   Additional containment penetrations and containment isolation valves introduce additional unnecessary potential pathways for radioactive leakage following a postulated accident. Also, since the component cooling water flow rates and temperatures are about equal during both plant power operation and plant refueling, periodic tests of these valves during a refueling outage would duplicate accident conditions. Additionally, possibility of failure of containment isolation is remote because an additional failure of the low-pressure fluid system in addition to failure of both isolation valves would have to occur to open a path through the containment.

   Based on the above described potential reactor coolant pump damage incurred with periodic testing of the component cooling water containment isolation valves at power, the duplication of at-power operating conditions during refueling outages, and since 1) no practical system design will permit operation of these valves without adversely affecting the safety or operability of the plant, 2) the probability that the protection system will fail to initiate actuation, and 3) these valves will be routinely tested during refueling outages when the reactor coolant pumps are not operating, the pro- posed resolution meets the guidelines of Section D.4 of Regulatory Guide 1.22.

8. Seal Water Return Valves (Close)

   Seal return line isolation valves are routinely tested during refueling outages. Closure of these valves during operation would cause the safety valve to lift, with the possibility of valve chatter. Valve chatter would damage this relief valve. Testing of these valves at power would cause equipment damage. Therefore, these valves will be tested during scheduled

refueling outages. As above, additional containment penetrations and containment isolation valves introduce additional unnecessary potential path-ways for radioactive release following a postulated accident. Thus, the guidelines of Section D.4 of Regulatory Guide 1.22 are met.

9. Residual Heat Removal Pumps Containment Sump Suction Valves - These valves are routinely tested during refueling outages. It is not practical to test these valves at power. Testing of these valves at power would introduce an unnecessary risk of flooding lower containment with potentially contaminated water.

   Based on the above identified problem with testing these valves at power and since, 1) no practical system design will permit operation of these valves without adversely affecting the safety or operability of the plant, 2) the probability that the protections system will fail to initiate the actuated equipment is acceptable low due to test up to final actuation, and 3) these valves will be routinely tested during refueling outages, the proposed resolution meets the guidelines of Section D.4 of Regulatory Guide 1.22.

10. Centrifugal Charging Pump Cold Leg Injection Isolation Valves - These valves are routinely tested during refueling outages. It is not practical to test these valves at power. Testing of these valves at power would result in flow of non-preheated water through the injection lines and thermal shocking of the injection nozzles. The introduction of colder water into the Reactor Coolant System would also be a reactivity management concern.

    Based on the above identified problem with testing these valves at power and since, 1) no practical system design will permit operation of these valves without adversely affecting the safety or operability of the plant, 2) the probability that the protections system will fail to initiate the actuated equipment is acceptable low due to test up to final actuation, and 3) these valves will be routinely tested during refueling outages, the proposed resolution meets the guidelines of Section D.4 of Regulatory Guide 1.22.

11. Certain valves in the Chemical Volume and Control System (NV-10A, 11A, 13A, 15B, 312A, 314B, 188A, 189B, 252A, and 253B)

    NV-10A, NV-11A, and NV-13A - Relief valve NV-14 has experienced lifting and subsequent seat leakage as a result of pressure transients during letdown orifice swaps. Any leakage past NV-14 is considered Reactor Coolant System leakage and directly impacts the Technical specifications. Therefore, it is not practical to test these valves during power operations. These valves are routinely tested during refueling outages.

    NV-15B - Testing of this valve at power would isolate letdown flow from the Reactor Coolant System. This could result in loss of pressurizer level control and cause plant shutdown. Therefore it is impractical to test this valve at power. This valve is routinely tested during refueling outages.

    NV-312A and NV-314B - Testing of these valves at power would isolate charging flow to the Reactor Coolant System. This could result in loss of pressurizer level control and cause plant shutdown. Therefore it is impractical to test these valves at power. These valves are routinely tested during refueling outages.

    NV-188A and NV-189B - Testing of these valves at power would isolate the normal suction of the charging pumps. Alternate suction paths would result in increasing the Reactor Coolant System boron concentration and could result in plant shutdown. Therefore it is not practical to test these valves at power. These valves are routinely tested during refueling outages.

NV-252A and NV-253B - Testing of these valves at power would require aligning the suction of the charging pumps to the Refueling Water Storage Tank. This would result in an increase in Reactor Coolant System boron concentration and could result in plant shutdown. Therefore it is not practical to test these valves at power. These valves are routinely tested during refueling outages.

Based on the above identified problems incurred with testing these valves at power and since, 1) no practical system design will permit operation of these valves without adversely affecting the safety or operability of the plant, 2) the probability that the protections system will fail to initiate the actuated equipment is acceptable low due to test up to final actuation, and 3) these valves will be routinely tested during refueling outages, these proposed resolutions meet the guidelines of Section D.4 of Regulatory Guide 1.22.

12. Reactor Coolant Drain Tank Heat Exchanger Component Cooling Isolation Valves - Testing of these valves at power would isolate the cooling water flow to the Reactor Coolant Drain Tank Heat Exchanger. This would result in boiling of the water in the drain tank resulting in excess heat in containment. This increased heat load could cause plant shutdown. Therefore it is not practical to test these valves at power. These valves are routinely tested during refueling outages.

    Based on the above identified problem with testing these valves at power and since, 1) no practical system design will permit operation of these valves without adversely affecting the safety or operability of the plant, 2) the probability that the protections system will fail to initiate the actuated equipment is acceptable low due to test up to final actuation, and 3) these valves will be routinely tested during refueling outages, the proposed resolution meets the guidelines of Section D.4 of Regulatory Guide 1.22.

13. Fire Suppression Containment Isolation Valves (RF-389B and RF-447B) - These valves are maintained closed (their safe position) during power operations. They are only opened upon verification of a fire in containment. Quarterly stroking of the valves introduces water into the containment header due to the piping configuration which has to be drained. Testing of these valves requires containment entry which exposes personnel to higher levels of radiation when draining the system. Also, the introduction of water accelerates corrosion and produces waste water. Therefore, based upon the above reasoning it is not practical to test these valves during power operation. The valves are tested routinely during refueling outages and at cold shutdown.

    Based upon the above identified problem with testing these valves at power and since, 1) no practical system design will permit operation of these valves without adversely affecting the safety or operability of the plant, 2) the probability that the protection system will fail to initiate the actuated equipment is acceptably low due to test up to final actuation, and 3) these valves will be routinely tested during refueling outages, the proposed resolution meets the guidelines of Section D.4 of Regulatory Guide 1.22.

14. Nuclear Service Water Valves (RN-484A, RN-437B and RN-487B) - The valves are normally open to provide cooling water to containment HVAC units during normal operation. If containment HVAC is lost during normal operation, the resulting increase in containment pressure could generate an "artificial" ESF actuation. Additionally these allow cooling water flow to the NC Pump Motor Air Coolers. Motor stator temperatures would increase due to closure of one of the valves, potentially resulting in the loss of the Reactor Coolant Pumps.

    Based upon the above identified problem with testing these valves at power and since, 1) no practical system design will permit operation of these valves without adversely affecting the safety or operability of the plant, 2) the probability that the protection system will fail to

initiate the actuated equipment is acceptable low due to test up to final actuation, and 3) these valves will be routinely tested during refueling outages, the proposed resolution meets the guidelines of Section D.4 of Regulatory Guide 1.22.

15. Instrument Air Valve (VI-77B) - Closing of the instrument air containment isolation prevents any air from entering containment and supplying various instruments, controllers, and air-operated valves. Even a short duration loss of air to containment can cause transients up to and potentially including a reactor trip. Both the charging line and letdown line have several air-operated valves that cannot tolerate a short duration loss of instrument air without resulting in a plant transient. Valves NV-10A, NV-11A, and NV-13A are air-operated valves and a loss of instrument air will fail these valves closed, resulting in a loss of letdown flow. The air-operated valve controlling charging flow (NV-294) fails open during a loss of air; thereby prevent the capability to reduce charging rate. The excess letdown line cannot be utilized since these valves are also air operated. If instrument air is not returned within a short period, this can lead to overfilling the pressurizer resulting in a reactor trip.

    Based upon the above identified problem with testing this valve at power since, 1) no practical system design will permit operation of these valves without adversely affecting the safety or operability of the plant, 2) the probability that the protection system will fail to initiate the actuated equipment is acceptable low due to test up to final actuation and 3) this valve will be routinely tested during refueling outages, the proposed resolution meets the guidelines of Section D.4 of Regulatory Guide 1.22.

16. Steam Generator Blowdown Valves (BB-8A, BB-10B, BB-19A, BB-21B, BB-56A, BB-57B, BB-60A, and BB-61B) - The valves are normally open to maintain steam generator blowdown to control the concentration of non-volatile solids and maintain proper secondary side chemistry. Closure of the valves during protection system testing results in a reactor thermal power increase; thus requiring reactor thermal power to be decreased prior to any protection system testing.

    Based upon the above identified reactivity management problem with testing these valves at power and since, 1) no practical system design will permit operation of these valves without adversely affecting the safety or operability of the plant, 2) the probability that the protection system will fail to initiate the actuated equipment is acceptably low due to test up to final actuation, and 3) these valves will be routinely tested during refueling outages, the proposed resolution meets the guidelines of Section D.4 of Regulatory Guide 1.22.

REGULATORY GUIDE 1.29 (Revision 3)

Class 1E instrumentation and control equipment is classified as Seismic Category I in accordance with the recommendations of Regulatory Guide 1.29. Category I electrical equipment is discussed in Section 3.10

REGULATORY GUIDE 1.30 (Safety Guide 30)

The quality assurance requirements for the installation, inspection, and testing of Class 1E instrumentation and controls is discussed in Chapter 17.

REGULATORY GUIDE 1.40 (Revision 0)

The qualification of continuous duty Class 1E motors installed inside the containment is discussed in Section 3.11.

REGULATORY GUIDE 1.47 (Revision 0)

The engineered safety features bypass indication panel is designed in accordance with the recommendations of Regulatory Guide 1.47. Bypass indication is discussed in Section 7.8.

REGULATORY GUIDE 1.53 (Revision 0)

The principles described in IEEE Standard 379-1972 were used in the design of the Westinghouse Protection System. The system complies with the intent of this standard and the additional guidance of Regulatory Guide 1.53 although the formal analyses have not been documented exactly as outlined. Westinghouse has gone beyond the required analyses and has performed a fault tree analysis, Reference 1.

The referenced topical report provides details of the analyses of the protection systems previously made to show conformance with single failure criterion set forth in paragraph 4.2 of IEEE Standard 279-1971. The interpretation of single failure criterion provided by IEEE Standard 379-1972 does not indicate substantial differences with the Westinghouse interpretation of the criterion except in the methods used to confirm design reliability. Established design criteria in conjunction with sound engineering practices form the bases for the Westinghouse protection systems. The Reactor Trip and Engineered Safeguards Actuation Systems are each redundant safety systems. The required periodic testing of these systems will disclose any failures or loss of redundancy which could have occurred in the interval between tests, thus ensuring the availability of these systems.

REGULATORY GUIDE 1.62 (Revision 0)

Means for manual initiation of protective actions are provided in the control room in accordance with the recommendations of Regulatory Guide 1.62.

REGULATORY GUIDE 1.63 (Revision 0)

Conformance to Regulatory Guide 1.63 is discussed in Sections 3.11.2.1.4 and 8.1.5.2.

REGULATORY GUIDE 1.68 (Revision 2)

Conformance to Regulatory Guide 1.68 is discussed in Table 14.1, Section 14.0, Section 3.11.2.1.4 and Section 8.1.5.2.

REGULATORY GUIDE 1.73 (Revision 0)

The qualification of Class 1E electric valve operators located inside containment is discussed in Section 3.11.

REGULATORY GUIDE 1.75 (Revision 1)

The recommendations of Regulatory Guide 1.75 are not applicable to Catawba based on the implementation date of the guide. The independence of redundant systems is discussed in Sections 7.1.2.2 and 8.3.1.4.

REGULATORY GUIDE 1.80 (Revision 0)

Conformance to Regulatory Guide 1.80 is discussed in Section 9.3.1.

REGULATORY GUIDE 1.89 (Revision 0)

The recommendations of Regulatory Guide 1.89 are not applicable to Catawba based on the implementation date of the guide. The seismic and environmental qualifications of Class 1E equipment are discussed in Sections 3.10 and 3.11.

REGULATORY GUIDE 1.97 (Revision 2)

Revision 2 to Regulatory Guide 1.97 was originally responded to in Chapter 5 of the Duke Power Company Catawba Nuclear Station Response to Supplement 1, NUREG 0737. This response has since been updated and included in Section 1.8.1 and Table 1-11.

REGULATORY GUIDE 1.100 (Revision 1)

The seismic qualification of Category I instrumentation and electrical equipment is discussed in Section 3.10.

REGULATORY GUIDE 1.105 (Revision 1)

Conformance to Regulatory Guide 1.105 is discussed in Section 1.7.

REGULATORY GUIDE 1.118 (Revision 2)

The periodic testing requirements for the electric power and protection systems are presented in the Technical Specifications. Additionally, the periodic testing of the Reactor Trip System and Engineered Safety Features Actuation System conforms to the requirements of IEEE 338-1971 with the following comments:

1. The surveillance requirements of the Technical Specifications for the protection system ensure that the system functional operability is maintained comparable to the original design standards. Periodic tests at frequent intervals demonstrate this capability for the system.

   Sensors are demonstrated to be adequate for use in the protection system by vendor testing, in situ testing in operating plants with similar design, or by suitable type testing.

   Periodic verification of the response time of differential pressure transmitters (level), differential pressure transmitters (flow), pressure transmitters, frequency transmitters, and voltage transmitters is demonstrated by one of the following methods:

   a. Test sensor in place by perturbing the process being monitored using existing equipment provided for normal plant operation.

   b. Test sensor in place by perturbing the process input using additional equipment provided for response time testing.

   c. Remove the sensor from service and bench test the device.

   Periodic verification of the time response of resistance temperature detectors (RTDs) is demonstrated by in situ self-heating tests.

   The Nuclear Instrumentation System detectors are excluded from response time testing since they exhibit response time characteristics such that delays attributable to them are negligible in the overall channel response time required for safety.

   The measurement of response time at the specified time intervals provides assurance that the protective and Engineered Safety Features function associated with each channel is completed within the time limit assumed in the accident analyses.

   Westinghouse WCAP-13632-P-A, ‘Elimination of Pressure Sensor Response Time Testing Requirements’ and WCAP-14036-P-A, ‘Elimination of Periodic Protection Channel Response Time Tests’ provide both the technical basis and the methodology for verifying the total channel response time using an allocated time. These documents specify ‘allocated response time’ values for specific sensor and electronic components. This methodology may be used in conjunction with or in lieu of response time measurement testing.

2. The reliability goals specified in paragraph 4.2 of IEEE 338-1971, have been developed, and adequacy of time intervals was demonstrated in WCAP-10271 and its supplements (Reference 5).
3. The periodic test interval times are discussed in paragraph 5.2 of IEEE 338-1971, and specified in the plant Technical Specifications, is conservatively selected to assure that equipment associated with protection functions has not drifted beyond its minimum performance requirements. If any protection channel appears to be marginal or requires more frequent adjustments due to plant condition changes, the time interval will be decreased to accommodate the situation until the marginal performance is resolved.
4. The test interval discussed in paragraph 5.2 of IEEE 338-1971, is developed primarily on past operating experience and modified if necessary to assure that system and subsystem protection is reliably provided. Analytic methods for determining reliability are not used to determine test interval.

Based on the scope definition given in IEEE 338-1971, no other systems described in Chapter 7 are required to comply with this standard.

7.1.2.4.3 NRC IE Bulletin 90-01 and Supplement 1

The NRC issued IE Bulletin 90-01, "Loss of Fill-Oil in Transmitters Manufactured by Rosemount," on March 9, 1990. IE Bulletin 90-01 requested that licensees promptly identify and take appropriate corrective actions for Model 1153 Series B, Model 1153 Series D, and Model 1154 transmitters manufactured by Rosemount that may be leaking fill-oil. Duke Power Company's Bulletin response actions included identification of transmitters from the suspect lots for Catawba Nuclear Station which were in use in safety-related applications, review of applicable calibration records to inspect transmitters for loss of fill-oil behavior, and development of an enhanced surveillance program to monitor applicable transmitters for symptoms of loss of fill-oil. Additionally, the IE Bulletin 90-01 requested that upon identification of any suspect Rosemount transmitters in use in reactor protection or engineered safety features actuation systems, operability determinations be performed for this equipment until the equipment could be replaced. In its response (letter from H.B. Tucker to NRC, dated August 10, 1990) DPC found no suspect transmitters installed in the reactor protection or engineering safety features actuation systems of Catawba Nuclear Station. However, two suspect lot transmitters were identified to be installed in safety related applications on Unit 2 (transmitters CN2KCFT5540 and CN2KCFT5541). Corrective actions and other response requirements of IE Bulletin 90-01 were submitted to the NRC in the above referenced letter.

The NRC issued Supplement 1 to IE Bulletin 90-01, "Loss of Fill-Oil in Transmitters Manufactured by Rosemount," on December 22, 1992, providing further details on monitoring programs for the transmitters described in the original bulletin. Duke Power Company responded on May 24, 1993 by the letter from H.B. Tucker to the NRC. Subsequently, the NRC issued its Safety Evaluation Report (SER) on January 27, 1995 which provided approval and closeout of IE Bulletin 90-01 and Supplement 1.

7.1.2.4.4 Industry Standards

IEEE 279-1971

Conformance to IEEE 279-1971 is discussed in Sections 7.1, 7.2, 7.3, 7.4, 7.6, 7.7 of this chapter.

7.1.3 References

1. Gangloff, W. C. and Loftus, W. D., "An Evaluation of Solid State Logic Reactor Protection in Anticipated Transients," *WCAP-7706-L*, February, 1971 (Proprietary) and *WCAP-7706*, July, 1971. (Non-Proprietary).
2. Katz, D. N., "Solid State Logic Protection System Description," *WCAP-7488-L*, January, 1971 (Proprietary) and *WCAP-7672*, June, 1971 (Non-Proprietary).
3. The Institute of Electrical and Electronics Engineers, Inc., "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations," IEEE Standard 279-1971.
4. Siroky, R. M. and Marasco, F. W., "Westinghouse 7300 Series Process Control System Noise Tests," *WCAP-8892-A*, June 1977 (Non-Proprietary).
5. Jansen, R. L., et al., "Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrumentation System," *WCAP-10271*, January 1983 (Proprietary), Supplement 1, July 1983, Supplement 2, February 1986 (rev.0) & March 1987 (rev. 1).
6. Nuclear Regulatory Commission, Letter to All Holders of Operating Licenses or Construction Permits for Nuclear Power Reactors, from Charles E. Rossi, March 9, 1990, NRC Bulletin No. 90-01, "Loss of Fill-Oil in Transmitters Manufactured by Rosemount."
7. Duke Power Company, Letter from H.B. Tucker to NRC, August 10, 1990, re: Response to NRC Bulletin No. 90-01, "Loss of Fill-Oil in Transmitters Manufactured by Rosemount."
8. Duke Power Company, Letter from H.B. Tucker to NRC, May 24, 1993, re: Response to NRC Bulletin No. 90-01, Supplement 1, "Loss of Fill-Oil in Transmitters Manufactured by Rosemount."
9. Nuclear Regulatory Commission, Letter from R.E. Martin to M.S. Tuckman (DPC), January 27, 1995, "Response to NRC Bulletin 90-01, Supplement 1, "Loss of Fill-Oil in Transmitters Manufactured by Rosemount" - Catawba Nuclear Station, Units 1 and 2 (TAC Nos. M85371 and M85372)."
10. T.W.T. Burnett, “Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors”, WCAP-7306, April, 1969.
11. Technical Specification Task Force (TSTF), TSTF-493, Rev. 4, "Clarify Application of Setpoint Mechodology for LSSS Functions" July 13, 2009.
12. Deleted per 2015 update
13. Deleted per 2015 update
14. Deleted per 2015 update
15. Deleted per 2015 update
16. Deleted per 2015 update
17. Deleted per 2015 update
18. Deleted per 2015 update
19. Deleted per 2015 update
20. Deleted per 2015 update
21. WCAP-17867-P-A, Revision 1, “Westinghouse SSPS Board Replacement Licensing Summary Report”

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.1.

7.2 Reactor Trip System

7.2.1 Description

7.2.1.1 System Description

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

The following systems make up the Reactor Trip System (see References 1, 2, and 3 for additional background information.)

1. Process Instrumentation and Control System.
2. Nuclear Instrumentation System.
3. Solid State Logic Protection System.
4. Reactor Trip Switchgear.
5. Manual Actuation Circuit.

The Reactor Trip System consists of sensors and analog circuitry, consisting of two to four redundant channels, which monitors various plant parameters; and digital circuitry, consisting of two redundant logic trains, which receives inputs from the analog protection channels to complete the logic necessary to automatically open the reactor trip breakers.

Each of the two logic trains, A and B, is capable of opening a separate and independent reactor trip breaker, RTA and RTB, respectively. The trip breakers in series connect three-phase ac power from the rod drive motor-generator sets to the rod drive power cabinets, as shown on Figure 7-2, page 3. During plant power operation, a dc undervoltage coil on each reactor trip breaker holds a trip plunger out against its spring, allowing the power to be available at the rod control power supply cabinets. For reactor trip, a loss of dc voltage to the undervoltage coil releases the trip plunger and trips open the breaker. Additionally the shunt trip coil is energized to independently trip open the breaker. When either of the trip breakers opens, power is interrupted to the rod drive power supply, and the control rods fall, by gravity, into the core. The rods cannot be withdrawn until the trip breakers are manually reset.

The trip breakers cannot be reset until the abnormal condition which initiated the trip is corrected. Bypass breakers BYA and BYB are provided to permit testing of the trip breakers, as discussed in Section 7.2.2.2.3.

7.2.1.1.1 Functional Performance Requirements

The Reactor Trip System automatically initiates reactor trip:

1. Whenever necessary to prevent fuel damage for an anticipated operational transient (Condition II),
2. To limit core damage for infrequent faults (Condition III),
3. So that the energy generated in the core is compatible with the design provisions to protect the reactor coolant pressure boundary for limiting fault conditions (Condition IV).

The Reactor Trip System initiates a turbine trip signal whenever reactor trip is initiated to prevent the reactivity insertion that would otherwise result from excessive reactor system cooldown and to avoid unnecessary actuation of the Engineered Safety Features Actuation System.

The Reactor Trip System provides for manual initiation of reactor trip by operator action.

7.2.1.1.2 Reactor Trips

The various reactor trip circuits automatically open the reactor trip breakers whenever a condition monitored by the Reactor Trip System reaches a preset level. To ensure a reliable system, high quality design, components, manufacturing, quality control, and testing are used. In addition to redundant channels and trains, the design approach provides a Reactor Trip System which monitors numerous system variables, therefore providing protection system functional diversity. The extent of this diversity has been evaluated for a wide variety of postulated accidents.

Table 7-1 provides a list of reactor trips which are described below.

1. Nuclear Overpower Trips

   The specific trip functions generated are as follows:

   a. Power range high neutron flux trip.

      The power range high neutron flux trip circuit trips the reactor when two of the four power range channels exceed the trip setpoint.

      There are two bistables, each with its own trip setting used for a high and low range trip setting. The high trip setting provides protection during normal power operation and is always active. The low trip setting, which provides protection during startup, can be manually bypassed when two out of the four power range channels read above approximately 10 percent power (P-10). Three out of the four channels below 10 percent automatically reinstates the low trip function. Refer to Table 7-2 for a listing of all protection system interlocks.

   b. Intermediate range high neutron flux trip

      The intermediate range high neutron flux trip circuit trips the reactor when one out of the two intermediate range channels exceed the trip setpoint. This trip, which provides protection during reactor startup, can be manually blocked if two out of four power range channels are above approximately 10 percent power (P-10). Three out of the four power range channels below this value automatically reinstates the intermediate range high neutron flux trip. The intermediate range channels can be individually bypassed at the nuclear instrumentation racks to permit channel testing during plant shutdown or prior to startup. This bypass action is annunciated on the control board.

   c. Source range high neutron flux trip.

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

d. Power range high positive neutron flux rate trip.

This circuit trips the reactor when a sudden abnormal increase in nuclear power occurs in two out of four power range channels. This trip is available for rod ejection accidents of low worth from mid-power and is always active.

Figure 7-2, page 4, shows the logic for all of the nuclear overpower and rate trips.

2. Core Thermal Overpower Trips

The specific trip functions generated are as follows:

a. Overtemperature ΔT trip

This trip protects the core against low DNBR and trips the reactor on coincidence as listed in Table 7-1 with one set of temperature measurements per loop. The setpoint for this trip is continuously calculated by analog circuitry for each loop by solving the overtemperature ΔT trip equation shown in Table 3.3.1-1, Note 1, of the Technical Specifications and in the Core Operating Limits Report (COLR). (The detailed terms and time constant values are given in Table 3.3.1-1 of the Technical Specifications and COLR.):

A separate long ion chamber unit supplies the flux signal for each overtemperature ΔT trip channel.

Increases in $\Delta\phi$ beyond a pre-defined deadband result in a decrease in trip setpoint. Refer to Figure 7-3.

The required one pressurizer pressure parameter per loop is obtained from separate sensors connected to three pressure taps at the top of the pressurizer. Four pressurizer pressure signals are obtained from the three taps by connecting one of the taps to two pressure transmitters. Refer to Section 7.2.2.3.3 for an analysis of this arrangement.

Figure 7-2, page 6, shows the logic for overtemperature ΔT trip function.

b. Overpower ΔT trip

This trip protects against excessive power (fuel rod rating protection) and trips the reactor on coincidence as listed in Table 7-1, with one set of temperature measurements per loop. The setpoint for each channel is continuously calculated using the overpower ΔT trip equation shown in Table 3.3.1-1, Note 2, of the Technical Specifications and in

the Core Operating Limits Report (COLR). (The detailed terms and time constant values are given in Table 3.3.1-1 of the Technical Specifications and COLR):

The source of temperature and flux information is identical to that of the overtemperature ΔT trip and the resultant ΔT setpoint is compared to the same ΔT. Figure 7-2, page 6, shows the logic for this trip function.

3. Reactor Coolant System Pressurizer Pressure and Water Level Trips

   The specific trip functions generated are as follows:

   a. Pressurizer low pressure trip

      The purpose of this trip is to protect against low pressure which could lead to DNB. The parameter being sensed is reactor coolant pressure as measured in the pressurizer. Above P-7 the reactor is tripped when two-out-of-four pressurizer pressure measurements (compensated for rate of change) fall below preset limits. This trip is blocked below P-7 to permit startup. The trip logic and interlocks are given in Table 7-1.

      The trip logic is shown on Figure 7-2, page 7.

   b. Pressurizer high pressure trip

      The purpose of this trip is to protect the Reactor Coolant System against system overpressure.

      The same sensors and transmitters used for the pressurizer low pressure trip are used for the high pressure trip except that separate bistables are used for trip. These bistables trip when two-out-of-four uncompensated pressurizer pressure signals exceed preset limits. The trip logic and interlocks are given in Table 7-1. There are no interlocks or permissives associated with this trip function.

      The logic for this trip is shown on Figure 7-2, page 7.

   c. Pressurizer high water level trip

      This trip is provided as a backup to the high pressurizer pressure trip and serves to prevent water relief through the pressurizer safety valves. This trip is blocked below P-7 to permit startup. The coincidence logic and interlocks of two-out-of-three pressurizer high water level signals are given in Table 7-1.

      The trip logic for this function is shown on Figure 7-2, page 7.

4. Reactor Coolant System Low Flow Trips

   These trips protect the core from DNB in the event of a loss of coolant flow situation. Figure 7-2, page 6 shows the logic for these trips. The means of sensing the loss of coolant flow are as follows:

   a. Low reactor coolant flow

      The parameter sensed is reactor coolant flow. One elbow in each of four coolant loops is used as a flow device that indicates the status of reactor coolant flow. Each elbow is monitored thru separate taps by 3 instrument channels. The basic function of this loop is to provide information as to whether or not a reduction in flow has occurred. An output signal from two out of the three bistables in a loop would indicate a low flow in that loop.

      The coincidence logic and interlocks are given in Table 7-1.

   b. Reactor coolant pump undervoltage trip

This trip is required in order to protect against low flow which can result from loss of voltage to more than one reactor coolant pump motor (e.g., from plant blackout or reactor coolant pump breakers opening).

An undervoltage monitor is provided which senses voltage to the pump motor at the motor side of each reactor coolant pump breaker.

These monitors provide an output signal when the pump voltage goes below approximately 77 percent of rated voltage. Signals from these monitors are time delayed to prevent spurious trips caused by short term voltage perturbations. The coincidence logic and interlocks are given in Table 7-1.

c. Reactor coolant pump underfrequency trip

This trip protects against low flow resulting from pump underfrequency, for example a major power grid frequency disturbance. The function of this trip is to trip the reactor when the system frequency drops below approximately 56Hz. The setpoint of the underfrequency monitor is adjustable between 54 and 59 Hz.

One underfrequency sensing monitor is provided for each reactor coolant pump motor. Signals from the monitor for any two of the pump motors (time delayed approximately 0.2 second to prevent spurious trips caused by short term frequency perturbations) will trip the RCP breakers and will trip the reactor if the power level is above P-7.

Undervoltage monitors, underfrequency monitors, associated auxiliary relays, and isolation devices for the four channels are housed in a special panel. The panel is divided into four separate compartments to maintain channel independence. Potential transformers from which the input signals for the undervoltage and underfrequency monitors are derived and the panel are classified as Class 1E and are located in a Seismic Category I structure.

5. Steam Generator Trip

The specific trip function generated is as follows:

Low-low steam generator water level trip

This trip protects the reactor from loss of heat sink. The trip is actuated on two out of four low-low water level signals occurring in any steam generator.

The logic for the low-low steam generator water level trip is shown on Figure 7-2, pages 8 and 9.

6. Safety Injection Signal Actuation Trip

A reactor trip occurs when the Safety Injection System is actuated. The means of actuating the Safety Injection System are described in Section 7.3. This trip protects the core against a loss of reactor coolant or steamline break.

Figure 7-2, page 10 shows the logic for this trip.

7. Reactor Trip on Turbine Trip (anticipatory)

The anticipatory reactor trip on turbine trip is actuated by a low pressure signal from two-out-of-four stop valve electro-hydraulic fluid pressure switches, or by valve closed signals from four-out-of-four turbine steam stop valve limit switches. A turbine trip initiates a direct reactor trip only when reactor power is above approx. 70% power. This trip provides conservatism and protection beyond that required to assure the health and safety of the

public, and is included as good engineering practice and prudent design. No credit is taken for this trip in any of the safety analyses of Section 15.1.

The anticipatory reactor trip on turbine trip at low power levels (below 70% power) is bypassed by the P-9 interlock. A safety evaluation performed in support of implementing the P-9 interlock demonstrates the acceptability of bypassing the reactor trip on turbine trip at power levels below 70% (Reference 6).

Separate cable routing is maintained for the four turbine trip channels. Each of the channels includes a signal from a turbine stop valve limit switch and a signal from a stop valve electro-hydraulic fluid pressure switch. Separation of the four channels is maintained from the sensors to the Reactor Protection System logic input cabinets. The channels are routed to the same redundance and separation criteria as Class 1E circuits; however, mounting and location of these circuits is in a non-seismic category 1 structure.

One of the design bases considered in the protection system is the possibility of an earthquake. With respect to the reactor trip on turbine trip contacts, their functioning is unrelated to a seismic event in that they are anticipatory to other diverse parameters that cause a reactor trip. The contacts are closed during plant operation and open to trip the reactor. No power is provided to the protection system from these contacts; they merely serve to interrupt power to cause a reactor trip.

This system functions in a de-energize-to-trip fashion to cause a trip if power is interrupted in the trip circuit. This design ensures that the protection will in no way be degraded by the anticipatory trip because seismic design considerations are not part of the design bases for the anticipatory trip sensors. (The reactor protection system cabinets that receive the anticipatory trip inputs are seismically qualified as discussed in Section 3.10). Thus, the anticipatory reactor trip on turbine trip meets the requirements of IEEE 279-1971 including redundancy, separation, single failure, etc. Seismic qualification of the sensors is not required.

The logic for this trip is shown on Figure 7-2, pages 24 and 25.

8. Manual Trip

The manual trip consists of two switches, one for train A and one for train B, in the control room. Operating a manual trip switch removes the voltage from the corresponding undervoltage trip coil and energizes the shunt coil while actuating the associated Reactor Trip Breaker.

There are no interlocks that can block this trip. The design conforms to Regulatory Guide 1.62.

7.2.1.1.3 Reactor Trip System Interlocks

1. Power Escalation Permissivies

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

A one out of two intermediate range permissive signal (P-6) is required prior to source range trip blocking. Source range trips are automatically reactivated when both intermediate range channels are below the permissive (P-6) setpoint. There are two manual reset switches for administratively reactivating the source range level trip when between the permissive P-6

and P-10 setpoints, if required. Source range level trip block is always maintained when above the permissive P-10 setpoint.

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

The development of permissives P-6 and P-10 is shown on Figure 7-2, page 5. All of the permissives are digital; they are derived from analog signals in the nuclear power range and intermediate range channels.

See Table 7-2 for the list of protection system interlocks.

2. Blocks of Reactor Trips at Low Power

Interlock P-7 blocks a reactor trip below approximately 10 percent of full power on low reactor coolant flow in more than one loop, reactor coolant pump undervoltage, reactor coolant pump underfrequency, pressurizer low pressure or pressurizer high water level. See Figure 7-2, pages 6, 7, 24 and 25, for permissive applications. The low power signal is derived from three out of four power range neutron flux signals below the setpoint in coincidence with two out of two turbine impulse chamber pressure signals below the setpoint (low plant load). See Figure 7-2, pages 5, 24 and 25, for the derivation of P-7.

The P-8 interlock blocks a reactor trip on low reactor coolant flow in any one loop when the plant is below approximately 50 percent of full power. The block action (absence of the P-8 interlock signal) occurs when three out of four neutron flux power range signals are below the setpoint. Thus, below the P-8 setpoint: the reactor is allowed to operate with one loop inactive and the low flow trip will not occur until two loops indicate low flow. See Figure 7-2, page 5, for the derivation of P-8, and pages 6, 24 and 25 for the applicable logic.

The P-9 interlock blocks a reactor trip following a turbine trip if the power is below approximately 70%. See Figure 7-2, pages 24 and 25, for the functional implementation of the P-9 interlock. See Figure 7-2, page 5 for the functional derivation of P-9. A safety evaluation and acceptability criteria for this bypass are discussed in reference 6.

See Table 7-2 for the list of protection system blocks.

7.2.1.1.4 Reactor Coolant Temperature Sensor Arrangement

The individual hot and cold loop temperature signals required for input to the reactor trip circuits and interlocks are obtained using RTDs installed in each reactor coolant loop.

The hot leg temperature measurement on each loop is accomplished with three fast response narrow range RTDs mounted in thermowells, spatially located 120°F around the hot leg. One fast response narrow range RTD is located in each cold leg at the discharge of the reactor coolant pump (replacements for the cold leg RTDs located in the bypass manifold). Temperature streaming in the cold leg is not a concern due to the mixing action of the RCP, hence, only one cold leg RTD is required. There is also one wide range RTD in each hot leg and each cold leg.

This cold leg temperature measurement, together with the average T_H obtained from the three hot leg temperatures, is used to calculate reactor coolant loop delta-T and T-avg. A penetration

exists to accept an additional well mounted narrow range cold leg RTD for use as an installed spare.

In the event of a single hot leg RTD failure, the channel can be returned to service once the channel has been rescaled to utilize the average of the two remaining hot leg RTDs and the application of the appropriate bias based on recent historical data. The resultant two-RTD Thot Average shall be comparable to the three-RTD average prior to the failure of the one RTD.

7.2.1.1.5 Pressurizer Water Level Reference Leg Arrangement

The design of the pressurizer water level instrumentation employs the usual tank level arrangement using differential pressure between an upper and a lower tap on a column of water. A reference leg connected to the upper tap is kept full of water by condensation of steam at the top of the leg.

7.2.1.1.6 Analog System

The analog system consists of two instrumentation systems; the Process Instrumentation System and the Nuclear Instrumentation System.

Process Instrumentation includes those devices (and their interconnection into systems) which measure temperature, pressure, fluid flow, fluid level as in tanks or vessels, and occasionally physiochemical parameters such as fluid conductivity or chemical concentration. "Process" instrumentation specifically excludes nuclear and radiation measurements. The process instrumentation includes the process measuring devices, power supplies, indicators, recorders, alarm actuating devices, controllers, signal conditioning devices, etc., which are necessary for day-to-day operation of the Nuclear Steam Supply System as well as for monitoring the plant and providing initiation of protective functions upon approach to unsafe plant conditions.

The primary function of nuclear instrumentation is to protect the reactor by monitoring the neutron flux and generating appropriate trips and alarms for various phases of reactor operating and shutdown conditions. It also provides a secondary control function and indicates reactor status during startup and power operation. The Nuclear Instrumentation System uses information from three separate types of instrumentation channels to provide three discrete protection levels. Each range of instrumentation (source, intermediate, and power) provides the necessary overpower reactor trip protection required during operation in that range. The overlap of instrument ranges provides reliable continuous protection beginning with source level through the intermediate and low power level. As the reactor power increases, the overpower protection level is increased by administrative procedures after satisfactory high range instrumentation operation is obtained. Automatic reset to more restrictive trip protection is provided when reducing power.

Various types of neutron detectors, with appropriate solid-state electronic circuitry, are used to monitor the leakage neutron flux from a completely shutdown condition to 200 percent of full power. The power range channels are capable of recording overpower excursions up to 200 percent of full power. The neutron flux covers a wide range between these extremes. Therefore, monitoring with several ranges of instrumentation is necessary.

The lowest range (source range) covers seven decades of leakage neutron flux. The lowest observed count rate, (generally greater than two counts per second) depends upon the strength of the neutron sources in the core and the core multiplication associated with the shutdown reactivity. When the count rate is below the established minimum value, administrative procedures as described in Section 14.1 prevent reactor startup. The next range (intermediate range) covers ten decades. Detectors and instrumentation are chosen to provide overlap

between the higher portion of the source range and the lower portion of the intermediate range. The highest range of instrumentation (power range) covers approximately two decades of the total instrumentation range. This is a linear range that overlaps with the higher portion of the intermediate range.

The system described above provides control room indication and recording of signals proportional to reactor neutron flux during core loading, shutdown, startup, and power operation, as well as during subsequent refueling. Start-up-rate indication for the source and intermediate range channels is provided at the control board. Reactor trip, rod stop, control, and alarm signals are transmitted to the Reactor Control and Protection System for automatic plant control. Equipment failures and test status information are annunciated in the control room.

See References 1 and 2 for additional background information on the process and nuclear instrumentation.

7.2.1.1.7 Solid State Logic Protection System

The Solid State Logic Protection System (also referred to as the Solid State Protection System, SSPS) takes binary inputs (voltage/no voltage) from the process and nuclear instrument channels corresponding to conditions (normal/ abnormal) of plant parameters. The system combines these signals in the required logic combination and generates a trip signal (no voltage) to the under-voltage coils of the reactor trip circuit breakers when the necessary combination of signals occur. The system also provides annunciator, status light, and plant computer sequence of events input signals which indicate the condition of bistable input signals, partial trip and full trip functions, and the status of the various blocking, permissive and actuation functions. In addition the system includes means for semi-automatic testing of the logic circuits. See Reference 3 for additional background information.

The WCAP listed in Reference 3 details the design and operation of the SSPS. Included in this description is the use of Motorola High Threshold Logic (MHTL) chips in the design of the SSP boards. WCAP 17867-P-A (Reference 16) has been approved by the NRC to allow use of a replacement design for the originally installed SSPS boards that no longer utilizes the MHTL chip. See Reference 16 for additional information.

7.2.1.1.8 Isolation Amplifiers

In certain applications, Westinghouse considers it advantageous to employ control signals derived from individual protection channels through isolation amplifiers contained in the protection channel, as permitted by IEEE 279-1971.

In all of these cases, analog signals derived from protection channels for non-protective functions are obtained through isolation amplifiers located in the analog protection racks. By definition, non-protective functions include those signals used for control, remote process indication, and computer monitoring. Refer to Section 7.1.2.2 for discussion of electrical separation of control and protection functions.

7.2.1.1.9 Energy Supply and Environmental Variations

The energy supply for the Reactor Trip System is described in Section 7.6 and Chapter 8. The environmental variations, throughout which the system will perform, are given in Section 3.11.

7.2.1.1.10 Setpoints

The setpoints that require trip action are given in the Technical Specifications. A detailed discussion on setpoints is found in Section 7.1.2.1.7.

7.2.1.1.11 Seismic Design

The seismic design considerations for the Reactor Trip System are given in Section 3.10 This design meets the requirements of Criterion 2 of the 1971 General Design Criteria (GDC).

7.2.1.2 Design Bases Information

The information given above presents the design bases information requested by Section 3 of IEEE 279-1971. Functional logic diagrams are presented in Figure 7-2.

7.2.1.2.1 Generating Station Conditions

The following are the generating station conditions requiring reactor trip.

1. DNBR approaching limiting value.
2. Power density (kilowatts per foot) approaching rated value for Condition II faults (See Chapter 4 for fuel design limits).
3. Reactor Coolant System overpressure creating stresses approaching the limits specified in Chapter 5.

7.2.1.2.2 Generating Station Variables

The following are the variables required to be monitored in order to provide reactor trips (see Table 7-1).

1. Neutron flux
2. Reactor coolant temperature
3. Reactor Coolant System pressure (pressurizer pressure)
4. Pressurizer water level
5. Reactor coolant flow
6. Reactor coolant pump operational status (voltage and frequency)
7. Steam generator water level
8. Turbine-generator operational status (control valve EH pressure and stop valve position)

7.2.1.2.3 Spatially Dependent Variables

The following variable is spatially dependent:

Reactor coolant temperature: See Section 7.3.1.2.3 for a discussion of this variable spatial dependence.

7.2.1.2.4 Limits, Margins, and Set Points

The setpoints for reactor trip required for Catawba are given in Section 2 of the Technical Specifications for each unit. The values for reactor trip assumed in the analyses of design basis

accidents are given in Chapter 15. These accident analyses demonstrate that the setpoints for reactor trip are conservative.

The setpoints for the various functions in the Reactor Trip System have been analytically determined such that the operational limits so prescribed will prevent fuel rod clad damage and loss of integrity of the Reactor Coolant System. As a result of any ANS Condition II incident, the Reactor Trip System limits the following parameters to:

1. Minimum DNBR = limiting value
2. Maximum system pressure = 2750 psia
3. Fuel rod maximum linear power for determination of protection setpoints = limiting value (See Section 4.2.4.1).

The accident analyses described in Section 15.2 demonstrate that the functional requirements as specified for the Reactor Trip System are adequate to meet the above considerations, even assuming, for conservatism, adverse combinations of instrument errors (Refer to Table 15-20). The safety limits associated with the reactor core and Reactor Coolant System, plus the limiting safety system setpoints, are presented in the Technical Specifications.

7.2.1.2.5 Abnormal Events

The malfunctions, accidents, or other unusual events which could physically damage Reactor Trip System components or could cause environmental changes are as follows:

1. Earthquakes (See Chapter 2 and Chapter 3)
2. Fire (See Section 9.5)
3. Explosion (hydrogen buildup inside containment).
4. (See Section 6.2)
5. Missiles (See Section 3.5)
6. Flood (See Chapter 2 and Chapter 3)
7. Wind and Tornadoes (See Section 3.3)

The Reactor Trip System fulfills the requirements of IEEE 279-1971 to provide automatic protection and to provide initiating signals to mitigate the consequences of faulted conditions. The Reactor Trip System relies upon provisions made by the owner and operator of the plant to provide protection against destruction of the system from fires, explosions, missiles, floods, wind, and tornadoes (see each item above).

7.2.1.2.6 Minimum Performance Requirements

1. Reactor Trip System response times

   Reactor Trip System response time is defined in Section 7.1. Maximum allowable time delays in generating the reactor trip signal are tabulated in Table 7-3. (See Section 7.1.2.4.2 for a discussion of periodic response time verification capabilities.)

2. Reactor trip accuracies

   Accuracy is defined in Section 7.1. Typical reactor trip accuracies are tabulated in Table 7-3. An additional discussion on accuracy is found in Section 7.1.2.1.7.

3. Protection System ranges

Typical Protection System ranges are tabulated in Table 7-3. Range selection for the instrumentation covers the expected range of the process variable being monitored during power operation. Limiting setpoints are at least 5% from the end of the instrument span.

7.2.1.3 Final Systems Drawings

Functional block diagrams, electrical elementaries, and other drawings required to perform a safety review are provided in the Catawba Schematics Books (see Section 1.7).

7.2.2 Analyses

7.2.2.1 Failure Mode and Effects Analyses

An analysis of the Reactor Trip System has been performed, and the results of this study, along with a fault tree analysis, are presented in Reference 4.

In addition to these analyses, the failure mode and effects analysis (FMEA) performed for the Engineered Safety Features Actuation System (ESFAS) also applies to the RTS because the processing of analog signals and the digital logic functions performed in the SSPS for actuating safeguards are also used for actuation of the reactor trip. This analysis is presented in Reference 5. The results of the above analyses confirm that the Reactor Trip System meets the single failure criteria of IEEE 279-1971.

WCAP 17867-P-A (Reference 16) has been approved by the NRC to allow use of a replacement design for the originally installed SSPS circuit cards. The board redesign was accomplished in a manner which retained the original operation of the SSPS boards. The system continues to operate as originally designed. See reference 16 for additional information regarding FMEA for the replacement design circuit cards.

7.2.2.2 Evaluation of Design Limits

While most setpoints used in the Reactor Protection System are fixed, there are variable setpoints, most notably the overtemperature ΔT and overpower ΔT setpoints. All setpoints in the Reactor Trip System have been selected on the basis of engineering design or safety studies. The capability of the Reactor Trip System to prevent loss of integrity of the fuel cladding and/or Reactor Coolant System pressure boundary during Condition II and III transients is demonstrated in Section 15.1. These accident analyses are carried out using those setpoints determined from results of the engineering design studies. Setpoint limits are presented in the Technical Specifications. A discussion of the intent for each of the various reactor trips and the accident analyses (where appropriate) which utilizes this trip is presented below. It should be noted that the selected trip setpoints all provide for margin before protection action is actually required to allow for uncertainties and instrument errors. The design meets the requirements of Criteria 10 and 20 of the 1971 GDC.

7.2.2.2.1 Trip Setpoint Discussion

It has been pointed out previously that below the limiting DNBR value specified in Section 4.4.2.1 there may be local fuel cladding failure. The DNBR existing at any point in the core for a given core design can be determined as a function of the core inlet temperature, power output, operating pressure and flow. Consequently, core safety limits in terms of a DNBR equal to limiting value specified in Section 4.4.2.1 for the hot channel can be developed as a function of core ΔT, Tavg, and pressure for a specified flow as illustrated by the solid lines in Figure 15-1. Also shown as solid lines in Figure 15-1 are the loci of conditions equivalent to 118 percent of

power as a function of ΔT and Tavg representing the overpower (KW/ft) limit on the fuel. The dashed lines indicate the maximum permissible setpoint (ΔT) as a function of Tavg and pressure for the overtemperature and overpower reactor trip. Actual setpoint constants in the equation representing the dashed lines are as given in the Technical Specifications. These values are conservative to allow for instrument errors. The design meets the requirements of Criteria 10, 15, 20 and 29 of the 1971 GDC.

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

Therefore, the Reactor Trip System has been designed to provide protection for fuel cladding and Reactor Coolant System pressure boundary integrity where: 1) a rapid change in a single variable or factor which will quickly result in exceeding a core or a system safety limit, and 2) a slow change in one or more variables will have an integrated effect which will cause safety limits to be exceeded. Overall, the Reactor Trip System offers diverse and comprehensive protection against fuel cladding failure and/or loss of Reactor Coolant System integrity for Condition II and III accidents. This is demonstrated by Table 7-4 which lists the various trips of the Reactor Trip System, the corresponding Technical Specifications on safety limits and safety analyses settings, and the appropriate accident discussed in the safety analyses in which the trip could be utilized.

It should be noted that the Reactor Trip System automatically provides core protection during non-standard operating configuration, i.e. operation with a loop out of service. Although operating with a loop out of service over an extended time is considered to be an unlikely event, no protection system setpoints need to be reset. This is because the nominal value of the power (P-8) interlock setpoint restricts the power such that DNB ratios less than the limiting value specified in Section 4.4.2.1 will not be realized during any Condition II transients occurring in this mode of operation. This restricted power is considerably below the boundary of permissible values as defined by the core safety limits for operation with a loop out of service. Thus the P-8 interlock acts essentially as a high nuclear power reactor trip when operating with one loop not in service. By first resetting the coefficient setpoints in the overtemperature ΔT function to more restrictive values as listed in the technical specifications, the P-8 setpoint can then be increased to the maximum value consistent with maintaining DNBR above the limiting value specified in Section 4.4.2.1 for Condition II transients in the one loop shutdown mode. The resetting of the ΔT overtemperature trip and P-8 will be carried out under prescribed administrative procedures, under the direction of authorized supervision, and with the plant conditions prescribed in Section 3.4.1.1 of the Technical Specifications.

The design meets the requirements of Criterion 21 of the 1971 GDC.

Preoperational testing is performed on Reactor Trip System components and systems to determine equipment readiness for startup. This testing serves as a further evaluation of the system design.

Analyses of the results of Condition I, II, III and IV events, including considerations of instrumentation installed to mitigate their consequences are presented in Section 15.1. The instrumentation installed to mitigate the consequences of load rejection and turbine trip is given in Section 7.4.

7.2.2.2.2 Reactor Coolant Flow Measurement

The elbows used to measure flow in each loop in the primary coolant system are instrument devices that indicate the status of the reactor coolant flow. The basic function of this device is to provide information as to whether or not a reduction in flow has occurred. The correlation between flow and differential pressure developed across the elbow is given by the following equation: $W = K\sqrt{\Delta \frac{P}{P}}$

where K is a constant (see Section 4.4.6.5.1 and Table 4-22 for flow coefficients for elbow differential pressure taps), ρ is the water density, and ΔP is the pressure differential at the corresponding flow, W. Plant data taken during early fuel cycles was used to determine the value of K. The expected absolute accuracy of the channel is within ± 10 percent of full flow and field results have shown the repeatability of the trip point to be within ± 1 percent.

7.2.2.2.3 Evaluation of Compliance to Applicable Codes and Standards

The Reactor Trip System meets the criteria of the General Design Criteria as indicated. The Reactor Trip System meets the requirements of Section 4 of IEEE 279-1971, as indicated below.

1. General Functional Requirement

   The Protection System automatically initiates appropriate protective action whenever a condition monitored by the system reaches a preset level.

   Functional performance requirements are given in Section 7.2.1.1.1. Section 7.2.1.2.4 presents a discussion of limits, margins, and levels; Section 7.2.1.2.5 discusses unusual (abnormal) events; and Section 7.2.1.2.6 presents minimum performance requirements.

2. Single Failure Criterion

   The Protection System is designed to provide two, three, or four instrumentation channels for each protective function and two logic train circuits. These redundant channels and trains are electrically isolated and physically separated. Thus, any single failure within a channel or train will not prevent protective action at the system level when required. Loss of input power (the most likely mode of failure) to a channel or logic train will result in a signal calling for a trip. This design meets the requirements of Criterion 23 of the 1971 GDC.

   To prevent the occurrence of common mode failures, such additional measures as functional diversity, physical separation, and testing as well as administrative control during design, production, installation, and operation are employed as discussed in Reference 4. The design meets the requirements of Criteria 21 and 22 of the 1971 GDC.

3. Quality of Components and Modules

For a discussion on the quality of the components and modules used in the Reactor Trip System, refer to Chapter 17. The quality assurance applied conforms to Criterion 1 of the 1971 GDC.

4. Equipment Qualification

   For a discussion of the type tests made to verify the performance requirements, refer to Section 3.11. The test results demonstrate that the design meets the requirements of Criterion 4 of the 1971 GDC.

5. Channel Integrity

   Protection System channels required to operate in accident conditions maintain necessary functional capability under extremes of conditions relating to environment, energy supply, malfunctions, and accidents. The energy supply for the Reactor Trip System is described in Chapter 8. The environmental variations, throughout which the system will perform is given in Section 3.11.

6. Independence

   Channel independence is carried throughout the system, extending from the sensor through to the devices actuating the protective function. Physical separation is used to achieve separation of redundant transmitters. Separation of wiring is achieved using separate wireways, cable trays, conduit runs, and containment penetrations for each redundant channel. Redundant analog equipment is separated by locating modules in different protection cabinets. Each redundant protection channel set is energized from a separate AC power feed. This design meets the requirements of Criterion 21 of the 1971 GDC.

   Two reactor trip breakers are actuated by two separate logic matrices which interrupt power to the control rod drive mechanisms. The breaker main contacts are connected in series with the power supply so that opening either breaker interrupts power to all full-length control rod drive mechanisms, permitting the rods to free fall into the core. See Figure 7-1.

   Separate routing is maintained for the four basic Reactor Trip System channel sets analog sensing signals, bistable output signals, and power supplies for such systems. The separation of these four channel sets is maintained from sensors to instrument cabinets to logic system input cabinets.

   Separate routing of the redundant reactor trip signals from the redundant logic system cabinets is maintained, and in addition, the redundant reactor trip signals are separated (by spatial separation or by provisions of barriers or by separate cable trays or wireways) from the four analog channel sets.

   The design philosophy is to make the maximum use of a wide variety of measurements. The Protection System continuously monitors numerous diverse system variables. Generally, two or more diverse protection functions would terminate an accident before intolerable consequences could occur. This design meets the requirements of Criterion 22 of the 1971 GDC.

7. Control and Protection System Interaction

   The Protection System is designed to be independent of the Control System as discussed in 7.2.2.3. In certain applications the control signals and other non-protective functions are derived from individual protective channels through isolation amplifiers. The isolation amplifiers are classified as part of the Protection System and are located in the analog protective racks. Nonprotective functions include those signals used for control, remote process indication, and computer monitoring. The isolation amplifiers are designed such

that a short circuit, open circuit, or the application of credible fault voltages from within the cabinets on the isolated output portion of the circuit (i.e., the non-protective side of the circuit) will not affect the input (protective) side of the circuit. The signals obtained through the isolation amplifiers are never returned to the protective racks. This design meets the requirements of Criterion 24 of the 1971 GDC and paragraph 4.7 of IEEE 279-1971.

The results of applying various malfunction conditions on the output portion of the isolation amplifiers show that no significant disturbances to the isolation amplifier input signal occurred. (Refer to Section 7.1.2.2.)

8. Derivation of System Inputs

   To the extent feasible and practical, Protection System inputs are derived from signals which are direct measures of the desired variables. Variables monitored for the various reactor trips are listed in Section 7.2.1.2.2.

9. Capability for Sensor Checks

   The operational availability of each system input sensor during reactor operation is accomplished by cross checking between channels that bear a known relationship to each other and that have read-outs available. Channel checks are discussed in Technical Specification 3.3.1 and Table 3.3.1-1 of the Technical Specifications.

10. Capability for Testing

    The Reactor Trip System is capable of being tested during power operation. Where only parts of the system are tested at any one time, the testing sequence provides the necessary overlap between the parts to assure complete system operation. The testing capabilities are in conformance with Regulatory Guide 1.22 as discussed in Section 7.1.2.4.2.

    The Protection System is designed to permit periodic testing of the analog channel portion of the Reactor Trip System during reactor power operation without initiating a protective action unless a trip condition actually exists. This is because of the coincidence logic required for reactor trip. These tests may be performed at any plant power from cold shutdown to full power. Before starting any of these tests with the plant at power, all redundant reactor trip channels associated with the function to be tested must be in the normal (untripped) mode in order to avoid spurious trips. Setpoints are referenced in the precautions, limitations, and setpoints portions of the plant technical manual.

    Analog Channel Tests

    Analog channel testing is performed at the analog instrumentation rack set by individually introducing dummy input signals into the instrumentation channels and observing the tripping of the appropriate output bistables. Process analog output to the logic circuitry is interrupted during individual channel tests by a test switch which, when thrown, de-energizes the associated logic input and inserts a proving lamp in the bistable output. Interruption of the bistable output to the logic circuitry for any cause (test, maintenance purposes, or removal from service) will cause that portion of the logic to be actuated (partial trip) accompanied by a partial trip alarm and channel status light actuation in the control room. Each channel contains those switches, test points, etc. necessary to test the channel. See References 1 and 2 for additional background information.

    The following periodic tests of the analog channels of the protection circuits are performed:

    a. Tavg and ΔT protection channel testing

    b. Pressurizer pressure protection channel testing

c. Pressurizer water level protection channel testing

d. Steam generator water level protection channel testing

e. Reactor coolant low flow, underfrequency, and undervoltage protection channels testing

f. Impulse chamber pressure channel testing

g. Steam pressure protection channels testing

h. Containment pressure testing

Nuclear Instrumentation Channel Tests

The power range channels of the Nuclear Instrumentation System are tested by superimposing a test signal on the actual detector signal being received by the channel at the time of testing. The output of the bistable is not placed in a tripped condition prior to testing. Also, since the power range channel logic is two out of four, bypass of this reactor trip function is not required.

To test a power range channel, a "TEST-OPERATE" switch is provided to require deliberate operator action and operation of which will initiate the "CHANNEL TEST" annunciator in the control room. Bistable operation is tested by increasing the test signal to its trip setpoint and verifying bistable relay operation by control board annunciator and trip status lights. The positive and negative rate trip bistables are tested using the same procedure.

It should be noted that a valid trip signal would cause the channel under test to trip at a lower actual reactor power level. A reactor trip would occur when a second bistable trips. No provision has been made in the channel test circuit for reducing the channel signal level below that signal being received from the Nuclear Instrumentation System detector.

A Nuclear Instrumentation System channel which can cause a reactor trip through one of the two protection logic (source or intermediate range) is provided with a bypass function which prevents the initiation of a reactor trip from that particular channel during the short period that it is undergoing test. These bypasses are annunciated in the control room.

The following periodic tests of the Nuclear Instrumentation System are performed:

a. Testing at plant shutdown
    1) Source range testing
    2) Intermediate range testing
    3) Power range testing

b. Testing between P-6 and P-10 permissive power levels
    1) Source range testing
    2) Power range testing

c. Testing above P-10 permissive power level
    1) Power range testing

Any deviations noted during the performance of these tests are investigated and corrected in accordance with the established calibration and trouble shooting procedures provided in the plant technical manual for the Nuclear Instrumentation System. Control and protection trip settings are indicated in the plant technical manual under precautions, limitations and setpoints.

For additional background information on the Nuclear Instrumentation System see Reference 2.

Solid State Logic Testing

The reactor logic trains of the Reactor Trip System are designed to be capable of complete testing at power. After the individual channel analog testing is complete, the logic matrices are tested from the train A and train B logic rack test. This step provides overlap between the analog and logic portions of the test program. During this test, all of the logic inputs are actuated automatically in all combinations of trip and non-trip logic. For those tests where the automatic test does not test all aspects of the logic then manual inputs are utilized to ensure all apsects of the logic are tested (see "Check of Logic Matrices" section). Trip logic is not maintained sufficiently long enough to permit opening of the reactor trip breakers. The reactor trip undervoltage coils are "pulsed" in order to check continuity. During logic testing of one train, the other train can initiate any required protective functions. Annunciation is provided in the control room to indicate when a train is in test (train output bypassed) and when a reactor trip breaker is bypassed. Logic testing can be performed in less than 30 minutes.

A direct reactor trip resulting from undervoltage or underfrequency on the reactor coolant pump buses is provided as discussed in Section 7.2.1 and shown on Figure 7-2, page 6. The use of two-out-of-four logic allows calibration and/or testing of one channel at a time during reactor operation without jeopardizing overall system performance. Key-lock test switches are provided on the Reactor Coolant Pump Monitor Panel to open the potential inputs to the voltage or frequency sensing circuits in order to functionally test each channel.

This design complies with the testing requirements of IEEE 279-1971 and IEEE 338-1971 discussed in Section 7.1.2.4.

The permissive and block interlocks associated with the Reactor Trip System and Engineered Safety Features Actuation System are given on Table 7-1, Table 7-2 and Table 7-7 and designated protection or "P" interlocks. As a part of the protection system, these interlocks are designed to meet the testing requirements of IEEE 279-1971 and 338-1971.

Testing of all protection system interlocks is provided by the logic testing and semi-automatic testing capabilities of the Solid State Protection System. In the Solid State Protection System the undervoltage coils (Reactor Trip) and master relays (Engineered Safeguards Actuation) are pulsed for all combinations of trip or actuation logic with and without the interlock signals. For example, reactor trip on low flow (2 out of 4 loops showing 2 out of 3 low flow) is tested to verify operability of the trip above P-7 and non-trip below P-7. (see Figure 7-2, page 6.) Interlock testing may be performed at power.

Testing of the logic trains of the Reactor Trip System includes a check of the input relays and a logic matrix check. The following sequence is used to test the system:

a. Check of input relays

   During testing of the Process Instrumentation System and Nuclear Instrumentation System channels, each channel bistable is placed in a trip mode causing one input relay in train A and one in train B to de-energize. A contact of each relay is connected to a universal logic printed circuit card. This card performs both the reactor trip and monitoring functions. Each reactor trip input relay contact causes a status lamp and an annunciator on the control board to operate. Either the train A or train B input relay operation will light the status lamp and annunciator.

Each train contains a multiplexing test switch. At the start of a process or nuclear instrumentation system test, this switch (in either train) is placed in the A + B position. The A + B position alternately allows information to be transmitted from the two trains to the control board. A steady status lamp and annunciator indicates input relays in both trains have been de-energized. A flashing lamp means that the input relays in the two trains did not both de-energize. Contact inputs to the logic protection system such as reactor coolant pump bus underfrequency relays operate input relays which are tested by operating the remote contacts as described above and using the same type of indications as those provided for bistable input relays.

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

b. Check of Logic Matrices

Logic matrices are checked one train at a time. Input relays are not operated during this portion of the test. Reactor trips from the train being tested are inhibited with the use of the input error inhibit switch on the semi-automatic test panel in the train. At the completion of the logic matrix tests one input in each channel shall be tripped to check closure of the input error inhibit switch contacts.

The logic test scheme uses pulse techniques to check the coincidence logic. All possible trip and non-trip combinations are checked. Pulses from the tester are applied to the inputs of the universal logic card at the same terminals that connect to the input relay contacts. Thus there is an overlap between the input relay check and the logic matrix check. Pulses are fed back from the reactor trip breaker undervoltage coil to the tester. The pulses are of such short duration that the reactor trip breaker undervoltage coil armature cannot respond mechanically.

Four manual input pushbuttons are also provided on the logic test rack so that a non pulse trip test can be performed. The manual input pushbuttons allow for an individual to choose the trip and non-trip logic to be tested.

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

General Warning Alarm Reactor Trip

Each of the two trains of the solid state protection system is continuously monitored by the general warning alarm reactor trip subsystem. The warning circuits are actuated if undesirable train conditions are set up by improper alignment of testing systems, circuit malfunction or failure, etc. as listed below. A trouble condition in a logic train is indicated in the control room. However, if any one of the conditions exists in train A at the same time any one of the conditions exists in train B, the general warning alarm circuits will automatically trip the reactor.

a. Loss of either of two 48 volt dc or either of two 15 volt dc power supplies.

b. Printed circuit card improperly inserted.

c. Input Error Inhibit switch in the INHIBIT position.

d. Slave relay tester Mode Selector in TEST position.

e. Multiplexing selector switch in INHIBIT position.

f. Bypass breaker of train not being tested racked in and closed.

g. Permissive or Memory test switch not in OFF position.

h. Logic Function test switch not in OFF position.

The testing capability meets the requirements of Criterion 21 of the 1971 GDC.

Testing of Reactor Trip Breakers

Normally, reactor trip breakers 52/RTA and 52/RTB are in service, and bypass breakers 52/BYA and 52/BYB are withdrawn (out of service). In testing the protection logic, pulse techniques are used to avoid tripping the reactor trip breakers thereby eliminating the need to bypass them during this testing. The following procedure describes the method used for testing the trip breakers:

a. With bypass breaker 52/BYA racked to the test position, manually close and trip it to verify its operation.

b. Rack in and close 52/BYA. Manually trip 52/RTA through a protection system logic matrix.

c. Reset 52/RTA.

d. Trip and rack out 52/BYA.

e. Repeat above steps to test trip breaker 52/RTB using bypass breaker 52/BYB.

Auxiliary contacts of the bypass breakers are connected into the alarm system of their respective trains such that if either train is placed in test while the bypass breaker of the other train is closed, both reactor trip breakers and both bypass breakers will automatically trip.

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

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

The complete Reactor Trip System is normally required to be in service. However, to permit online testing of the various protection channels or to permit continued operation in the event of a subsystem instrumentation channel failure, a Technical Specification, 3/4.3, defining the minimum number of operable channels has been formulated. This Technical Specification also defines the required restriction to operation in the event that the channel operability requirements cannot be met.

11. Channel Bypass or Removal from Operation

The Protection System is designed to permit periodic testing of the analog channel portion of the Reactor Trip System during reactor power operation without initiating a protective action unless a trip condition actually exists. This is because of the coincidence logic required for reactor trip.

12. Operating Bypasses

    Where operating requirements necessitate automatic or manual bypass of a protective function, the design is such that the bypass is removed automatically whenever permissive conditions are not met. Devices used to achieve automatic removal of the bypass of a protective function are considered part of the protective system and are designed in accordance with the criteria of this section. Indication is provided in the control room if some part of the system has been administratively bypassed or taken out of service.

13. Indication of Bypasses

    Bypass indication is discussed in Section 7.8.

14. Access to Means for Bypassing

    The design provides for administrative control of access to the means for manually bypassing channels or protective functions.

15. Multiple Setpoints

    The Reactor Trip System is designed such that no resetting of setpoints is required from startup to full power operation.

16. Completion of Protective Action

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

17. Manual Initiation

    Switches are provided on the control board for manual initiation of protective action. Failure in the automatic system does not prevent the manual actuation of the protective functions. Manual actuation relies on the operation of a minimum of equipment.

18. Access

    The design provides for administrative control of access to all setpoint adjustments, module calibration adjustments, and test points.

19. Identification of Protective Actions

    Protective channel identification is discussed in Section 7.1.2.3. Indication is discussed in Item 20 below.

20. Information Read Out

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

    Any reactor trip will actuate an alarm and an annunciator. Such protective actions are indicated and identified down to the channel level.

Alarms and annunciators are also used to alert the operator of deviations from normal operating conditions so that he may take appropriate corrective action to avoid a reactor trip. Actuation of any rod stop or trip of any reactor trip channel will actuate an alarm.

21. System Repair

    The system is designed to facilitate the recognition, location, replacement, and repair of malfunctioning components or modules. Refer to the discussion in Item 10 above.

7.2.2.3 Specific Control and Protection Interactions

7.2.2.3.1 Neutron Flux

Four power range neutron flux channels are provided for overpower protection. An isolated second highest signal is derived from the four channels and used for automatic rod control. If any channel fails in such a way as to produce a low output, that channel is incapable of proper overpower protection but will not cause control rod movement because of the auctioneer. Two out of four overpower trip logic will ensure an overpower trip if needed even with an independent failure in another channel.

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

7.2.2.3.2 Reactor Coolant Temperature

The accuracy of the narrow range resistance temperature detector loop temperature measurements is demonstrated during plant startup tests by comparing temperature measurements from the loop narrow range resistance temperature detectors with one another as well as with the temperature measurements obtained from the wide range resistance temperature detector located in the hot leg and cold leg piping of each loop. The comparisons are done with the Reactor Coolant System in an isothermal condition. The linearity of the ΔT measurements obtained from the hot leg and cold leg loop narrow range resistance temperature detectors as a function of plant power is also checked during plant startup tests. The absolute value of ΔT versus plant power is not important, per se, as far as reactor protection is concerned. Reactor Trip System setpoints are based upon percentages of the indicated ΔT at nominal full power rather than on absolute values of ΔT. This is done to account for loop differences which are inherent. Therefore the percent ΔT scheme is relative, not absolute, and therefore provides better protective action without the expense of accuracy. For this reason, the linearity of the ΔT signals as a function of power is of importance rather than the absolute values of the ΔT. As part of the plant startup tests, the loop narrow range resistance temperature detector signals compared with the core exit thermocouple signals.

Reactor control is based upon signals derived from protection system channels after isolation by isolation amplifiers such that no feedback effect can perturb the protection channels.

Since control is based on the second highest average temperature of the loop, the control rods are always moved based upon this conservative temperature measurement with respect to margins to DNB. Using the second highest temperature prevents control action if a single channel fails high or low.

Channel deviation signals in the control system will give an alarm if any temperature channel deviates significantly from the second highest value. Automatic rod withdrawal blocks and turbine runback (power demand reduction) will also occur if any two of the four overtemperature or overpower ΔT channels indicate an adverse condition.

Section 4.7 of IEEE 279-1971 and GDC 24 requirements concerning Control and Protection Systems Interaction are satisfied, even though control signals are derived from protection sets, because the 2/4 voting coincidence logic of the protection sets is maintained. Where a single random failure can cause a control system action that results in a condition requiring protective action and can also prevent proper action of a protective system channel designed to protect against the condition, the remaining three redundant protection channels are capable of providing the protective action even if degraded by a second random failure.

7.2.2.3.3 Pressurizer Pressure

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

Since the second highest pressure signal is used for control, a single channel failing high or low will not cause an inadvertent control action. Additional redundancy is provided in the low pressurizer pressure reactor trip and in the logic for safety injection to ensure low pressure protection.

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

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

Redundancy is not compromised by having a shared tap since the logic for this trip is two out of four. If the impulse line bursts, the indicated pressure in these two channels will drop to zero and the protective function will be maintained.

7.2.2.3.4 Pressurizer Water Level

Three pressurizer water level channels are used for reactor trip. Isolated signals from these channels are used for pressurizer water level control. Since the median level signal is used for control, a single channel failing high or low will not cause an inadvertent control action.

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

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

7.2.2.3.5 Steam Generator Water Level

The basic function of the reactor protection circuits associated with low-low steam generator water level is to preserve the steam generator heat sink for removal of long-term residual heat. Should a complete loss of feedwater occur, the reactor would be tripped on low-low steam generator water level. In addition, redundant auxiliary feedwater pumps are provided to supply feedwater in order to maintain residual heat removal after trip. This reactor trip acts before the steam generators are dry. This reduces the required capacity, increases the time interval before auxiliary feedwater pumps are required, and minimizes the thermal transient on the Reactor Coolant System and steam generators. Therefore, a low-low steam generator water level reactor trip circuit is provided for each steam generator to ensure that sufficient initial thermal capacity is available in the steam generator at the start of the transient. Two-out-of-four low-low steam generator water level trip logic ensures a reactor trip (if needed) even with an independent failure in another channel used for control and when degraded by an additional second postulated random failure.

For control, the median feedwater flow signal is used. This should prevent control action if a single channel fails high or low. If a mismatch occurs between steam flow and feedwater flow, alarms will alert the operator of the situation in time for manual correction. If the condition continues, a two-out-of-four high steam generator water level signal in any loop, independent of the indicated feedwater flow, will cause feedwater isolation and trip the turbine. The high-high steam generator water level trip is an equipment protective trip preventing excessive moisture carryover, which could damage the turbine blading.

In addition, the three element feedwater controller incorporates reset action on the level error signal, such that with expected controller settings a rapid increase or decrease in the flow signal would cause only a small change in level before the controller would compensate for the level error. A slow change in the feedwater signal would have no affect at all. A spurious low or high steam flow signal would have the same effect as high or low feedwater signal, discussed above.

Since the second highest water level is used for control, a single channel failing high or low will not cause an inadvertent control action.

Before a reactor trip would occur, two-out-of-four channels in a loop would have to indicate a low-low water level. Any slow drift in the water level signal will permit the operator to respond to the level alarms and take corrective action.

Automatic protection is provided in case the spurious high level reduces feedwater flow sufficiently to cause low-low level in the steam generator. Automatic protection is also provided in case the spurious low level signal increases feedwater flow sufficiently to cause high level in the steam generator. A turbine trip and feedwater isolation would occur on two-out-of-four high-high steam generator water level in any loop.

With the addition of the Feedwater Control System (FCS) upgrade, the likelihood for feedwater control transients has been reduced by the use of input signal validation by using second highest, median and arbitrator selection logic. A failure of one input signal for any variable will not have an effect on the control system. This logic is available for the following signals:

- S/G NR Level

- S/G WR Level
- S/G Steam Flow (Arbitrator)
- S/G Feedwater Flow
- Feedwater Temperature
- Nuclear Power
- Steam Pressure

Deleted Per 2012 Update.

7.2.2.4 Additional Postulated Accidents

Loss of plant instrument air or loss of component cooling water is discussed in Section 7.3.2.3. Load rejection and turbine trip are discussed in further detail in Section 10.2.2.

The control interlocks, called rod stops, that are provided to prevent abnormal power conditions which could result from excessive control rod withdrawal are discussed in Section 7.7.1.4.1 and listed on Table 7-12. Excessively high power operation (which is prevented by blocking of automatic rod withdrawal), if allowed to continue, might lead to safety limit (as given in the Technical Specifications) being reached. Before such a limit is reached, protection will be available from the Reactor Trip System. At the power levels of the rod block setpoints, safety limits have not been reached; and therefore these rod withdrawal stops do not come under the scope of safety-related system, and are considered as control systems.

7.2.3 Tests and Inspections

The Reactor Trip System meets the testing requirements of IEEE 338-1971, as discussed in Section 7.1.2.4. The testability of the system is discussed in Section 7.2.2.2.3. The initial test intervals are specified in the Technical Specifications. Written test procedures and documentation, conforming to the requirements of IEEE 338-1971, will be available for audit by responsible personnel. Periodic testing complies with Regulatory Guide 1.22 as discussed in Sections 7.1.2.4 and 7.2.2.2.3.

7.2.4 References

1. Reid, J.B., "Process Instrumentation for Westinghouse Nuclear Steam Supply Systems," *WCAP-7913*, January, 1973. (Additional background information only)
2. Lipchak, J.B., "Nuclear Instrumentation System," *WCAP-8255*, January, 1974. (Additional background information only)
3. Katz, D.N., "Solid State Logic Protection System Description," *WCAP-7488-L*, January, 1971 (Proprietary) and *WCAP-7662*, June 1971 (Non-Proprietary). (Additional background information only)
4. Gangloff, W.C. and Loftus, W.D., "An Evaluation of Solid State Logic Reactor Protection In Anticipated Transients, *WCAP-7706-L*, July, 1971 (Proprietary) and *WCAP-7706*, July, 1971 (Non-Proprietary).
5. Eggleston, F.T., Rawlins, D.H., Petrow, J.R., "Failure Mode and Effects Analysis (FMEA) of the Engineered Safeguard Features Actuation System," *WCAP-8584* (Proprietary), April 1976, and *WCAP-8760* (Non-Proprietary), April 1976.

6. Letter, from W. O. Parker Jr. (DPC) to H. R. Denton (NRC), Subject: Bypassing the Anticipatory Reactor Trip on Turbine Trip at Low Power, dated July 26, 1982.
7. Deleted per 2015 update
8. Deleted per 2015 update
9. Deleted per 2015 update
10. Deleted per 2015 update
11. Deleted per 2015 update
12. Deleted per 2015 update
13. Deleted per 2015 update
14. Deleted per 2015 update
15. Deleted per 2015 update
16. WCAP-17867-P-A, Revision 1, “Westinghouse SSPS Board Replacement Licensing Summary Report”
17. License Amendments 40/33 for Units 1 and 2, respectively; February 17, 1988.
18. Letter of May 26, 1987, RTD Bypass Elimination, from Hal B. Tucker to U.S. Nuclear Regulatory Commission.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.2.

7.3 Engineered Safety Features Actuation System

In addition to the requirements for a reactor trip for anticipated abnormal transients, the facility is provided with adequate instrumentation and controls to sense accident situations and initiate the operation of necessary Engineered Safety Features. The occurrence of a limiting fault, such as loss of coolant accident or a steam line break, requires a reactor trip plus actuation of one or more of the Engineered Safety Features in order to prevent or mitigate damage to the core and Reactor Coolant System components, and insure containment integrity.

In order to accomplish these design objectives the Engineered Safety Features System has proper and timely initiating signals which are supplied by the sensors, transmitters, and logic components making up the various instrumentation channels of the Engineered Safety Features Actuation System.

7.3.1 Description

The Engineered Safety Features Actuation System using selected plant parameters, determines whether or not predetermined safety limits are being exceeded and, if they are, combines the signals into logic matrices sensitive to combinations indicative of primary or secondary system boundary ruptures (Class III or IV faults). Once the required logic combination is completed, the system sends actuation signals to the appropriate Engineered Safety Features components. The Engineered Safety Features Actuation System meets the requirements of Criteria 13, 20, 27, 28 and 38 of the 1971 General Design Criteria (GDC).

7.3.1.1 System Description

The Engineered Safety Features Actuation System is a functionally defined system described in this section. The equipment which provides the actuation functions identified in Section 7.3.1.1.1 is listed below and discussed in this section. (For additional background information refer to References 1 and 2.)

1. Process Instrumentation and Control System
2. Solid State Logic Protection System
3. Engineered Safety Features Test Cabinet
4. Manual Actuation Circuits

The Engineered Safety Features Actuation System consists of two discrete portions of circuitry: 1) An analog portion consisting of three to four redundant channels per parameter or variable to monitor various plant parameters such as Reactor Coolant System and steam system pressures, temperatures, and flows and containment pressures; and 2) a digital portion consisting of two redundant logic trains which receive inputs from the analog protection channels and perform the logic needed to actuate the Engineered Safety Features. Each digital train is capable of actuating the Engineered Safety Features equipment required. The intent is that any single failure within the Engineered Safety Features Actuation System shall not prevent system action when required.

The redundancy concept is applied to both the analog and logic portions of the system. Separation of redundant analog channels begins at the process sensors and is maintained in the field wiring, containment vessel penetrations and analog protection racks terminating at the redundant safeguards logic racks. The design meets the requirements of Criteria 20, 21, 22, 23 and 24 of the 1971 GDC.

The variables are sensed by the analog circuitry as discussed in Reference 1 and in Section 7.2. The outputs from the analog channels are combined into actuation logic as shown on Figure 7-2, pages 6, 7, 8, 9, and 10. Table 7-5 and Table 7-6 give additional information pertaining to logic and function.

The interlocks associated with the Engineered Safety Features Actuation System are outlined in Table 7-7. These interlocks satisfy the functional requirements discussed in Section 7.1.2.

All safety-related equipment remains in its emergency mode upon manual reset of the ESF actuation signal. The latching relays in the SSPS output bay maintain the safety-related equipment in their emergency mode due to either a maintained or momentary automatic or manual ESF actuation signal. Once the ESF signal is manually reset, a second operator action is needed to return each device from its emergency mode to its normal mode. Therefore, Catawba Nuclear Station is in compliance with IE Bulletin 80-06, Engineered Safety Features (ESF) reset controls, actions 1 thru 4 as required.

Manual actuation from the control board for containment isolation Phase A is provided by operating either the train A or train B containment isolation Phase A controls. Also on the control board is manual actuation of safety injection by either train A or train B controls and a manual activation of containment isolation Phase B by either train A or train B controls.

Manual controls are also provided to switch from the injection to the recirculation phase after a loss of coolant accident.

The NRC issued Generic Letter 89-19, "Request for Action Related to the Resolution of Unresolved Issue A-47, `Safety Implication of Control Systems in LWR Plants' Pursuant to 10 CFR 50.54(f)," on September 20, 1989. This generic letter required PWR licensees to provide a description of their steam generator overfill protection systems, which was responded to in the letter from H.B. Tucker to NRC, dated March 19, 1990. As described in that response to the NRC, the CNS overfill protection system is initiated on high water level in any one steam generator based on a safety grade 2-out-of-4 initiating logic. The system isolates MFW by closing the MFW isolation valves and tripping the MFW pumps. In accordance with the Generic Letter 89-19 guidance, the overfill protection channels are electrically isolated from the control channels through isolator cards in the Westinghouse 7300 PCS. Section 3.3.2 of the CNS Technical Specifications includes requirements to periodically verify operability of the overfill protection system.

A description of the Ice Condenser System and its associated instrumentation is given in Chapter 6.

7.3.1.1.1 Function Initiation

The specific functions which rely on the Engineered Safety Features Actuation System for initiation are:

1. A reactor trip, provided one has not already been generated by the Reactor Trip System.
2. Charging pumps, safety injection pumps, residual heat removal pumps, and associated valving which provide emergency makeup water to the cold legs of the Reactor Coolant System following a loss of coolant accident.
3. Service water pumps which provide cooling water to the component cooling system heat exchangers and are thus the heat sink for containment cooling.
4. Motor driven auxiliary feedwater pumps.

5. Phase A containment isolation, whose function is to prevent fission product release. (Isolation of all lines not essential to reactor protection.)
6. Steam line isolation to prevent the continuous, uncontrolled blowdown of more than one steam generator and thereby uncontrolled Reactor Coolant System cooldown.
7. Main feedwater line isolation as required to prevent or mitigate the effect of excessive cooldown.
8. Start the emergency diesels to assure backup supply of power to emergency and supporting systems components.
9. Annulus Ventilation System actuation to maintain a negative pressure in the Annulus.
10. High-high containment pressure signal which performs the following functions:
    a. Initiates containment air return fans (after time delay) to reduce containment pressure and temperature following a loss of coolant or steamline break accident inside of containment.
    b. Initiates Phase B containment isolation which isolates the containment following a loss of reactor coolant accident or a steam or feedwater line break within containment to limit radioactive releases. (Phase B isolation together with Phase A isolation results in isolation of all but safety injection and spray lines penetrating the containment.)
11. The Auxiliary Building Ventilation System, the Control Room Area Ventilation System, and the Diesel Building Ventilation System actuate to the following safety modes.
    a. The Auxiliary Building Ventilation System is continuously aligned to the filtered exhaust mode to maintain the emergency core cooling system pump rooms at a negative pressure. Additionally, the Auxilliary Shutdown Panel Supply Units (ASPSUs) A and B receive ESF start signals as described in UFSAR section 9.4.3.1 and Table 8-6.
    b. Diesel Building Ventilation System actuates to maintain proper ventilation of the Diesel Building for Equipment operation.
    c. Control Room Area Ventilation System actuates to maintain the environment in the control room, control room area, and switchgear rooms within acceptable limits for equipment operation and post-accident habitability.

7.3.1.1.2 Analog Circuitry

The process analog sensors and racks for the Engineered Safety Features Actuation System are covered in Reference 1. Discussed in this report are the parameters to be measured including pressures, flows, tank and vessel water levels, and temperatures as well as the measurement and signal transmission considerations. These latter considerations include the transmitters, orifices and flow elements, resistance temperature detectors, as well as automatic calculations, signal conditioning, and location and mounting of the devices.

The sensing points for monitoring the primary system are located as shown on the piping flow diagrams in Chapter 5. The secondary system sensing points are shown on the steam system flow diagrams given in Chapter 10.

Containment pressure is sensed by four transmitters which are seismically mounted outside the containment. Four physically separated ½" stainless steel instrument tubing lines penetrate the containment and lead to the transmitters (one line per transmitter). This design conforms to GDC 56 and Regulatory Guide 1.11.

7.3.1.1.3 Digital Circuitry

The Engineered Safety Features logic racks are discussed in detail in Reference 2. The description includes the considerations and provisions for physical and electrical separation as well as details of the circuitry. Reference 2 also covers certain aspects of on-line test provisions, provisions for test points, considerations for the instrument power source, and considerations for accomplishing physical separation. The outputs from the analog channels are combined into actuation logic as shown on pages 6 (T_{avg}), 7 (Pressurizer Pressure), 8 and 9 (Steam Pressure), 10 (Engineered Safety Features Actuation), and 23 (Auxiliary Feedwater) of Figure 7-2.

WCAP 17867-P-A (Reference 16) has been approved by the NRC to allow use of a replacement design for the originally installed SSPS circuit cards. Certain items pertaining to the SSPS cards, which are detailed in Reference 2 may now be encompassed by the WCAP (Reference 16) for these replacement circuit cards.

To facilitate Engineered Safety Features actuation testing, two cabinets (one per train) are provided which enable operation, to the maximum practical extent, of safety features loads on a group by group basis until actuation of all devices has been checked. Final actuation testing is discussed in detail in Section 7.3.2.

7.3.1.1.4 Final Actuation Circuitry

The outputs of the Solid State Logic Protection System (the slave relays) are energized to actuate, as are most final actuators and actuated devices. These devices are listed as follows:

1. Safety Injection System pump and valve actuators. See Chapter 6 for flow diagrams and additional information.
2. Containment isolation (Phase A - "T" signal isolates all non-essential process lines on receipt of safety injection signal; Phase B - "P" signal isolates remaining process lines (which do not include safety injection lines) on receipt of 2/4 High-High containment pressure signal). For further information, see Section 6.2.4.
3. Service water pump and valve actuators. (See Chapter 9).
4. Auxiliary feedwater pumps start (See Chapter 10).
5. Diesel start (See Chapter 8).
6. Feedwater isolation (See Chapter 10).
7. Ventilation isolation valve and damper actuators (See Chapter 6).
8. Steam line isolation valve actuators (See Chapter 10).
9. Containment air return fans (See Chapter 6).
10. Annulus ventilation.

If an accident is assumed to occur coincident with a blackout, the Engineered Safety Features loads are sequenced onto the diesel generators. This sequence is discussed in Chapter 8. The design meets the requirements of Criterion 35 of the 1971 GDC.

7.3.1.1.5 Support Systems

The following systems are required for support of the Engineered Safety Features:

1. Service Water - Heat Removal (See Chapter 9).

2. Component Cooling Water Systems - Heat Removal (See Chapter 9).
3. Electrical Power Distribution Systems (See Chapter 8).

7.3.1.2 Design Bases Information

The functional diagrams presented in Figure 7-2, pages 6, 7, 8, 9 and 10 provide a graphic outline of the functional logic associated with requirements for the Engineered Safety Features Actuation System. Requirements for the Engineered Safety Features System are given in Chapter 6. Given below is the design bases information required in IEEE 279-1971, Reference 3.

7.3.1.2.1 Generating Station Conditions

The following is a summary of those generating station conditions requiring protective action:

1. Primary System:
   a. Rupture in small pipes or cracks in large pipes
   b. Rupture of a reactor coolant pipe (loss of coolant accident)
   c. Steam generator tube rupture
2. Secondary System
   a. Minor secondary system pipe breaks resulting in steam release rates equivalent to a single dump, relief, or safety valve
   b. Rupture of a major steam pipe

7.3.1.2.2 Generating Station Variables

The following list summarizes the generating station variables required to be monitored for the automatic initiation of Safety Injection during each accident identified in the preceding section. Post accident monitoring requirements are discussed in Section 7.5.

1. Primary System Accidents
   a. Pressurizer pressure
   b. Containment pressure (not required for steam generator tube rupture)
2. Secondary System Accidents
   a. Pressurizer pressure
   b. Containment pressure

   Deleted Per 2009 Update

7.3.1.2.3 Spatially Dependent Variables

The only variable sensed by the Engineered Safety Features Actuation System which has spatial dependence is reactor coolant temperature. The effect on the measurement is negated by taking three hot leg temperature measurements spatially oriented around the hot leg.

7.3.1.2.4 Limits, Margins and Levels

Prudent operational limits, available margins, and setpoints before onset of unsafe conditions requiring protective action are discussed in Chapter 15 and the Technical Specifications.

7.3.1.2.5 Abnormal Events

The malfunctions, accidents, or other unusual events which could physically damage protection system components or could cause environmental changes are as follows:

1. Loss of coolant accident (See Chapter 15)
2. Steam breaks (See Chapter 15)
3. Earthquakes (See Chapter 2 and Chapter 3)
4. Fire (Section 9.5.1)
5. Explosion (Hydrogen buildup inside containment) (See Section 15.4)
6. Missiles (See Section 3.5)
7. Flood (See Chapter 2 and Chapter 3)

7.3.1.2.6 Minimum Performance Requirements

Minimum performance requirements are as follows:

1. System Response Times

   The ESFAS response time is defined as the interval required for the ESF sequence to be initiated subsequent to the time that the appropriate variable(s) exceed this setpoint(s). The ESF sequence is initiated by the output of the ESFAS which is by the operation of the dry contacts of the slave relays (600 series relays) in the output cabinets of the solid state protection system. The response times listed below include the interval of time which will elapse between the time the parameter as sensed by the sensor exceeds the safety setpoint and the time the solid state protection system slave relay dry contacts are operated. These values (as listed below) are maximum allowable values consistent with the safety analyses and are systematically verified during plant preoperational startup tests. For the overall ESF response time; refer to Table 7-15. In a similar manner for the overall reactor trip system instrumentation response time; refer to Table 7-3.

   The Engineered Safety Features Actuation System is always capable of having response time tests performed using the same methods as those tests performed during the preoperational test program or following significant component changes.

   Typical maximum allowable time delays in generating the actuation signal for loss of coolant protection are:

Pressurizer pressure	2.0 seconds

   Typical maximum allowable time delays in generating the actuation signal for steamline break protection are:

a. Steam line pressure (from which steamline pressure rate is derived)[1]	2.0 seconds

[1] Steamline pressure is used only for steamline isolation.

b. Steamline pressure rate 2.0 seconds

c. Reactor Coolant System T_{avg} (as measured) at the resistance temperature detector sensor output. 7.0 seconds

d. High containment pressure for closing mainsteamline isolation valves 1.5 seconds

e. Actuation signals for auxiliary feed pumps 2.0 seconds

2. System accuracies:

   Typical accuracies required for generating the required actuation signals for loss of coolant protection are:

   Pressurizer pressure (uncompensated) ±14 psi

   Typical accuracies required in generating the required actuation signals for steamline protection are:

   a. Steam line pressure (from which steamline pressure rate is derived)[1] ±4% of span

   b. Containment pressure signal ±1.8% of full scale

3. Ranges of sensed variables to be accommodated until conclusion of protective action is assured:

   Typical ranges required in generating the required actuation signals for loss of coolant protection are:

   a. Pressurizer pressure 1700 to 2500

   b. Containment pressure -5 to 5 psig

   Typical ranges required in generating the required actuation signals for steamline break protection are:

   a. T_{avg} 530 to 630F

   b. Steam line pressure (from which steamline pressure rate is derived)[2] 0 to 1300 psig

   c. Containment pressure -5 to 5 psig

7.3.2 Analysis

7.3.2.1 Failure Mode and Effects Analyses

Failure mode and effects analyses (FMEA) have been performed on generic Engineered Safety Features Actuation System (ESFAS) equipment similar to that used at Catawba (Reference 4). These analyses quantitatively demonstrate the reliability of the ESFAS to perform its intended function and show that the ESFAS complies with the single failure criteria of IEEE 279-1971. No single failure was found that could prevent the ESFAS from generating the proper actuation signal on demand. Failures are either in the safe direction, or a redundant channel or train insures the necessary actuation capability.

---

[2] Steamline pressure is used only for steamline isolation.

These generic ESFAS analyses are applicable to the Catawba ESFAS for the following reasons:

1. The Catawba ESFAS equipment is designed to the same equivalent safety design criteria as the Westinghouse generic Standard Plant ESFAS analyzed.
2. The actuation of the Catawba ESFAS is functionally the same as the systems studied in the analyses.
3. The FMEA was of an ESFAS that employed the Solid State Protection System (SSPS) and the 7300 series Process Control System (PCS).
4. The FMEA has been performed down to the replaceable component level such as transmitters, relays, modules, and cards which are of the same family of components as in Catawba.

Duke Power and Westinghouse have jointly reviewed the interface criterion of WCAP 8584 Revision 1 (Reference 4). All items important to preserve the redundancy, and to ensure that no single credible event will prevent operation of the required balance of plant safety systems have been complied with.

WCAP 17867-P-A (Reference 16) has been approved by the NRC to allow use of a replacement design for the originally installed SSPS circuit cards. The board redesign was accomplished in a manner which retained the original operation of the SSPS boards. The system continues to operate as originaly designed. See Reference 16 for additional information regarding FMEA for the replacement design circuit cards.

7.3.2.2 Compliance With Standards and Design Criteria

Discussion of the General Design Criteria (GDC) is provided in various sections of Chapter 7 where a particular GDC is applicable. Applicable GDC's include Criteria 13, 20, 21, 22, 23, 24, 25, 27, 28, 35, 37, 38, 40, 43, and 46 of the 1971 GDC. In addition, the hydrogen recombiner meets GDC 41. Compliance with Regulatory Guides and IEEE Standards is presented in Section 7.1.2.4.

The discussion given below shows that the Engineered Safety Features Actuation System complies with IEEE 279-1971, Reference 3.

7.3.2.2.1 Single Failure Criteria

The discussion presented in section 7.2.2.2.3 (Item 2) is applicable to the Engineered Safety Features Actuation System, with the following exception.

Deleted Per 2012 Update.

In the Engineered Safety Features, a loss of instrument power will call for actuation of Engineered Safety Features equipment controlled by the specific bistable that lost power (except for: 1) containment pressure Hi-Hi and 2) FWST Low Level coincident with SI, switchover to containment sump). The actuated equipment must have power to comply. The power supply for the protection systems is discussed in Chapter 8. For containment pressure Hi-Hi and FWST Low Level coincident with SI, switchover to containment sump, the final bistables are energized to avoid spurious actuation. Also, it is possible for all Engineered Safety Features equipment (valves, pumps, etc.) to be individually actuated manually from the control board. The design meets the requirements of Criteria 21 and 23 of the 1971 GDC.

7.3.2.2.2 Equipment Qualification

Equipment qualifications are discussed in Sections 3.10 and 3.11.

7.3.2.2.3 Independence

Channel independence is carried throughout the system, extending from the sensor through to the devices actuating the protective function. Physical separation is used to achieve separation of redundant transmitters. Separation of wiring is achieved using separate wireways, cable trays, conduit runs, and containment penetrations for each redundant channel. Redundant analog equipment is separated by locating modules in different protection cabinets. Each redundant protection channel set is energized from a separate AC power feed. This design meets the requirements of Criterion 21 of the 1971 GDC.

Separate routing is maintained for the four basic sets of Engineered Safety Features Actuation System analog sensing signals, bistable output signals, and power supplies. The separation of these four channel sets is maintained from sensors to instrument cabinets to logic system input cabinets.

Separate routing of control and power circuits associated with the operation of the Engineered Safety Features equipment is provided in the system design and power supplies.

The Engineered Safety Features slave relay outputs from the solid state logic protection cabinets are redundant, and the actuations associated with each train are energized up to and including the final actuators by the separate ac power supplies that power the logic trains.

The design philosophy is to make maximum use of a wide variety of measurements. The Engineered Safety Features Actuation System continuously monitors numerous diverse system variables. Generally, two or more diverse protection functions would terminate an accident before intolerable consequences could occur. This design meets the requirements of Criterion 22 of the 1971 GDC.

7.3.2.2.4 Control and Protection System Interaction

The discussions presented in Section 7.2.2.2.3 (Item 7) are applicable.

7.3.2.2.5 Capability for Sensor Checks and Equipment Test and Calibration

The discussions of system testability in Section 7.2.2.2.3 (Item 9) are applicable to the sensors, analog circuitry, and logic trains of the Engineered Safety Features Actuation System.

The following discussions cover those areas in which the testing provisions differ from those for the Reactor Trip System.

Testing of Engineered Safety Features Actuation Systems

The Engineered Safety Features Systems are tested to provide assurance that the systems will operate as designed and will be available to function properly in the unlikely event of an accident. The testing program meets the requirements of Criteria 21, 37, 40 and 43 of the 1971 GDC and Regulatory Guide 1.22 as discussed in Section 7.1.2.4.2. The tests described in this section and further discussed in Section 6.3.4 meet the requirements on testing of the Emergency Core Cooling System as stated in GDC 37 except for the operation of those components that will cause an actual safety injection. The test, as described, demonstrates the performance of the full operational sequence that brings the system into operation, the transfer between normal and emergency power sources, and the operation of associated cooling water systems. The safety injection and residual heat removal pumps are started and operated and

their performance verified in a separate test discussed in Section 6.3.4. When the pump tests are considered in conjunction with the Emergency Core Cooling System test, the requirements of GDC 37 on testing of the Emergency Core Cooling System are met as closely as possible without causing an actual safety injection.

Testing as described in Sections 6.3.4, 7.2.2.2.3 and 7.3.2.2.5 provides complete periodic testability during reactor operation of all logic and components associated with the Emergency Core Cooling System. This design meets the requirements of Regulatory Guide 1.22 as discussed in the above sections. The program is as follows:

1. Prior to initial plant operation, Engineered Safety Features System tests will be conducted.
2. Subsequent to initial startup, Engineered Safety Features System tests will be conducted during each regularly scheduled refueling outage.
3. During on-line operation of the reactor, all of the Engineered Safety Features analog and logic circuitry will be fully tested. In addition, essentially all of the Engineered Safety Features final actuators will be fully tested. For the remaining few control circuits whose operation is not compatible with continued on-line plant operation, the final digital device in the actuator circuitry is verified by a continuity check.
4. During normal operation, the operability of testable final actuation devices of the Engineered Safety Features Systems will be tested by manual initiation of the test from the control room.

Performance Test Acceptability Standard for the "S" (Safety Injection Signal) and for the "P" Containment Pressure Hi-Hi Actuation Signals Generation.

During reactor operation the basis for Engineered Safety Features Actuation Systems acceptability will be the successful completion of the overlapping tests performed on the initiating system and the Engineered Safety Features Actuation System (see Figure 7-4). Checks of process indications verify operability of the sensors. Analog checks and tests verify the operability of the analog circuitry from the input of these circuits through the logic input relays except for the input relays associated with the containment pressure Hi-Hi which are tested during the solid state logic testing. Solid state logic testing also checks the digital signal path from and including logic input relay contacts through the logic matrices and master relays and perform continuity tests on the coils of the output slave relays; final actuator testing operates the output slave relays and verifies operability of those devices which require safeguards actuation and which can be tested without causing plant upset. A continuity check is performed on the actuators of the untestable devices. Operation of the final devices is confirmed by control board indication and visual observation that the appropriate pump breakers close and automatic valves have completed their travel.

The basis for acceptability for the Engineered Safety Features interlocks will be control board indication of proper receipt of the signal upon introducing the required input at the appropriate setpoint and with overlapping testing via the semi-automatic logic tester.

In order to minimize the possibilities of accidentally shorting or grounding safety system circuits during testing, a voltage indicator has been wired to the reactor trip breaker terminal blocks which will allow the operators to check the status of certain P-4 interlock described in Table 7-7.

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

Frequency of Performance of Engineered Safety Features Actuation Tests

During reactor operation, complete system testing (excluding sensors or those devices whose operation would cause plant upset) is performed periodically as specified in the Technical Specifications. Testing, including the sensors, is also performed during scheduled plant shutdown for refueling.

Engineered Safety Features Actuation Test Description

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

1. The test procedures must not involve the potential for damage to any plant equipment.
2. The test procedures must minimize the potential for accidental tripping.
3. The provisions for on-line testing must minimize complication of Engineered Safety Features actuation circuits so that their reliability is not degraded.

Description of Initiation Circuitry

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

The remaining functions (listed in Section 7.3.1.1.1) are initiated by a common signal (safety injection) which in turn may be generated by different process conditions.

In addition, operation of all other vital auxiliary support systems, such as auxiliary feedwater, component cooling, and service water, is initiated by the safety injection signal.

Each function is actuated by a logic circuit which is duplicated for each of the two redundant trains of Engineered Safety Features initiation circuits.

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

Analog Testing

Analog testing is identical to that used for reactor trip circuitry and is described in Section 7.2.2.2.3. (Item 10)

Exceptions to this are containment pressure Hi-Hi and FWST Low Level coincident with SI, switchover to containment sump. In both of these cases, the input relays are energized to actuate 2/4 and reverts to 2/3 when one channel is in test.

Solid State Logic Testing

Except for containment pressure Hi-Hi channels; solid state logic testing is the same as that discussed in Section 7.2.2.2.3 (Item 10). During logic testing of one train, the other train can initiate the required Engineered Safety Features function. For additional details, see Reference 2.

Actuator Testing

At this point, testing of the initiation circuits through operation of the master relay and its contacts to the coils of the slave relays has been accomplished. The ESFAS logic slave relays in the Solid State Protection System (SSPS) output cabinets are subjected to coil continuity tests by the output relay tester in the SSPS cabinets. Slave relays (K601, K602, etc.) do not

operate because of reduced voltage applied to their coils by the mode selector switch (TEST/OPERATE). A multiple position master relay selector switch chooses different master relays and corresponding slave relays to which the coil continuity is applied. The master relay selector switch is returned to "OFF" before the mode selector switch is placed back in the "OPERATE" mode. However, failure to do so will not result in defeat of the protective function. The ESFAS slave relays are activated during testing by the on-line test cabinet, so that overlap testing is maintained.

The ESFAS final actuation device or actuated equipment testing shall be performed from the engineered safeguards test cabinets. These cabinets are located near the Solid State Logic Protection System equipment. There is one set of test cabinets provided for each of the two protection trains A and B. Each set of cabinets contains individual test switches necessary to actuate the slave relays. To prevent accidental actuation, test switches are of the type that must be rotated and then depressed to operate the slave relays. Assignments of contacts of slave relays for actuation of various final devices or actuators has been made such that groups of devices or actuated equipment can be operated individually during plant operation without causing plant upset or equipment damage. In the unlikely event that a safety injection signal is initiated during the test of the final device that is actuated by this test, the device will already be in its safeguards position.

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

By means of the procedure outlined above, all engineered safety features devices actuated by ESFAS initiation circuits, with the exceptions noted below and in Section 7.1.2.4 under the discussion of Regulatory Guide 1.22, are operated by the automatic circuitry.

Actuator Blocking and Continuity Test Circuits

The final actuation devices that are not designed to be actuated during plant operation (discussed in Section 7.1.2.4) are tested by the following two test methods:

1) They have been assigned to slave relays for which additional test circuitry has been provided to individually block actuation of a final device upon operation of the associated slave relays during testing. Operation of these slave relays, including contact operations and continuity of the electrical circuits associated with the final devices control are checked in lieu of actual operation. The circuits provide for monitoring of the slave relay contacts, the devices' control circuit cabling, and control voltage.

2) The actuation equipment is placed in a condition where the relay contact operation can be verified without operation of the equipment. In this case, a continuity check is performed on the slave relay contact to verify proper operation of the slave relay, which is the final digital device in the actuator circuitry.

In cases where isolation amplifiers or other devices are used to isolate ESF signals that are used in the control of non-safety devices, continuity is verified through the last component before the isolation device. Interlocking prevents blocking the output from more than one output relay in a protection train at a time. Interlocking between trains is also provided to prevent continuity testing in both trains simultaneously; therefore, the redundant device associated with the protection train not under test will be available in event protection action is required. If an

accident occurs during testing, the automatic actuation circuitry will override testing as noted above. One exception to this is that if the accident occurs while testing a slave relay whose output must be blocked, those few final actuation devices associated with this slave relay will not be overridden; however, the redundant devices in the other train would be operational and would perform the required safety function.

The continuity test circuits for these components that cannot be actuated on line are verified by proving lights on the safeguards test racks.

The typical schemes for blocking operation of selected protection function actuator circuits are shown in Figure 7-5 as details A and B. The schemes operate as explained below and are duplicated for each safeguards train.

Detail A shows the circuit for contact closure for protection function actuation. Under normal plant operation, and equipment not under test, the test lamps "DS*" for the various circuits will be energized. Typical circuit path will be through the normally closed test relay contact "K8*" and through test lamp connections 1 to 3. Coils "X1" and "X2" will be capable of being energized for protection function actuation upon closure of solid state logic output relay contacts "K*". Coil "X1" or "X2" is typical for a breaker closing auxiliary coil, motor starter master coil, coil of a solenoid valve, auxiliary relay, etc. When the contacts "K8*" are opened to block energizing of coil "X1" and "X2", the white lamp is de-energized, and the slave relay "K*" may be energized to perform continuity testing. To verify operability of the blocking relay in both blocking and restoring normal service, open the blocking relay contact in series with lamp connections - the test lamp should be de-energized; close the blocking relay contact in series with the lamp connections - the test lamp should now be energized, which verifies that the circuit is now in its normal (i.e., operable) condition.

Detail B shows the circuit for contact opening for protection function actuation. Under normal plant operation, and equipment not under test, the white test lamps "DS*" for the various circuits will be energized, and green test lamp "DS*" will be de-energized. Typical circuit path for white lamp "DS*" will be through the normally closed solid state logic output relay contact "K*" and through test lamp connections 1 to 3. Coils "Y1" and "Y2" will be capable of being de-energized for protection function upon opening of solid state logic output relay contacts "K*". Coil "Y2" is typical for a solenoid valve coil, auxiliary relay, etc. When the contacts "K8*" are closed to block de-energizing of coils "Y1" and "Y2", the green test lamp is energized and the slave relay "K*" may be energized to verify operation (opening of its contacts). To verify operability of the blocking relay in both blocking and restoring normal service, close the blocking relay contact to the green lamp - the green lamp should now be energized also; open this blocking relay contact - the green test lamp should be de-energized, which verifies that the circuit is now in its normal (i.e., operable) position.

Deleted Per 2009 Update

Summary of On-Line Testing Capabilities

The procedures described provide capability for checking completely from the process signal to the logic cabinets and from there to the individual pump and fan circuit breakers or starters, valve contactors, pilot solenoid valves, etc. including all field cabling actually used in the circuitry called upon to operate for an accident condition. For those few devices whose operation could adversely affect plant or equipment operation, the same procedure provides for checking from the process signal to the logic rack. The final digital device in the actuator circuitry is verified by a continuity check.

The procedures require testing at various locations.

1. Analog testing and verification of bistable setpoint are accomplished at process analog racks. Verification of bistable relay operation is done at the main control room status lights.
2. Logic testing through operation of the master relays and low voltage application to slave relays is done at the logic rack test panel.
3. Testing of pumps, fans, and valves is done at a test panel located in the vicinity of the logic racks in combination with the control room operator.
4. Continuity testing for those circuits that can not be operated is done at the same test panel mentioned in 3 above.

The reactor coolant pump essential service isolation valves consist of the isolation valves for the component cooling water return and the seal water return header.

The main reason for not testing these valves periodically is that the reactor coolant pumps may be damaged. Although pump damage from this type of test would not result in a situation which endangers the health and safety of the public, it could result in unnecessary shutdown of the reactor for an extended period of time while the reactor coolant pump or certain of its parts could be replaced. This would result in a severe economic burden.

Testing During Shutdown

Emergency Core Cooling System tests will be performed periodically in accordance with the Technical Specifications with the Reactor Coolant System isolated from the Emergency Core Cooling System by closing the appropriate valves. A test safety injection signal will then be applied to initiate operation of active components (pumps and valves) of the Emergency Core Cooling System. This is in compliance with Criterion 37 of the 1971 GDC.

Containment Spray System tests will be performed at each major fuel reloading. The test will be performed with the isolation valves in the spray supply lines at the containment blocked closed and are initiated by tripping the normal actuation instrumentation.

Periodic Maintenance Inspections

The periodic maintenance will be accomplished per applicable plant procedures. The frequency will depend on the operating conditions and requirements of the reactor power plant. If any degradation of equipment operation is noted, either mechanically or electrically, remedial action is taken to repair, replace, or readjust the equipment. Optimum operating performance must be achieved at all times.

Deleted Per 2009 Update

The balance of the requirements listed in IEEE 279-1971 (Paragraphs 4.11 through 4.22) are discussed in Section 7.2.2.2.1. Paragraph 4.20 receives special attention in Section 7.5.

7.3.2.2.6 Manual Blocking Features

The manual block features associated with pressurizer safety injection signal and steam line main steam isolation signal provide the operator with means to block initiation of safety injection and main steam isolation during plant startup. These block features meet the requirements of paragraph 4.12 of IEEE 279-1971 in that automatic removal of the block occurs when plant conditions require the protection system to be functional.

The manual block feature associated with the Steam Generator Hi-Hi Level (P-14) signal provides the operator with the means to block initiation of Turbine Trip and Feedwater Isolation functions during Modes 4, 5 and 6. This block is administratively removed prior to entry into Mode 3. Automatic removal is provided via the ESFAS when the unit reaches the P-11 setpoint.

The manual block feature associated with the automatic start of the Auxiliary Feedwater Pumps provides the operator with the means to block initiation of this function during Modes 4, 5 and 6. This block is administratively removed prior to entry into Mode 3. Automatic removal is provided via the ESFAS when the unit reaches the P-11 setpoint.

7.3.2.2.7 Manual Initiation of Protective Actions (Regulatory Guide 1 .62)

There are four individual main steam isolation valve momentary control switches (one per loop) mounted on the control board. Each switch, when actuated, will isolate one of the main steam lines. In addition, there will be two system level switches. Each switch will actuate all four main steam line isolation and bypass valves at the system level.

Manual initiation of switchover to recirculation is in compliance with Section 4.17 of IEEE 279-1971 with the following comment:

Manual initiation of either one of two redundant safety injection actuation main control board mounted switches provides for actuation of the components required for reactor protection and mitigation of adverse consequences of the postulated accident. Switchover from the safety injection mode to the cold leg recirculation mode following a loss of primary coolant accident is by semi-automatic means (Section 6.3).

No exception to the requirements of IEEE 279-1971 has been taken in the manual initiation circuit of safety injection. Although paragraph 4.17 of IEEE 279- 1971 requires that a single failure within common portions of the protective system shall not defeat the protective action by manual or automatic means, the standard does not specifically preclude the sharing of initiated circuitry logic between automatic and manual functions. It is true that the manual safety injection initiation functions associated with one actuation train (e.g., train A) shares portions of the automatic initiation circuitry logic of the same logic train; however, a single failure in shared functions does not defeat the protective action of the redundant actuation train (e.g., train B). A single failure in shared functions does not defeat the protective action of the safety function, because a single failure in shared functions in one train does not affect the opposite train. It is further noted that the sharing of the logic by manual and automatic initiation is consistent with the system level action requirements of the IEEE 279-1971, paragraph 4.17 and consistent with the minimization of complexity.

Manual actuation of containment isolation (Phase A) and containment spray actuation is provided by operating either train A, train B, or both controls. These manual actuation functions meet the same criteria described for manual safety injection actuation.

7.3.2.3 Further Considerations

In addition to the considerations given above, a loss of instrument air or loss of component cooling water to vital equipment has been considered. Neither the loss of instrument air nor the loss of cooling water (assuming no other accident conditions) can cause safety limits as given in the Techincal Specifications to be exceeded. Likewise, loss of either one of the two will not adversely affect the core or the Reactor Coolant System nor will it prevent an orderly shutdown if this is necessary. Furthermore, all pneumatically operated valves and controls will assume a preferred operating position upon loss of instrument air. It is also noted that, for conservatism during the accident analysis (Section 15.1), credit is not taken for the instrument air systems nor for any control system benefit.

The design does not provide any circuitry which will directly trip the reactor coolant pumps on a loss of component cooling water. Indication is provided in the control room for a loss of component cooling. The reactor coolant pumps can run approximately 10 minutes after a loss

of component cooling water. This provides adequate time for the operator to correct the problem or trip the plant if necessary.

In regards to the Auxiliary Feedwater System, there are two motor-driven pumps and one turbine-driven pump. The motor-driven pumps are initiated automatically by the following signals: (These signals also close the blowdown isolation and sample line valves for all steam generators).

1. Safety injection, or safeguards sequence (from Solid State Protection System) or
2. 2/4 low-low level in any steam generator (from Solid State Protection System) or
3. Trip of all main feed pumps or
4. Blackout signal

The motor-driven pumps are also started manually.

The turbine-driven pump as well as the closing of blowdown and sample valves are initiated automatically by:

1. 2/4 low-low level in 2/4 steam generators (from Solid State Protection System) or
2. Blackout signal

The turbine driven pump is also started manually.

The controls for the Auxiliary Feedwater System are described in Section 7.4.1.

7.3.2.4 Summary

The effectiveness of the Engineered Safety Features Actuation System is evaluated in Section 15.1, based on the ability of the system to contain the effect of Condition III and IV faults, including loss of coolant and steam break accidents. The Engineered Safety Features Actuation System parameters are based upon the component performance specifications which are given by the manufacturer or verified by test for each component. Appropriate factors to account for uncertainties in the data are factored into the constants characterizing the system.

The Engineered Safety Features Actuation System must detect Condition III and IV faults and generate signals which actuate the Engineered Safety Features. The system must sense the accident condition and generate the signal actuating the protection function reliably and within a time determined by and consistent with the accident analyses in Chapter 15.

Much longer times are associated with the actuation of the mechanical and fluid system equipment associated with Engineered Safety Features. This includes the time required for switching, bringing pumps and other equipment to speed, and the time required for them to take load.

Operating procedures require that the complete Engineered Safety Features Actuation System normally be operable. However, redundancy of system components is such that the system operability assumed for the safety analyses can still be met with certain instrumentation channels out of service. Channels that are out of service are to be placed in the tripped mode or bypass mode in the case of containment pressure Hi-Hi and FWST Low Level coincident with SI, switchover to containment sump.

7.3.2.4.1 Loss of Coolant Protection

By analysis of loss of coolant accident and in system tests it has been verified that except for very small coolant system breaks which can be protected against by the charging pumps

followed by an orderly shutdown, the effects of various loss of coolant accidents are reliably detected by the low pressurizer pressure signal; the Emergency Core Cooling System is actuated in time to prevent or limit core damage.

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

High containment pressure also actuates the Emergency Core Cooling System. Therefore, emergency core cooling actuation can be brought about by sensing this other parameter which is a direct consequence of a primary system break. Thus, the Engineered Safety Features Actuation System detects the leakage of the coolant into the Containment. The generation time of the actuation signal of approximately 1.5 seconds, after detection of the consequences of the accident, is adequate. Containment spray will provide additional emergency cooling of containment and also limit fission product release upon sensing elevated containment pressure (high-high) to mitigate the effects of a loss-of-coolant accident.

The delay time between detection of the accident condition and the generation of the actuation signal for these systems is assumed to be 1.0 second; well within the capability of the protection system equipment. However, this time is short compared to that required for startup of the fluid systems. The analyses in Section 15.1 show that the diverse methods of detecting the accident condition and the time for generation of the signals by the protection systems are adequate to provide reliable and timely protection against the effects of loss-of-coolant.

7.3.2.4.2 Steam Line Break Protection

The Emergency Core Cooling System is also actuated in order to protect against a steam line break. Approximately 2.0 seconds elapse between the sensing of low pressurizer pressure and the generation of the actuation signal. Analysis of steam break accidents assuming this delay for signal generation shows that the Emergency Core Cooling System is actuated for a steam line break in time to limit or prevent further core damage for steam line break cases. There is a reactor trip and the core reactivity is further reduced by the highly borated water injected by the Emergency Core Cooling System.

Additional protection against the effects of steam line break is provided by feedwater isolation which occurs upon actuation of the Emergency Core Cooling System. Feedwater line isolation is initiated in order to prevent excessive cooldown of the reactor vessel and thus protect the Reactor Coolant System boundary.

Additional protection against a steam break accident is provided by closure of all steam line isolation valves in order to prevent uncontrolled blowdown of all steam generators. The generation of the protection system signal (approximately 2.0 seconds) is again short compared to the time to trip the fast acting steam line isolation valves which are designed to close in less than approximately 8.0 seconds.

In addition to actuation of the Engineered Safety Features, the effect of a steam line break accident also generates a signal resulting in a reactor trip on overpower or following Emergency Core Cooling System actuation. However, the core reactivity is further reduced by the highly borated water injected by the Emergency Core Cooling System.

The analyses in Chapter 15 of the steam break accidents and an evaluation of the protection system instrumentation and channel design shows that the Engineered Safety Features Actuation Systems are effective in preventing or mitigating the effects of a steam break accident.

7.3.3 References

1. Reid, J. B., "Process Instrumentation for Westinghouse Nuclear Steam Supply System (4 Loop Plant using WCID 7300 Series Process Instrumentation," *WACP-7913*, March, 1973.
2. Katz, D. N., "Solid State Logic Protection System Description," *WCAP-7488-L*, January, 1971 (Proprietary) and *WCAP-7672*, June, 1971 (Non-Proprietary).
3. The Institute of Electrical and Eletronics Engineers, Inc., "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations," IEEE Standard 279-1971.
4. Mesmeringer, J. C., "Failure Mode and Effects Analysis (FMEA) of the Engineered Safety Features Actuation System, " *WCAP-8584* Revision 1, (Proprietary) and *WCAP-8760* Revision 1, (Non-Proprietary), February 1980.
5. Nuclear Regulatory Commission, Letter to All Licensees of Operating Reactors, Applicants for Operating Licenses and Holders of Construction Permits for Light Water Reactor Power Plants, from James G. Partlow, September 20, 1989, "Request for Action Related to the Resolution of Unresolved Issue A-47, `Safety Implication of Control Systems in LWR Plants' Pursuant to 10 CFR 50.54(f) (Generic Letter 89- 19)."
6. Duke Power Company, Letter from H.B. Tucker to NRC, March 19, 1990, re: Response to Generic Letter 89-19, "Request for Action Related to the Resolution of Unresolved Issue A-47, `Safety Implication of Control Systems in LWR Plants' Pursuant to 10 CFR 50.54(f)."
7. Deleted per 2015 update
8. Deleted per 2015 update
9. Deleted per 2015 update
10. Deleted per 2015 update
11. Deleted per 2015 update
12. Deleted per 2015 update
13. Deleted per 2015 update
14. Deleted per 2015 update
15. Deleted per 2015 update
16. WCAP-17867-P-A, Revision 1, “Westinghouse SSPS Board Replacement Licensing Summary Report”

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.3.

7.4 Systems Required for Safe Shutdown

The functions necessary for safe shutdown are available from instrumentation channels that are associated with the major systems in both the primary and secondary of the Nuclear Steam Supply System as well as portions of the balance-of-plant. These channels are normally aligned to serve a variety of operational functions, including startup and shutdown as well as protective functions. There are no identifiable safe shutdown systems per se. However, prescribed procedures for securing and maintaining the plant in a safe condition can be instituted by appropriate alignment of selected systems. The discussion of these systems together with the applicable codes, criteria, and guidelines is found in other sections of the Safety Analysis Report. In addition the alignment of shutdown functions associated with the Engineering Safety Features which are invoked under postulated limiting fault situations is discussed in Chapter 6 and Section 7.3.

The instrumentation and control functions which are required to be aligned for maintaining safe shutdown of the reactor that are discussed in this section are the minimum number under non-accident conditions. These functions will permit the necessary operations that will:

1. Prevent the reactor from achieving criticality in violation of the Technical Specifications and
2. Provide an adequate heat sink such that design and safety limits are not exceeded.

The designation of systems that can be used for safe shutdown depends on identifying those systems which provide the following capabilities for maintaining a safe shutdown:

1. Boration
2. Adequate supply for auxiliary feedwater
3. Residual heat removal

IEEE 279-1971 establishes the specific design basis information required for the protection systems of nuclear power stations. The following addresses each of these design bases as they apply to the systems required for safe shutdown:

1. Conditions Requiring Protective Action

   The generating station conditions that require protective action are addressed in the subsections of Section 7.4 in which the individual systems are discussed. Additional discussions of these systems are provided in Chapter 5, Chapter 6, Chapter 9, and Chapter 10.

2. Variables Monitored to Provide Protective Action

   The generating station variables monitored to provide protective action are addressed in the subsections of Section 7.4 in which the individual systems are discussed.

3. Sensors for Spatially Dependent Variables

   There are no spatially dependent variables associated with the safety functions performed by the systems in this section.

4. Operational Limits, Margins, and Levels Requiring Protective Action

   Prudent operational limits, available margins, and setpoints before the onset of unsafe conditions requiring protective action are discussed in Chapter 15 and the Technical Specifications.

5. Range of Transient and Steady-State Conditions

The range of energy supply and environmental conditions during normal, abnormal, and accident conditions are provided in Sections 8.3 and 3.11, respectively.

6. Events Which Could Damage or Degrade Systems

   Events that could damage or degrade system components are analyzed and discussed in the High Energy Line Break Analysis, and the seismic and environmental qualification sections (Sections 3.10 and 3.11) of the FSAR.

7. Minimum Performance Requirements

   The minimum performance requirements for critical variables that initiate or control system safety functions are discussed in Chapter 15 and the Technical Specifications.

7.4.1 Auxiliary Feedwater System Instrumentation and Control

7.4.1.1 Description

The Auxiliary Feedwater System (AFS) assures an adequate supply of feedwater to the steam generators during normal plant startup and shutdown, and during emergency conditions when the supply from the Main Feedwater System is not available.

The system is provided with two motor-driven auxiliary feedwater pumps powered from separate trains of Class 1E power, and one turbine-driven auxiliary feedwater pump provided with Class 1E dc control power. Any one of the three auxiliary feedwater pumps has the capacity to supply the minimum feedwater requirements defined above. The Auxiliary Feedwater System is discussed in detail in Section 10.4.9.

The motor driven auxiliary feedwater pumps are automatically started to feed the steam generators on any of the following conditions:

1. Two-out-of-four low-low level signals in any steam generator
2. Loss of both main feedwater pumps
3. Safety injection initiation
4. Blackout

The turbine-driven auxiliary feedwater pump is automatically started to feed the steam generators on either of the following conditions:

1. Two-out-of-four low-low level signals in any two steam generators
2. Blackout

Automatic starting of the auxiliary feedwater pumps by a safety injection signal or by low-low steam generator level signals is initiated by the Engineered Safety Features Actuation System (ESFAS) as shown on Figure 7-2, page 10. Automatic starting of the motor driven pumps on a blackout is initiated by the diesel sequencer as described in Section 8.3.1. A safety injection signal or a blackout blocks the automatic start of the motor-driven pumps on low-low steam generator level or loss of main feedwater pumps in order to allow the diesel sequencer to start the pumps in the proper load sequence.

During normal station operation, the Auxiliary Feedwater System normal condensate grade suction supply valves and the pump discharge valves are aligned to provide auxiliary feedwater flow without repositioning on an automatic start signal.

The Auxiliary Feedwater System can be manually controlled from either the main control room or the local control panels as selected by the transfer switches on the local control panels. Transferring control to the local control panels limits control of the pumps to manual control and control by the diesel sequencer. This transfer scheme is discussed further in Section 7.4.7.

A control grade auxiliary feedwater flow indication is provided in the control room. The auxiliary feedwater flow indication for the Catawba Nuclear Station follows the requirements as set forth in NUREG-0737. Single channel monitoring and indication is provided in the control room for each steam generator loop auxiliary feedwater flow. High reliability battery-backed power sources for the instrumentation are selected in conformance with auxiliary systems branch technical position 10-1. Failure of one power source will not cause a loss of flow indication to all steam generators.

NUREG-0737 does not require Westinghouse plants to have a redundant channel for the auxiliary flow indication. The single channel required needs not be seismically qualified or powered by a class IE power source since the flow indication is of limited importance in assuring steam generator cooling capability for U-tube type designs.

Controls are provided in the control room to manually initiate a bypass of the automatic start of the motor driven auxiliary feedwater pumps on low-low steam generator level or loss of both main feedwater pumps. This feature allows the operator to control the starting and stopping of auxiliary feedwater pumps during plant startup and shutdown. The bypass of the automatic starting logic can be manually reset during the startup procedure or it will be automatically reset by a signal from the ESFAS when the unit reaches the P-11 setpoint. Either manual or automatic resetting of the "Auto-Start Defeat" logic allows the motor driven auxiliary feedwater pumps to be automatically started by any one of the four auto-start conditions listed above.

Indication of this bypass is provided in the control room by an indicating light on the control switch that actuates the bypass and by lights on the OAC 1.47 Bypass Panel Graphic Displays as described in Section 7.8. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell.

To provide a long term safety-related source of cooling water, each of the auxiliary feedwater pumps is automatically connected to the Nuclear Service Water (NSW) System. Each motor driven auxiliary feedwater pump is automatically aligned to take suction from its' associated drain of NSW when all of the following conditions exist:

1. Motor Driven auxiliary feedwater pump is started automatically
2. Motor Driven auxiliary feedwater pump is running
3. Low pressure is sensed by two-out-of-three pressure switches sensing the normal suction supply pressure

The turbine driven auxiliary feedwater pump is automatically aligned to take suction from both trains of NSW when all of the following conditions exist:

1. Turbine Driven auxiliary feedwater pump is started automatically.
2. Low pressure is sensed by two out of three pressure switches sensing the normal suction supply pressure.

The logic for the automatic alignment to NSW is provided on Figure 7-6 and Figure 7-7.

Auxiliary Feedwater System instrumentation and controls provided for remote shutdown capabilities are described in Section 7.4.7.

7.4.1.2 Design Bases

The Auxiliary Feedwater System instrumentation and controls are designed to provide reliable monitoring and control of the Auxiliary Feedwater System so that the minimum required feedwater is provided to the steam generators in the event the main feedwater and condensate systems are not available.

7.4.1.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to these controls. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.4.1.3.1 General Functional Requirement

The Auxiliary Feedwater System safety-related instrumentation and controls automatically control the operation of the Auxiliary Feedwater System to assure that an adequate supply of feedwater is provided to the steam generators when the main feedwater and condensate systems are not available.

7.4.1.3.2 Single Failure Criterion

No single failure of the Auxiliary Feedwater System safety-related instrumentation and controls can prevent the system from supplying feedwater to less than two steam generators.

7.4.1.3.3 Quality of Components

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.4.1.3.4 Equipment Qualification

Qualification of the electrical equipment in the Auxiliary Feedwater System is discussed in Sections 3.10 and 3.11.

7.4.1.3.5 Channel Integrity

The safety-related instrumentation and controls for the redundant trains of auxiliary feedwater are designed to assure system functional capability.

7.4.1.3.6 Channel Independence

The safety-related instrumentation and controls of the redundant auxiliary feedwater trains are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.4.1.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls of the Auxiliary Feedwater System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the Auxiliary Feedwater System are part of the ESFAS and are described in Section 7.3

7.4.1.3.8 Derivation of System Inputs

Input signals to the Auxiliary Feedwater System instrumentation and controls are provided by the ESFAS or are derived from direct measurement of the desired variable.

7.4.1.3.9 Capability for Test and Calibration

The Auxiliary Feedwater System safety-related instrumentation and controls are designed to facilitate testing and calibration as required by the Technical Specifications.

7.4.1.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls of the Auxiliary Feedwater System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the Auxiliary Feedwater System are part of the ESFAS and are described in Section 7.3.

7.4.1.3.11 Operating Bypasses

A manually initiated bypass is provided to prevent the motor driven Auxiliary Feedwater Pumps from automatically starting during plant startup or shutdown. This bypass can be removed during the startup procedure, or it will be automatically removed by a signal from the ESFAS when the unit reaches the P-11 setpoint.

7.4.1.3.12 Indication of Bypasses

Bypass of the Auxiliary Feedwater System automatic start is indicated in the control room as described in Section 7.4.1.1 above. Bypass indication is also provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either train of auxiliary feedwater has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. The ESF bypass indication panel is discussed in Section 7.8.3.

7.4.1.3.13 Access to Means for Bypassing

Access to the controls and equipment that initiate a bypass of the Auxiliary Feedwater System instrumentation and controls is controlled by administrative and security measures.

7.4.1.3.14 Multiple Setpoints

Multiple setpoints are not required for the Auxiliary Feedwater System.

7.4.1.3.15 Completion of Protective Action Once it is Initiated

Once initiated by a protective signal, the Auxiliary Feedwater System continues to operate until deliberate action is taken by the operator.

7.4.1.3.16 Manual Initiation

The Auxiliary Feedwater System can be manually initiated from the control room or from the local control panels once the local transfer switches have been operated.

7.4.1.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to all setpoint adjustments, calibration adjustments, and test points is controlled by administrative and security measures.

7.4.1.3.18 Identification of Protective Action

The safety-related instrumentation and controls of the Auxiliary Feedwater System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the Auxiliary Feedwater System are part of the ESFAS and are described in Section 7.3.

7.4.1.3.19 Information Read-Out

Information read-outs pertinent to the correct operation of the Auxiliary Feedwater System are provided in the control room and at the local control panels.

7.4.1.3.20 System Repair

The Auxiliary Feedwater System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.4.1.3.21 Identification

The Auxiliary Feedwater System safety-related instrumentation and control equipment is physically identified as described in Section 7.1.2.3.

7.4.2 Nuclear Service Water System Instrumentation and Control

7.4.2.1 Description

The Nuclear Service Water (NSW) System supplies cooling water to safety and non-safety loads in both units. Cooling water taken from either Lake Wylie or the Standby Nuclear Service Water Pond (SNSWP) is pumped through heat exchangers in both units and returned to its source. The NSW System is discussed in detail in Section 9.2.1.

The NSW System is controlled manually under normal conditions. One NSW train per unit is normally in operation with pump suctions and discharges shared between units to provide cooling water from Lake Wylie.

On receipt of a safety injection signal, all four NSW pumps (both pumps on each unit) are started. On the affected unit, NSW isolation valves for the component cooling heat exchangers, and diesel generator engine jacket water heat exchangers receive a signal to open; and the NSW isolation valves on the NSW pump general use header crossover line and nonessential HVAC loads in the Auxiliary Building receive a signal to close. Upon receipt of a Phase B containment isolation signal, the isolation valves to nonessential loads in the Reactor Building and all remaining nonessential loads are automatically closed.

An emergency low level in either NSW pump pit initiates automatic realignment of the system from the lake to the SNSWP.

The NSW pump outlet valves and motor cooler inlet valves are interlocked to open when their associated pump starts. Additionally, the heat exchanger inlet valves for the diesel generators are interlocked to open when their associated diesel generator starts.

There are no automatic bypasses capable of preventing the NSW System from performing its safety function; however, in the event system control has been transferred to the Auxiliary Shutdown Complex, all automatic signals to the Auxiliary Shutdown Complex controlled components are defeated (refer to Section 7.4.7). Automatic closure of nonessential equipment isolation valves is blocked during system testing.

NSW System safety-related instrumentation and controls are powered from the same train of essential auxiliary power as their associated train of NSW equipment.

When the NSW is aligned in Single Supply Header Operation (refer to Section 9.2.1.7), the RN supply header crossover valves 1RN47A, 1RN48B, 2RN47A, and 2RN48B are prevented from auto-closing on a Phase B containment isolation signal, or an emergency low pumphouse pit level. Similarly, the RN return header crossover isolation valves 1RN53B and 1RN54B are prevented from auto-closing on an emergency low pumphouse pit level. This ensures that NSW cooling water flow is available to all four essential headers if there is an event that generates either or both of these signals while the NSW system is aligned in Single Supply Header Operation.

7.4.2.2 Design Bases

The Nuclear Service Water System instrumentation and controls are designed to provide reliable monitoring and control of the NSW System so that a continuous flow of cooling water is supplied to the systems and components required for safety under normal and accident conditions.

7.4.2.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to these controls. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.4.2.3.1 General Functional Requirements

The Nuclear Service Water System instrumentation and controls monitor and control the operation of the NSW System to assure a continuous supply of cooling water to essential systems and components under normal and accident conditions.

7.4.2.3.2 Single Failure Criterion

No single failure in the NSW System instrumentation and controls can affect the operation of more than one train of NSW.

7.4.2.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.4.2.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.4.2.3.5 Channel Integrity

The redundant trains of safety-related instrumentation and controls for the NSW System are designed to assure system functional capability.

7.4.2.3.6 Channel Independence

The safety-related instrumentation and controls for the redundant NSW trains are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.4.2.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls of the Nuclear Service Water System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the Nuclear Service Water System are part of the ESFAS and are described in Section 7.3.

7.4.2.3.8 Derivation of System Inputs

Input signals to the NSW System instrumentation and controls are provided by the ESFAS or are derived from direct measurement of the desired variable.

7.4.2.3.9 Capability for Test and Calibration

The NSW System safety-related instrumentation and controls are designed to facilitate testing and calibration as required by the Technical Specifications.

7.4.2.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls of the NSW System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the NSW System are part of the ESFAS and are described in Section 7.3.

7.4.2.3.11 Operating Bypasses

The train related NSW System instrumentation and controls do not employ operating bypasses in their initiating logic. The protection channels that actuate the NSW System are part of the ESFAS and are described in Section 7.3.

7.4.2.3.12 Indication of Bypasses

Indication is provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either train of the NSW System has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. The ESF bypass indication panel is discussed in Section 7.8.3.

7.4.2.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the NSW System inoperable is controlled by administrative and security measures.

7.4.2.3.14 Multiple Setpoints

Multiple setpoints are not required for the NSW System.

7.4.2.3.15 Completion of Protective Action Once it is Initiated

Once initiated by a protective signal, the NSW System continues to operate until deliberate action is taken by the operator.

7.4.2.3.16 Manual Initiation

The NSW System pumps and valves can be manually operated from the control room.

7.4.2.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

No protection system setpoints are derived from the NSW System.

7.4.2.3.18 Identification of Protective Action

The safety-related instrumentation and controls of the NSW System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the NSW System are part of the ESFAS and are described in Section 7.3.

7.4.2.3.19 Information Read-Out

Information read-outs related to the operation of the NSW System for safety-related functions are provided in the control room.

7.4.2.3.20 System Repair

The NSW System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.4.2.3.21 Identification

The NSW System safety-related instrumentation and control equipment is physically identified as described in Section 7.1.2.3.

7.4.3 Component Cooling Water System Instrumentaton and Control

7.4.3.1 Description

The Component Cooling Water System supplies cooling water to the safety-related heat exchangers of the Residual Heat Removal (RHR) System and to non-safety-related heat exchangers in various other plant systems. The Component Cooling Water System is described in Section 9.2.2.

The Component Cooling Water System is controlled manually during normal conditions. In the event of an accident, a safety injection signal overrides the manual controls to automatically start all four component cooling water pumps. Low refueling water tank level coincident with safety injection or containment isolation will open the RHR system heat exchanger isolation valves and close the Auxiliary and Reactor Building non-essential header isolation valves. Low surge tank level in either surge tank will isolate the affected train from the opposite train and the Auxiliary and Reactor Building non-essential headers. All component cooling water pumps are also started on a blackout signal. Receipt of a containment isolation signal automatically isolates all nonessential heat exchangers inside the Containment. Component Cooling Water System control logic is provided in Figure 7-8.

Instrumentation is provided to monitor flow in the component cooling water return lines from the reactor coolant pump thermal barriers. High flow in these lines is indicative of reactor coolant leakage into the Component Cooling Water System through a leaking thermal barrier cooling coil. Should flow in a thermal barrier return line exceed the instrument high flow setpoint, the associated thermal barrier return line isolation valve is automatically closed. Additionally,

instrumentation is provided to monitor flow to the reactor coolant pump bearing coolers. A low flow condition will actuate a control room annunicator.

Flow instrumentation is provided to protect the component cooling water pumps from a low flow condition. Should the flow from a component cooling water pump decrease below the low flow setpoint, the assoicated pump recirculation line isolation valve is automatically opened.

There are no bypasses capable of preventing the Component Cooling Water System from performing its safety function; however, in the event system control must be transferred to the auxiliary shutdown panel, some automatic signals are defeated (refer to Section 7.4.7).

Component Cooling Water System safety related instrumentation and controls are powered from the same train of essential auxiliary power as their associated train of component cooling water equipment.

7.4.3.2 Design Bases

The Component Cooling Water System instrumentation and controls are designed to provide reliable and continuous control of system equipment under all plant operating conditions. The controls provide for manual operation of the system under normal conditions with overriding automatic controls to realign equipment to a safety mode of operation at the onset of abnormal plant conditions.

7.4.3.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to these controls. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.4.3.3.1 General Functional Requirements

The Component Cooling Water System instrumentation and controls monitor and control the operation of the Component Cooling Water System to assure a continuous supply of cooling water to essential systems and components under normal and accident conditions.

7.4.3.3.2 Single Failure Criterion

No single failure of the Component Cooling Water System instrumentation and controls can prevent the system from performing its required safety function.

7.4.3.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.4.3.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.4.3.3.5 Channel Integrity

The safety-related instrumentation and controls for the redundant trains of component cooling water are designed to assure system functional capability.

7.4.3.3.6 Channel Independence

The safety-related instrumentation and controls for the redundant trains of component cooling water are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.4.3.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls of the Component Cooling Water System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the Component Cooling Water System are part of the ESFAS and are described in Section 7.3.

7.4.3.3.8 Derivation of System Inputs

Input signals to the Component Cooling Water System instrumentation and controls are provided by the ESFAS or are derived from direct measurement of the desired variable.

7.4.3.3.9 Capability for Test, and Calibration

The Component Cooling Water System safety-related instrumentation and controls are designed to facilitate testing and calibration as required by the Technical Specifications.

7.4.3.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls of the Component Cooling Water System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the Component Cooling Water System are part of the ESFAS and are described in Section 7.3.

7.4.3.3.11 Operating Bypasses

The train related Component Cooling Water System instrumentation and controls do not employ operating bypasses in their initiating logic. The protection channels that actuate the Component Cooling Water System are part of the ESFAS and are described in Section 7.3.

7.4.3.3.12 Indication of Bypasses

Indication is provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either train of the Component Cooling Water System has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. The ESF bypass indication panel is discussed in Section 7.8.3.

7.4.3.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the Component Cooling Water System inoperable is controlled by administrative and security measures.

7.4.3.3.14 Multiple Setpoints

Multiple setpoints are not required for the Component Cooling Water System.

7.4.3.3.15 Completion of Protective Action Once it is Initiated

Once initiated by a protective signal, the Component Cooling Water System continues to operate until deliberate action is taken by the operator.

7.4.3.3.16 Manual Initiation

The Component Cooling Water System pumps and valves can be manually operated from the control room.

7.4.3.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

No protection system setpoints are derived from the Component Cooling Water System.

7.4.3.3.18 Identification of Protective Action

The safety-related instrumentation and controls of the Component Cooling Water System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the Component Cooling Water System are part of the ESFAS and are described in Section 7.3.

7.4.3.3.19 Information Read-Out

Information read-outs related to the operation of the Component Cooling Water System for safety-related functions are provided in the control room.

7.4.3.3.20 System Repair

The Component Cooling Water System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.4.3.3.21 Identification

The Component Cooling Water System safety-related instrumentation and control equipment is physically identified as described in Section 7.1.2.3.

7.4.4 Chemical and Volume Control System Instrumentation and Control

7.4.4.1 Description

The Chemical and Volume Control System (CVCS) maintains a predetermined water level in the pressurizer, provides seal water to the reactor coolant pumps, controls reactor coolant chemistry, and serves as part of the ECCS during accident conditions. The CVCS is discussed in detail in Section 9.3.4.

The CVCS is controlled manually and/or automatically during normal conditions as described in Section 9.3.4. Upon receipt of a safety injection signal, the centrifugal charging pumps are automatically started, the volume control tank and charging line isolation valves are closed, and the suction valves from the refueling water storage tank are opened. A blackout signal automatically starts the boric acid transfer pumps. A containment isolation signal automatically closes the letdown isolation valves and the seal water return isolation valves. Process instrumentation and equipment status indication are provided on the control board to allow the operator to assess CVCS performance. The logic for the CVCS is provided on Figure 7-9.

There are no bypasses capable of preventing the CVCS from performing its safety function; however, in the event system control must be transferred to the Auxiliary Shutdown Complex, all safety signals to the Auxiliary Shutdown Complex controlled components are defeated (refer to Section 7.4.7).

7.4.4.2 Design Bases

The CVCS instrumentation and controls are designed to provide reliable control of the Chemical and Volume Control System under all plant operating conditions. The controls allow for manual/automatic operation of the CVCS under normal conditions with overriding automatic controls to realign the system to a safety mode of operation at the onset of abnormal plant conditions.

7.4.4.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to these controls. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.4.4.3.1 General Functional Requirements

The CVCS instrumentation and controls monitor and provide manual and automatic control of the system during normal plant conditions. Overriding automatic controls align the CVCS to its safety mode of operation in the event of an accident.

7.4.4.3.2 Single Failure Criterion

No single failure of the CVCS instrumentation and controls can prevent the system from performing its required safety function.

7.4.4.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.4.4.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.4.4.3.5 Channel Integrity

The safety-related instrumentation and controls channels for the CVCS are designed to assure system functional capability.

7.4.4.3.6 Channel Independence

The safety related instrumentation and controls of the redundant CVCS trains are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.4.4.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls of the CVCS are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the CVCS are part of the ESFAS and are described in Section 7.3.

7.4.4.3.8 Derivation of System Inputs

Input signals to the CVCS instrumentation and controls are provided by the ESFAS or are derived from direct measurement of the desired variable.

7.4.4.3.9 Capability for Test and Calibration

The CVCS safety-related instrumentation and controls are designed to facilitate testing and calibration as required by the Technical Specifications.

7.4.4.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls of the CVCS are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the CVCS are part of the ESFAS and are described in Section 7.3.

7.4.4.3.11 Operating Bypasses

The train related CVCS instrumentation and controls do not employ operating bypasses in their initiating logic. The protection channels that actuate the CVCS are part of the ESFAS and are described in Section 7.3.

7.4.4.3.12 Indication of Bypasses

Indication is provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either train of the CVCS has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. The ESF bypass indication panel is discussed in Section 7.8.3.

7.4.4.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the CVCS inoperable is controlled by administrative and security measures.

7.4.4.3.14 Multiple Setpoints

Multiple setpoints are not required for the CVCS.

7.4.4.3.15 Completion of Protective Action Once it is Initiated

Once initiated by a protective signal, the CVCS continues to operate until deliberate action is taken by the operator.

7.4.4.3.16 Manual Initiation

The CVCS can be manually initiated from the control room.

7.4.4.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

No protection system setpoints are derived from the CVCS.

7.4.4.3.18 Identification of Protective Action

The safety-related instrumentation and controls of the CVCS are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the CVCS are part of the ESFAS and are described in Section 7.3.

7.4.4.3.19 Information Read-Out

Information read-outs related to the operation of the CVCS for safety-related functions are provided in the control room.

7.4.4.3.20 System Repair

The CVCS is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.4.4.3.21 Identification

The CVCS safety-related instrumentation and control equipment is physically identified as described in Section 7.1.2.3.

7.4.5 Residual Heat Removal System Instrumentation and Controls

7.4.5.1 Description

The Residual Heat Removal (RHR) System transfers heat from the Reactor Coolant System to the Component Cooling Water System during plant cooldown and controls plant temperature during periods of cold shutdown (refer to Section 5.4.7). During accident conditions the RHR system serves as part of the Emergency Core Cooling and Containment Spray Systems (refer to Sections 5.4.7, 6.3, and 6.2.2).

During normal plant operation the RHR System is not inservice and is aligned for operation as a part of the ECCS. In the event of an accident, a safety injection signal automatically starts the RHR pumps in their proper sequence. The safety injection signal also automatically aligns the RHR heat exchanger bypass and outlet valves to provide flow through the heat exchangers. The logic for the RHR pumps and heat exchanger bypass and outlet valves is shown on Figure 7-10.

Two lines connect the suction of the RHR pumps to the Reactor Coolant System (RCS). Two normally closed motor-operated isolation valves are provided in series in each line to isolate the high pressure Reactor Coolant System from the low pressure RHR System. Each of the four isolation valves are separately interlocked to protect the RHR System from overpressurization.

The RHR isolation valves nearest the RCS are prevented from opening when any of the following conditions exist:

1. Reactor Coolant System pressure is above 385.5 psig,
2. Refueling Water Storage Tank isolation valve is open,
3. Containment Sump isolation valve is open,
4. RHR discharge to containment spray isolation valve is open, or

5. RHR supply to the safety injection pumps isolation valve is open

The RHR isolation valves nearest the RHR System are provided the same permissive interlocks as their series counterparts. The pressure interlocks for these isolation valves are derived from sensors of a different process control channel than the interlocks of their series counterparts.

There are no bypasses capable of preventing the RHR system from performing its safety functions; however, in the event system control must be transferred to the Auxiliary Shutdown Complex, all automatic safety actuation signals to the Auxiliary Shutdown Complex controlled components are defeated. The Auxiliary Shutdown Complex is discussed in Section 7.4.7.

RHR System safety related instrumentation and controls are powered from the same train of essential auxiliary power as their associated train of RHR equipment.

7.4.5.2 Design Bases

The Residual Heat Removal System instrumentation and controls are designed to protect the RHR System from overpressurization and assure its ability to perform its required safety function.

7.4.5.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to these controls. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.4.5.3.1 General Functional Requirements

The RHR System instrumentation and controls protect the RHR System from overpressurization and automatically start the system to perform its safety function in the event of an accident.

7.4.5.3.2 Single Failure Criterion

No single failure in the RHR System instrumentation and controls can affect the operation of more than one train of RHR.

7.4.5.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.4.5.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.4.5.3.5 Channel Integrity

The safety-related instrumentation and controls for the redundant trains of RHR are designed to assure system functional capability.

7.4.5.3.6 Channel Independence

The safety-related instrumentation and controls for the redundant RHR trains are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.4.5.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls of the RHR System are train related and do not include protection channels as defined in IEEE 279-1971.

The protection channels that actuate the RHR System are part of the ESFAS and are described in Section 7.3.

7.4.5.3.8 Derivation of System Inputs

Input signals to the RHR System instrumentation and controls are provided by the ESFAS or are derived from direct measurement of the desired variable.

7.4.5.3.9 Capability for Test, Calibration, and Sensor Checks

The RHR System safety-related instrumentation and controls are designed to facilitate testing and calibration as required by the Technical Specifications.

7.4.5.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls of the RHR System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the RHR System are part of the ESFAS and are described in Section 7.3.

7.4.5.3.11 Operating Bypasses

The train related RHR System instrumentation and controls do not employ operating bypasses in their initiating logic. The protection channels that actuate the RHR System are part of the ESFAS and are described in Section 7.3.

7.4.5.3.12 Indication of Bypasses

Indication is provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either train of the RHR System has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. The ESF bypass indication panel is discussed in Section 7.8.3.

7.4.5.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the RHR System inoperable is controlled by administrative and security measures.

7.4.5.3.14 Multiple Setpoints

Multiple setpoints are not required for the RHR System.

7.4.5.3.15 Completion of Protective Action Once it is Initiated

Once initiated by a protective signal, the RHR System continues to operate until deliberate action is taken by the operator.

7.4.5.3.16 Manual Initiation

The RHR System pumps and heat exchanger bypass and outlet valves can be manually operated from the control room.

7.4.5.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

No protection system setpoints are derived from the RHR System.

7.4.5.3.18 Identification of Protective Action

The safety-related instrumentation and controls of the RHR System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the RHR System are part of the ESFAS and are described in Section 7.3.

7.4.5.3.19 Information Read-Out

Information read-outs related to the operation of the RHR System for safety-related functions are provided in the control room.

7.4.5.3.20 System Repair

The RHR System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.4.5.3.21 Identification

The RHR System safety-related instrumentation and control equipment is physically identified as described in Section 7.1.2.3.

7.4.6 Emergency Core Cooling System Instrumentation and Control

The interaction of the various systems that make up the ECCS is discussed in Section 6.3. The instrumentation and controls for the ECCS are discussed in the sections that cover the systems which make up the ECCS:

1. Engineered Safety Features Actuation System (refer to Section 7.3)
2. Residual Heat Removal System Instrumentation and Controls (refer to Section 7.4.5)
3. Cold Leg Accumulator Controls (refer to Section 7.6.3)
4. Refueling Water Tank Interlocks (refer to Section 7.6.5)

7.4.7 Auxiliary Shutdown Control

7.4.7.1 Description

In the event the control room must be evacuated, sufficient instrumentation and controls are provided outside the control room to bring the plant safely to a hot standby condition (Mode 3). Cold shutdown conditions can be reached from outside the control room with some temporary instrumentation and control modification.

The reactor is manually tripped in the control room prior to evacuation; however, the reactor can also be manually tripped at the reactor trip switchgear.

Instrumentation and controls for hot standby from outside the control room are located in the Auxiliary Building on the auxiliary shutdown panels and auxiliary feedwater pump turbine control panel (refer to Figure 1-3). The instrumentation and controls provided on the auxiliary shutdown panels are listed on Table 7-8 and Table 7-9. The instrumentation and controls provided on the auxiliary feedwater pump turbine control panel are listed on Table 7-10.

Selector switches on the auxiliary shutdown panels allow the operator to transfer control of the equipment required for shutdown from the control room to the shutdown panels. When equipment control is transferred to auxiliary shutdown panels, all control room controls and all interlocks that originate or pass through the control room and/or cable room are defeated, except for valves NV148, 294, and 309. These valves have their control room controls defeated manually by procedural guidance using plugs/receptacles in a terminal box prior to using the ASP. The auxiliary shutdown panels are physically and electrically separated from each other and from the control room and cable room. The electrical power that supplies all of the devices controlled from these panels is available following a loss of offsite power. Transfer of control to the shutdown panels is alarmed in the control room.

Plant shutdown in the event of fire or sabotage is addressed in the Fire Plan or Security Plan.

7.4.7.2 Analysis

Hot standby is a stable condition automatically reached following a unit shutdown. The hot standby condition can be safely maintained for an extended period of time. In the event the control room is not accessible, a unit can be kept in hot standby until control room access is restored.

The controls available on the ASP's provide the capabilities of achieving and maintaining hot standby when the control room is inaccessible. The controls provide a means of sustaining the capabilities for boration, supplying steam generator feedwater and RHR, and continuing reactor coolant pump seal injection and/or thermal barrier cooling water flow.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.4.

THIS PAGE LEFT BLANK INTENTIONALLY.

7.5 Safety-Related Display Instrumentation

7.5.1 Description

Section 1.8 provides information concerning the instrumentation provided to the operator to enable him to perform required manual safety functions and to determine the effect of automatic and/or manual actions taken following a reactor trip due to a design basis event.

Table 7-11 lists the information available to the operator for monitoring conditions in the reactor, the Reactor Coolant System, and in the containment and process systems throughout all normal operating conditions of the plant, including anticipated operational occurrences.

Type B and C variable selection is based on the SPDS Critical Safety Functions, which comply with the requirements of NUREG 0737, Supplement 1. The SPDS is provided as an aid to the Control Room operating crew in monitoring the status of the Critical Safety Functions. The Critical Safety Functions monitored are those defined in the Westinghouse Owners Group Critical Safety Function Status Trees. The SPDS provides continuous status, updated at regular intervals, of the Critical Safety Functions as defined in the Emergency Response Guidelines (ERG).

Since these Critical Safety Functions constitute the basis of the Catawba SPDS and the emergency operating procedures, it is Duke Power's position that they should also be identified as the plant safety functions for accident monitoring (i.e., the basis for Type B and C variable selection).

Using the SPDS Critical Safety Functions as the basis for defining the accident monitoring instrumentation incorporates the concept of monitoring the multiple barriers to the release of radioactive material and demonstrates compliance with NUREG 0737, Supplement 1. The Critical Safety Functions monitored are those which assure the integrity of these barriers. The Status Tree provides an explicit, systematic mechanism for organizing the plant data required to evaluate a Critical Safety Function. The prioritization of the Critical Safety Functions is consistent with the concept of multiple barriers to radiation release.

The Critical Safety Functions are:

1. Subcriticality

   The Subcriticality Critical Safety Function (CSF) logic monitors Reactivity Control (NUREG 0737, Supplement 1, (CSF). The subcriticality status tree monitors all of the NUREG 0737, Supplement 1, suggested neutron flux indications as well as rod position and Reactor Protection System (RPS) trip status of the reactor core to assure that it is maintained in a subcritical condition following a successful reactor trip or other shutdown.

2. Core Cooling

   The Core Cooling CSF logic monitors the Core Cooling CSF of NUREG 0737, Supplement 1. The core cooling status tree monitors those variables required by NUREG 0737, Supplement 1, to evaluate the status of fuel clad heat removal.

3. Reactor Coolant System Integrity

   The Reactor Coolant System integrity CSF logic monitors *those variables* required by NUREG 0737, Supplement 1, for RCS Integrity and Radioactivity Control. The RCS integrity CSF logic status tree monitors the pressure-temperature relationship of the Reactor Coolant System with respect to various regions of the pressure-temperature curves.

4. Heat Sink

   The heat sink status tree monitors the ability to transfer energy from the reactor coolant to an ultimate heat sink.

5. Containment

   The containment CSF logic status tree monitors those variables which would indicate Containment Conditions (NUREG 0737, Supplement 1 CSF), status of Radioactivity Control (NUREG 0737, Supplement 1 CSF) in the containment, or a threat to containment integrity.

6. Inventory

   The inventory CSF logic status tree supplements the RCS Integrity CSF logic for indications of a breach in RCS integrity or the existence of off-normal quantities of reactor coolant outside of the primary system.

7.5.2 Inadequate Core Cooling Instrumentation

The Inadequate Core Cooling Monitor (ICCM) is of Westinghouse design. The ICCM system monitors lower vessel level, upper vessel level, loop subcooling margin, core sub-cooling margin and core exit temperature and provides advanced warning of the approach to inadequate core cooling. The ICCM is a redundant two train Nuclear Safety-Related system. The microprocessor-based monitoring trains provide information to the control room operator so that conditions inherent to or leading to Inadequate Core Cooling (ICC) can be recognized and addressed.

The functions addressed by the ICCM are as follows:

1. Assists in detecting loss of level in the core during natural circulation
2. Indicates loss of subcooling margin
3. Assists in detecting presence of a gas bubble or void in the reactor vessel head
4. Assists in the detection of the approach to inadequate core cooling

7.5.2.1 Core Exit Thermocouples (CET)

The incore thermocouples (TC's) are positioned to sense exit coolant temperature for selected fuel assemblies. The output of safety related TC's are routed to the ICCM system.

Additionally, all TC values are displayed on the Plant Computer. The primary display for the Incore Thermocouple System is the ICCM system plasma display in the Control Room. The ICCM system uses the values from the TC's to calculate and display temperatures of the reactor coolant as it exits the core and to provide indication of thermal conditions across the core at the core exit. The Plant Computer, which can be viewed on monitors in the Control Room, acts as backup displays for the Incore Thermocouple System.

7.5.2.2 Subcooling Monitor

The margin to saturation is calculated form Reactor Coolant System pressure and temperature measurements using the Subcooling Margin Monitor (SMM) which is part of the ICCM System.

Averaging of the thermocouple readings and calculation of margin to saturation are performed by the ICCM System. There are two Class 1E trains of SMM which are provided by the ICCM. For each train of the SMM, the average of the five highest value incore thermocouples for that is used to represent core exit conditions for the subcooling margin calculations.

The SMM performs calculations and a comparison to adjusted saturation curves (adjusted for possible measurement uncertainties) to compute margins.

The SMM output consists of a main control plasma display (one per train) which plots plant pressure and temperature in relation to the SMM generated adjusted saturation curve. In addition, numerical values are provided for parameters of interest such as pressure (Reactor Coolant System), temperatures (hot leg), and subcooling margins. Alarm status is indicated by messages on the display.

Analysis

The Catawba subcooling monitor meets the requirements called for in Regulatory Guide 1.97, Rev.2. The subcooling margin is continuously monitored. The SMM which is part of the ICCM is a fully qualified, redundant, Class 1E processor and display. Inputs to the SMM are provided from QA Condition 1 instruments.

7.5.2.3 Reactor Vessel Level Instrumentation System (RVLIS)

ICCM (RVLIS) is designed to monitor and detect a "void", with the NC Pumps running, in the reactor vessel. It is also used to accurately identify the amount of liquid coolant level in the vessel, with NC Pumps not running, during normal and accident conditions.

RVLIS has three ranges of transmitters: upper plenum, lower range and wide range. The upper plenum and lower range level is a level measurement over a specific height of the vessel, when no NC Pumps running. The wide range channels indicate a differential pressure across the Reactor Vessel, with the NC Pumps running. The system instrumentation permits vessel level measurement from the bottom to the top of the reactor vessel.

This is a two train system containing Trains A and B which are physically separate and electrically isolated from eachother. The trains perform the same function using identical but redundant inputs for differential pressure transmitters, impulse line temperature sensors, reactor coolant temperature sensors and wide range reactor coolant system pressure.

Software algorithms automatically perform compensation calculations required for variations in impulse line temperatures. Software also calculates and provides the necessary compensation for reactor coolant density.

The Train A measurements are recorded on a continuous recorder in the Control Room.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.5.

THIS PAGE LEFT BLANK INTENTIONALLY

7.6 All Other Systems Required for Safety

This section includes a description of those instrumentation and control systems required for safety which have not been discussed in Sections 7.2 through 7.5.

IEEE 279-1971 establishes the specific design basis information required for the protection systems of nuclear power stations. The following addresses each of these design bases as they apply to the systems discussed in Section 7.6.

Section 1.8, Item II.F.1, evaluates compliance of Catawba Nuclear Station with NUREG 0737, Supplement 1, and NRC Regulatory Guide 1.97, Revision 2. Table 1-11 provides a comparison of plant specific accident monitoring variables with the recommendations of Regulatory Guide 1.97, Revision 2.

1. Conditions Requiring Protective Action

   The generating station conditions that require protective action are addressed in the subsections of 7.6 in which the individual systems are discussed. Additional discussions of these systems are provided in Chapter 6, Chapter 9, and Chapter 11.

2. Variables Monitored to Provide Protective Action

   The generating station variables monitored to provide protective action are addressed in the subsections of Section 7.6 in which the individual systems are discussed.

3. Sensors for Spatially Dependent Variables

   There are no spatially dependent variables associated with the safety functions performed by the systems in this section.

4. Operational Limits, Margins, and Levels Requiring Protective Action

   Prudent operational limits, available margins, and setpoints before the onset of unsafe conditions requiring protective action are discussed in Chapter 15 and the Technical Specifications.

5. Range of Transient and Steady-State Conditions

   The range of energy supply and environmental conditions during normal, abnormal, and accident conditions are provided in Sections 8.3 and 3.11, respectively.

6. Events Which Could Damage or Degrade Systems

   Events that could damage or degrade system components are analyzed and discussed in the High Energy Line Break Analysis, and the seismic and environmental qualification sections (Sections 3.10 and 3.11) of the FSAR.

7. Minimum Performance Requirements

   The minimum performance requirements for critical variables that initiate or control system safety functions are discussed in Chapter 15 the Technical Specifications.

7.6.1 Instrumentation and Control Power Supply System

Refer to Sections 8.3.2.1.2.1 and 8.3.2.2 for a description of this ESF Support System.

7.6.2 Deleted Per 2012 Update

7.6.3 Cold-Leg Accumulator Motor-Operated Isolation Valves

7.6.3.1 Description

Separate Safety Injection System accumulators are provided to inject borated water into the cold leg of each reactor coolant loop. These four accumulators are filled with dilute boric acid and are pressurized with nitrogen. The contents of the accumulators are injected into the Reactor Coolant System if reactor coolant pressure decreases below the accumulator pressure. Injection from only three of the four accumulators is required to partially cover the reactor core. The Safety Injection System and the function of these accumulators are described in detail in Chapter 6.

During normal power operation each accumulator is isolated from the Reactor Coolant System by two series check valves in the accumulator injection line.

For each accumulator, a single motor-operated valve is provided upstream of the isolation check valves. The motor-operated isolation valves are normally open.

Two position pushbuttons are provided on the main control board for manual control of each accumulator isolation valve. The controls for each isolation valve are interlocked such that:

1. An open accumulator isolation valve cannot be closed when a safety injection "S" signal is present.
2. A closed accumulator isolation valve automatically opens upon receipt of a safety injection "S" signal regardless of the valve control switch position.
3. A closed accumulator isolation valve automatically opens when reactor coolant pressure exceeds the safety injection unblock pressure (P-11).

An annunciator alarm is provided in the control room for each Accumulator Isolation Valve to alert the operator of an Accumulator Isolation Valve not in the fully opened position when the reactor coolant pressure is above the safety injection unblock pressure. To remind the operator of this abnormal alignment, this annunciator alarm, “Accumulator Isolation Not Fully Opened”, is repeated at a predetermined time interval until the valve is opened or the reactor coolant pressure falls below the safety injection unblock pressure. This annunciator only functions when the associated valve breaker is closed. There are also two separate monitor lights for each Accumulator Isolation Valve that indicate “Accumulator Isolation Valve Not Open”, and “Accumulator Isolation Valve Closed”. The “Not Open” monitor light is fed from an external stem mounted limit switch, and the “Closed” monitor light is fed from motor operator limit switch contacts. Both monitor lights function regardless of associated valve breaker position.

The control and alarm logic for the cold leg accumulator isolation valves is shown on Figure 7-13.

During normal power operation the accumulator isolation valves are placed in their safety position and the circuit breakers are opened to prevent inadvertent valve closure. The accumulator isolation valve annunciators will not alarm with the accumulator isolation valves de-energized. The “Not Open” monitor light, however, serves as the position indication for surveillance purposes while the valve circuits are unpowered. The valves are closed during plant shutdown, and the valve circuit breakers are opened to prevent inadvertent accumulator injection. Administrative controls assure that the valves and circuit breakers are positioned at the appropriate times.

Control power for the accumulator isolation valves is from the same source as the valves' motor power.

7.6.3.2 Design Bases

The controls and interlocks for the cold leg accumulator isolation valves assure that the accumulators are connected to the Reactor Coolant System in the event they are required for emergency core cooling.

The signals provided to the accumulator valve control circuits are from the ESFAS and are discussed in Section 7.3.

7.6.3.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to these controls. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279-1971, Section 4, is provided below.

7.6.3.3.1 General Functional Requirements

The accumulator isolation valve instrumentation and controls ensure the availability of the cold leg accumulators for emergency core cooling.

7.6.3.3.2 Single Failure Criterion

No single failure in the control circuits for the accumulator isolation valves can prevent the proper operation of more than one cold leg accumulator.

7.6.3.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.3.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.3.3.5 Channel Integrity

Accumulator isolation valve controls are designed to assure functional capability.

7.6.3.3.6 Channel Independence

The safety-related instrumentation and controls of the cold leg accumulator motor operated isolation valves are physically separated and electrically isolated as discussed in Section 8.3.1.4 to assure independence between accumulators.

7.6.3.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls for the cold leg accumulator isolation valves are train related and do not include protection channels as defined in IEEE 279-1971. The

protection channels that actuate safety injection are part of the ESFAS and are described in Section 7.3.

7.6.3.3.8 Derivation of System Inputs

Inputs signals to the accumulator isolation valve controls are provided by the ESFAS or are derived from signals that are direct measures of the desired system variables.

7.6.3.3.9 Capability for Test, Calibration, and Sensor Checks

The cold leg accumulator motor operated isolation valves safety-related instrumentation and controls are designed to facilitate testing and calibration.

7.6.3.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls for the cold leg accumulator motor operated isolation valves are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate safety injection are part of the ESFAS and are discussed in Section 7.3.

7.6.3.3.11 Operating Bypasses

The instrumentation and controls for the cold leg accumulator isolation valves do not employ operating bypasses in their initiating logic. The protection channels that actuate safety injection are part of the ESFAS and are described in Section 7.3.

7.6.3.3.12 Indication of Bypasses

Indication is provided on the OAC 1.47 Bypass Panel Graphics Displays in the control room when either train of the Refueling Water System has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. The ESF bypass indication panel is discussed in Section 7.8.3.

7.6.3.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the cold leg accumulator motor operated isolation valves inoperable is controlled by administrative and security measures.

7.6.3.3.14 Multiple Setpoints

Multiple setpoints are not required for the cold leg accumulator isolation valves.

7.6.3.3.15 Completion of Protective Action Once it is Initiated

The cold leg accumulator isolation valves are normally open, but are also given an open signal by the ESFAS as a precautionary measure. Once the valve controls have received a safety injection signal, they will remain in the open position to allow accumulator injection until they are manually closed by the operator after the safety injection signal is reset. The accumulator isolation valves are only closed during unit shutdown.

7.6.3.3.16 Manual Initiation

The cold leg accumulator isolation valves can be manually operated from the control room.

7.6.3.3.17 Access to Setpoint Adjustments, Calibration, and Test Point s

No protection system setpoints are derived from the cold leg accumulators or their isolation valves.

7.6.3.3.18 Identification of Protective Action

The safety-related instrumentation and controls for the cold leg accumulator isolation valves are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate safety injection are part of the ESFAS and are described in Section 7.3.

7.6.3.3.19 Information Read-Out

Information read-outs related to the operation of the cold leg accumulator isolation valves are provided in the control room.

7.6.3.3.20 System Repair

The Safety Injection System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.3.3.21 Identification

The safety-related instrumentation and control equipment for the cold leg accumulator isolation valves is physically identified as described in Section 7.1.2.3.

7.6.4 Containment Pressure Control System

7.6.4.1 Description

As described in Chapter 6 and Section 7.3, certain engineered safety features (i.e., Containment Spray System) are provided to prevent overpressurizing the Containment in the event of a LOCA. The Containment Pressure Control System (CPCS) is provided to prevent excessive depressurization of the Containment through inadvertent or excessive operation of these engineered safety features.

The CPCS allows operation of the Containment Spray System only when it is required for reducing Containment pressure and inhibits their operation when not required for containment protection.

The CPCS is designed for operation over a pressure range of -5 to +60 psig. For accuracy, the containment pressure sensors are designed to respond to the reduced range of -0.5 to +1.5 psig, though not adversely affected by pressure transients up to 60 psig. The CPCS is designed such that it does not affect the accuracy, margin, or response of the ESFAS as the permissive setpoint is below the ESFAS setpoint for high containment pressure. Initiation of these engineered safety features is discussed in Section 7.3.

The system permissive and terminate features of the redundant Containment Pressure Control System are provided by eight independent pressure sensors (four per train). These pressure sensors interlock the controls of the Containment Spray System and the Containment Air Return Fans to prevent operation when containment pressure is below approximately 0.25 psig. The CPCS control logic is presented in Figure 7-14.

Electrical power to each train of CPCS is supplied by a Safety-Related power source. The CPCS permissives for the NS containment spray valves and VX air return dampers, are supplied from uninterruptible Safety-Related power sources. The CPCS permissives for the NS pumps and VX air return fan motors are supplied on load group 11 of Safety-Related power.

7.6.4.2 Design Bases

The CPCS instrumentation and controls are designed to protect the Containment from negative pressure by preventing inadvertent or excessive operation of Containment pressure reducing systems and equipment.

7.6.4.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to these controls. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below.

7.6.4.3.1 General Functional Requirement

The CPCS functions reliably and automatically to prevent inadvertent or excessive operation of engineered safety features that could result in a negative pressure in the Containment.

7.6.4.3.2 Single Failure Criterion

Controls for the CPCS are designed such that a single failure can neither permit operation of any train of the Containment Spray System or the Containment Air Return Fan System when Containment pressure is below 0.25 psig, nor can it prevent the operation of more than one train in each of these systems when containment pressure is above 1.00 psig. The single failure criterion is met by assuring physical and electrical separation between the redundant trains.

7.6.4.3.3 Quality of Components

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.4.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.4.3.5 Channel Integrity

The redundant trains of safety-related controls for the CPCS are designed to assure system functional capability.

7.6.4.3.6 Channel Independence

The safety-related instrumentation and controls for the CPCS are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.6.4.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls of the CPCS are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.4.3.8 Derivation of System Inputs

The inputs to the Containment Pressure Control System are derived from direct measurements of containment pressure.

7.6.4.3.9 Capability for Test, Calibration, and Sensor Checks

The CPCS safety-related instrumentation and controls are designed to facilitate testing and calibration as required by the Technical Specifications.

The CPCS can be tested during power operation by connecting a test meter to the containment pressure sensor output and cross checking it with the installed containment pressure indication.

7.6.4.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls of the CPCS are train related and do not include protection channels as defined in IEEE 279-1971.

System redundancy is reduced when the CPCS is tested; however, testing is only a short period during the periodic test of the ESFAS, and is automatically indicated on the OAC 1.47 Bypass Panel Graphic Displays in the control room. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell.

7.6.4.3.11 Operating Bypasses

The CPCS instrumentation and controls do not employ operating bypasses in their initiating logic.

7.6.4.3.12 Indication of Bypass

Indication is provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either train of the Containment Spray or Containment Air Return Fan System has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. The ESF bypass indication panel is discussed in Section 7.8.3.

7.6.4.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the CPCS inoperable is controlled by administrative and security measures.

7.6.4.3.14 Multiple Setpoints

Multiple setpoints are not required for the Containment Pressure Control System.

7.6.4.3.15 Completion of Protective Action Once it is Initiated

Once initiated the Containment Pressure Control System continues to block the operation of the Containment Spray System and the Containment Air Return Fan System until containment pressure increases above approximately 1.00 psig. The inhibit signal automatically clears when containment pressure increases above the 0.35 psig setpoint.

7.6.4.3.16 Manual Initiation

Operation of the containment spray system and containment air return fan system can be manually terminated from the control room.

7.6.4.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points is controlled by administrative and security measures.

7.6.4.3.18 Identification of Protective Action

The safety-related instrumentation and controls of the CPCS are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.4.3.19 Information Read-Out

Indication of the permissive/inhibit status of the Containment Pressure Control System is provided in the control room. Control room annunciators alarm loss of power to the CPCS.

7.6.4.3.20 System Repair

The CPCS is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.4.3.21 Identification

The CPCS safety-related instrumentation and control equipment is physically identified as described in Section 7.1.2.3.

7.6.5 Refueling Water System Instrumentation and Switchover From Safety Injection to Recirculation Mode

7.6.5.1 Description

The Refueling Water System provides borated water for use during refueling and during a postulated loss-of-coolant accident (LOCA). The Refueling Water System is discussed in Section 9.2.7.

The Refueling Water System is manually controlled by the operator under normal conditions. On receipt of an ESFAS signal, the system is automatically realigned to isolate the Refueling Water Storage Tank (RWST) from all other systems except the emergency core cooling systems.

Four wide range level channels and two narrow range instruments loops monitor the level in the RWST and one wide range channel provides a pre lo level level, lo level alarm, or lo-lo level alarm. Either one of the two narrow range instrument loops provides a high level alarm and make up level alarm. Also, a low level is sensed by two of the four wide range level channels and initiates an alarm in the control room. A lo RWST level coincident with a safety injection signal automatically initiates realignment of the ECCS to the recirculation mode after a LOCA by opening containment sump isolation valves and isolating the RWST. Then a position switch, indicating that the sump isolation valve is full open, will automatically initiate closure of the RHR/RWST isolation valves [FW27A and FW55B]. This realignment is referred to as switchover from the safety injection mode to the recirculation mode after a LOCA. The safety injection

signal is initiated by the contact of a slave relay in the Solid State Protection System output cabinet that picks up [actuates] on safety injection and remains latched in until manually reset by the sump valve automatic open circuit reset switch. This reset switch is separate from the main systems level safety injection reset switch. Reset of the systems level safety injection signal will not reset or block the safety injection function which in coincidence with the lo RWST level signal will initiate switchover to the recirculation mode. The purpose of the sump valve automatic open circuit reset switch is to permit the operator to unlatch the slave relay which was latched by a safety injection signal in the event the corresponding sump isolation valve must be closed and retained in a closed position following a LOCA, such as, for maintenance purposes. These functions are shown on Figure 7-15 and Figure 7-16. The sump valve automatic open circuit reset switch is shown on Figure 7-16. A control board installed reset light is located near this reset switch to indicate when the aforementioned slave relay is unlatched. As shown on Figure 7-15, the RWST level channel bistables from the Protection System are normally de-energized. The trip signal is provided when energized. Thus, loss of power will not cause an inadvertent trip. Realignment to recirculation is further discussed in Section 6.3.2.8. RWST level instruments also provide control room indication of RWST level.

Four 30 KW heater clusters, two per group, are provided to maintain RWST temperature above 70°F. When the refueling water temperature decreases to 75°F, one heater cluster in each group is automatically energized. Should the water temperature continue to decrease, the remaining heater cluster in each group is energized when the temperature reaches 72°F. Indication of refueling water temperature is provided in the control room.

7.6.5.2 Design Bases

The Refueling Water System instrumentation and controls are designed to provide reliable manual and automatic system control under normal operating conditions, and overriding automatic controls to align the system to its safety mode during accident conditions.

7.6.5.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to these controls. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.6.5.3.1 General Functional Requirements

The Refueling Water System safety-related instrumentation and controls monitor and provide manual and automatic control of the Refueling Water System.

7.6.5.3.2 Single Failure Criterion

No single failure in the Refueling Water System safety-related instrumentation and controls can prevent the system from performing its required safety function.

7.6.5.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.5.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.5.3.5 Channel Integrity

The redundant trains of the Refueling Water System safety-related instrumentation and controls are designed to assure system functional capability.

7.6.5.3.6 Channel Independence

The redundant trains of the Refueling Water System safety-related instrumentation and controls are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.6.5.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls for the Refueling Water System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the Refueling Water System are part of the ESFAS and are described in Section 7.3.

7.6.5.3.8 Derivation of Inputs

Input signals to the Refueling Water System instrumentation and control are provided by the ESFAS and are from direct measurements of the desired variables.

7.6.5.3.9 Capability for Test, Calibration, and Sensor Checks

The Refueling Water System safety-related instrumentation and controls are designed to facilitate testing and calibration as required by the Selected Licensee Commitments.

7.6.5.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls for the Refueling Water System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the Refueling Water System are part of the ESFAS and are described in Section 7.3.

7.6.5.3.11 Operating Bypasses

The Refueling Water System instrumentation and controls do not employ operating bypasses in their initiating logic. The protection channels that actuate the Refueling Water System are part of the ESFAS and are described in Section 7.3.

7.6.5.3.12 Indication of Bypass

Indication is provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either train of the Refueling Water System has been made inoperable at the system level. The refueling water valves (FW27A & FW55B) provide the input to the OAC 1.47 Bypass Panel Graphic Displays as ND Train A (B) bypassed or NS Train A (B) bypassed. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. The ESF bypass indication panel is discussed in Section 7.8.3.

7.6.5.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the Refueling Water System inoperable is controlled by administrative and security measures.

7.6.5.3.14 Multiple Setpoints

Multiple setpoints are not required for the Refueling Water System.

7.6.5.3.15 Completion of Protective Action Once it is Initiated

Once initiated by a protective signal, the Refueling Water System continues to perform its safety function until deliberate action is taken by the operator.

7.6.5.3.16 Manual Initiation

The Refueling Water System can be manually operated from the control room.

7.6.5.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points is controlled by administrative and security measures.

7.6.5.3.18 Identification of Protective Action

The safety-related instrumentation and controls for the Refueling Water System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the Refueling Water System are part of the ESFAS and are described in Section 7.3.

7.6.5.3.19 Information Read-Out

Refueling water storage tank levels are provided in the control room.

7.6.5.3.20 System Repair

The Refueling Water System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.5.3.21 Identification

The safety-related instrumentation and control equipment for the Refueling Water System is physically identified as described in Section 7.1.2.3.

7.6.6 Liquid Radwaste System

7.6.6.1 Description

The Liquid Radwaste System collects, segregates, and processes all radioactive and potentially radioactive liquids generated in the plant. This system is described in detail in Section 11.2.

The safety-related instrumentation and controls for the Liquid Radwaste System monitor sump levels and control the sump pumps in the containment spray and residual heat removal (RHR) pump room sump and in the auxiliary feedwater pump pit sumps. Level instrumentation in each

of these sumps automatically controls the sump pumps to regulate sump level and provides a remote level alarm in the event the sump level exceeds a predetermined value.

Each of the two motor-driven auxiliary feedwater pump pit sumps are provided with a single sump pump powered from the same train of Class 1E power as the associated auxiliary feedwater pump. The level instruments in these sumps automatically start their associated sump pump on a high sump level and stop the pump at a predetermined low sump level. Manual controls for these sump pumps are provided locally at the sumps.

The turbine-driven auxiliary feedwater pump pit sump is provided with two sump pumps powered from separate trains of Class 1E power. Sump level instruments start the lead pump on a high sump level, and the backup pump on high-high sump level. When the sump has been pumped down to a predetermined low level, the level instrumentation stops both pumps. A manual selector switch allows the operator to equalize pump run times by periodically alternating the selection of which pump will operate as the lead and which as the backup pump. Manual controls for these pumps are provided locally at the sump.

The containment spray and residual heat removal pump room sump is common to both units and is provided with four sump pumps: two pumps powered from separate trains of Unit 1 Class 1E power and two pumps powered from separate trains of Unit 2 Class 1E power. The pumps of one unit operate independently as though there are no pumps provided from the opposite unit. For a given unit, sump level instrumentation starts the unit's lead pump on a high sump level, and the unit's backup pump on high-high sump level. When the sump has been pumped down to a predetermined low level, the unit's level instrumentation stops both of the associated sump pumps. Manual selector switches allow the operators to equalize pump run times by periodically alternating the selection of which pumps will operate as the lead and which as the backup pumps. Manual controls for these pumps are provided in the associated unit control room.

The safety-related instrumentation and controls of the Liquid Radwaste System are powered from the Essential Auxiliary Power System.

7.6.6.2 Design Bases

The safety-related instrumentation and controls of the Liquid Radwaste System are designed to provide reliable indication of safety related sump levels and continuous automatic control sump pump operation to maintain sump levels within design limits.

7.6.6.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of the standard; therefore, these requirements are not directly applicable to the controls of this ESF support system. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.6.6.3.1 General Functional Requirements

The Liquid Radwaste System safety-related instrumentation and controls automatically control safety related sump levels to protect essential equipment from flooding.

7.6.6.3.2 Single Failure Criterion

These instrumentation and controls are designed such that no single failure within the system can prevent proper action at the system level.

Instrumentation and controls for the motor-driven auxiliary feedwater pump sumps are completely independent and are powered from the same train of Class 1E power as their associated auxiliary feedwater pump and sump pump. Any single failure could affect only one train.

Two redundant and independent trains of sump level instrumentation and controls are provided for the turbine-driven auxiliary feedwater pump pit sump and the containment spray and residual heat removal pump room sump. Any single failure could affect only one train.

7.6.6.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.6.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.6.3.5 Channel Integrity

The redundant trains of safety-related instrumentation and controls of the Liquid Radwaste System are designed to assure system functional capability.

7.6.6.3.6 Channel Independence

Redundant trains of safety-related instrumentation and controls are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.6.6.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls for the Liquid Radwaste System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.6.3.8 Derivation of System Inputs

The inputs to these safety-related instrumentation and controls are derived from direct sump level measurements.

7.6.6.3.9 Capability for Test, Calibration, and Sensor Checks

The Liquid Radwaste System safety-related instrumentation and controls are designed to facilitate testing and calibration as required by the Selected Licensee Commitments.

7.6.6.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls for the Liquid Radwaste System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.6.3.11 Operating Bypasses

The Liquid Radwaste System instrumentation and controls do not employ operating bypasses in their initiating logic.

7.6.6.3.12 Indication of Bypass

No system level ESF bypass indication is required for the Liquid Radwaste System per Table 7-14. The ESF bypass indication panel is discussed in Section 7.8.3.

7.6.6.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the Liquid Radwaste System inoperable is controlled by administrative and security measures.

7.6.6.3.14 Multiple Setpoints

Multiple setpoints are not required for the Liquid Radwaste System.

7.6.6.3.15 Completion of Protective Action Once it is Initiated

The redundant trains of the Liquid Radwaste System will continue to operate until the conditions requiring operation have been eliminated.

7.6.6.3.16 Manual Initiation

Manual controls are provided for the Liquid Radwaste System as described in Section 7.6.6.1.

7.6.6.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points is administratively controlled.

7.6.6.3.18 Identification of Protective Action

The safety-related instrumentation and controls of the Liquid Radwaste System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.6.3.19 Information Read-Out

Information read-outs related to the operation of the Liquid Radwaste System for safety-related functions are provided in the control room.

7.6.6.3.20 System Repair

The Liquid Radwaste System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.6.3.21 Identification

The safety-related instrumentation and control equipment of the Liquid Radwaste System is physically identified as described in Section 7.1.2.3.

7.6.7 Diesel Generator Room Sump Pump System

7.6.7.1 Description

The Diesel Generator Room Sump Pump System removes leakage and equipment drainage from the diesel rooms. In the event of a major pipe rupture in a diesel room, this system protects the diesel generators from flooding. The Diesel Generator Room Sump Pump System is discussed in detail in Section 9.5.9.

Each diesel room has a sump with two sump pumps. For each sump, level instrumentation starts the lead sump pump on high sump level and the backup pump on high-high sump level. When the sump has been pumped down to a predetermined low level, the level instrumentation stops both pumps. The pumps are automatically sequenced to alternate starting in the normal mode of operation. A manual selector switch allows the operator to equalize pump run times by periodically alternating the selection of the lead and backup pump. Manual controls for these pumps are provided locally at the sump.

An alarm for high-high sump level is provided at the associated diesel control panel and in the control room.

The safety-related instrumentation and controls for the Diesel Generator Room Sump Pump System are powered from the Essential Auxiliary Power System.

7.6.7.2 Design Bases

The safety-related instrumentation and controls for the Diesel Generator Room Sump Pump System are designed to provide continuous automatic control of the diesel room sump pumps to maintain the sump levels within design limits.

7.6.7.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to the controls of this ESF support system. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.6.7.3.1 General Functional Requirements

The Diesel Generator Room Sump Pump System instrumentation and controls automatically control diesel room sump pump operation to protect essential equipment from flooding.

7.6.7.3.2 Single Failure Criterion

These instrumentation and controls are designed such that no single failure can prevent proper action at the system level. A single failure in the sump pump controls of one diesel room can only affect the diesel equipment in that room.

7.6.7.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.7.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.7.3.5 Channel Integrity

The redundant trains of diesel room sump pump instrumentation and controls are designed to assure system functional capability.

7.6.7.3.6 Channel Independence

The safety-related instrumentation and controls of the redundant diesel generator room sump pump trains are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.6.7.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls for the diesel generator room sump pump system are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.7.3.8 Derivation of System Inputs

The input signals to these safety-related controls are derived from direct measurement of diesel room sump level.

7.6.7.3.9 Capability for Test, Calibration, and Sensor Checks

The diesel generator room sump pump system safety-related instrumentation and controls are designed to facilitate testing and calibration.

7.6.7.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls for the diesel generator room sump pumps are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.7.3.11 Operating Bypasses

The diesel generator room sump pump instrumentation and controls do not employ operating bypasses in their initiating logic.

7.6.7.3.12 Indication of Bypass

Indication is provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either safety train has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. The ESF bypass indication panel is discussed in Section 7.8.3.

7.6.7.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the diesel generator room sump pumps inoperable is controlled by administrative and security measures.

7.6.7.3.14 Multiple Setpoints

Multiple setpoints are not required for the diesel generator room sump pump controls.

7.6.7.3.15 Completion of Protective Action Once it is Initiated

The diesel generator room sump pumps will continue to operate until the conditions requiring their operation have been eliminated.

7.6.7.3.16 Manual Initiation

Provisions for manual operation of the diesel room sump pumps are provided locally in the diesel rooms.

7.6.7.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points is controlled by administrative measures.

7.6.7.3.18 Identification of Protective Action

The safety-related instrumentation and controls for the diesel generator room sump pumps are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.7.3.19 Information Read-Out

Information read-outs to monitor the operation of the diesel generator room sump pump system are provided in the control room.

7.6.7.3.20 System Repair

The diesel generator room sump pump system is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.7.3.21 Identification

The safety-related instrumentation and control equipment of the diesel generator room sump pump system is physically identified as described in Section 7.1.2.3.

7.6.8 Diesel Building Ventilation System Instrumentation and Controls

7.6.8.1 Description

The Diesel Building Ventilation System automatically maintains a suitable environment for the operation of equipment in the Diesel Building. This system is discussed in detail in Section 9.4.4.

Safety-related instrumentation and controls serve the emergency ventilation subsystem of the Diesel Building Ventilation System. The fans in the emergency ventilation subsystem start automatically when the diesel starts. Diesel starting also actuates the automatic return air and outdoor air dampers. Once actuated the dampers are thermostatically regulated to maintain Diesel Building temperature within the design range. When the diesel is shutdown, the emergency ventilation subsystem dampers and fans are automatically shutdown.

The Diesel Building Ventilation System is automatically shutdown on receipt of a fire protection signal.

The safety-related instrumentation and controls of the Diesel Building Ventilation System are powered from the Essential Auxiliary Power System.

7.6.8.2 Design Bases

The safety-related instrumentation and controls of the Diesel Building Ventilation System automatically controls the emergency ventilation subsystem to maintain the Diesel Building temperature within the design range.

7.6.8.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of the standard; therefore, these requirements are not directly applicable to the controls of this ESF support system. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.6.8.3.1 General Functional Requirements

The Diesel Building Ventilation System safety-related instrumentation and controls automatically control the operation of the Diesel Building Ventilation System to maintain a suitable operating environment for the diesel generators.

7.6.8.3.2 Single Failure Criterion

Safety-related instrumentation and controls for the Diesel Building Ventilation System are designed such that no single failure can affect the ventilation of more than one diesel room. A single failure can not prevent proper action at the system level.

7.6.8.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.8.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.8.3.5 Channel Integrity

The redundant trains of safety-related instrumentation and controls for the Diesel Building Ventilation System are designed to assure system functional capability.

7.6.8.3.6 Channel Independence

Redundant trains of Diesel Building Ventilation System safety-related instrumentation and controls are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.6.8.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls of the Diesel Building Ventilation System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate diesel building ventilation are part of the ESFAS and are described in Section 7.3.

7.6.8.3.8 Derivation of System Inputs

Inputs to the Diesel Building Ventilation System safety-related instrumentation and controls are derived from signals that are direct measurements of the desired variables or are provided by the ESFAS.

7.6.8.3.9 Capability for Test, Calibration, and Sensor Checks

The Diesel Building Ventilation System safety-related instrumentation and controls are designed to facilitate testing and calibration.

7.6.8.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls for the Diesel Building Ventilation System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate diesel building ventilation are part of the ESFAS and are described in Section 7.3.

7.6.8.3.11 Operating Bypasses

The Diesel Building Ventilation System instrumentation and controls do not employ operating bypasses in their initiating logic. The protection channels that actuate the system are part of the ESFAS and are described in Section 7.3.

7.6.8.3.12 Indication of Bypass

Indication is provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either train of safety injection has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. The ESF bypass indication panel is discussed in Section 7.8.3.

7.6.8.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the Diesel Building Ventilation System inoperable is controlled by administrative and security measures.

7.6.8.3.14 Multiple Setpoints

Multiple setpoints are not required for the Diesel Building Ventilation System.

7.6.8.3.15 Completion of Protective Action Once it is Initiated

Once initiated by a protective signal, the Diesel Building Ventilation System continues to perform its safety function as long as required, or until a fire protection signal is initiated.

7.6.8.3.16 Manual Initiation

Provisions for manually initiating the Diesel Building Ventilation System emergency ventilation subsystem are provided in the diesel room.

7.6.8.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points is controlled by administrative measures.

7.6.8.3.18 Identification of Protective Action

The safety-related instrumentation and controls of the Diesel Building Ventilation System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate Diesel Building ventilation are part of the ESFAS and are described in Section 7.3.

7.6.8.3.19 Information Read-Out Temperature

Indication and alarms are provided in the diesel room to monitor the safety-related operation of the Diesel Building Ventilation System. Temperature alarms are reflashed to the control room.

7.6.8.3.20 System Repair

The Diesel Building Ventilation System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.8.3.21 Identification

The safety-related instrumentation and control equipment of the Diesel Building Ventilation System is physically identified as described in Section 7.1.2.3.

7.6.9 Groundwater Drainage System Instrumentation and Control

7.6.9.1 Description

The safety-related portion of the Groundwater Drainage System consists of three sumps in the Auxiliary Building that are maintained below a design liquid level to minimize hydrostatic pressure. The Groundwater Drainage System is discussed further in Section 9.5.11.

Each of the three Auxiliary Building sumps is provided with two sump pumps powered from separate trains of Class 1E power. Unit 1 supplies power to both pumps in one sump, unit 2 supplies power to both pumps in another sump, and each unit supplies one pump in the remaining sump.

Separate and independent level instrumentation is provided for each pump. In a given sump the level instruments start the lead pump on high sump level and the backup pump on high-high sump level. When the sump has been pumped down to a predetermined low level, the level instrumentation stops both pumps. A manual selector switch allows the operator to equalize pump run times by periodically alternating the selection of the lead and backup pump. Manual controls for these pumps are provided locally near the sump. Operation of the groundwater drainage sump pumps is monitored by the plant computers.

The Groundwater Drainage System safety-related instrumentation and controls are powered from the Essential Auxiliary Power System.

7.6.9.2 Design Bases

The safety-related instrumentation and controls of the Groundwater Drainage System are designed to protect the integrity of the Auxiliary Building by minimizing hydrostatic pressure.

7.6.9.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to the controls of this ESF support system. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below.

7.6.9.3.1 General Functional Requirements

The Groundwater Drainage System safety related instrumentation and controls automatically control the operation of the Auxiliary Building sump pumps to protect the building from excessive hydrostatic pressure.

7.6.9.3.2 Single Failure Criterion

This instrumentation and control system is designed such that no single failure can prevent the automatic control of the Auxiliary Building safety-related sump levels.

7.6.9.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.9.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.9.3.5 Channel Integrity

The redundant trains of the safety-related Groundwater Drainage System instrumentation and controls are designed to assure system functional capability.

7.6.9.3.6 Channel Independence

Redundant trains of safety-related Groundwater Drainage System instrumentation and controls are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.6.9.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls of the Groundwater Drainage System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.9.3.8 Derivation of System Inputs

The input signals to this instrumentation and control system are derived from direct measurements of groundwater drainage sump levels.

7.6.9.3.9 Capability for Test, Calibration, and Sensor Checks

The Groundwater Drainage System safety-related instrumentation and controls are designed to facilitate testing and calibration as required by Selected Licensee Commitments.

7.6.9.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls for the Groundwater Drainage System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.9.3.11 Operating Bypasses

The Groundwater Drainage System instrumentation and controls do not employ operating bypasses in their initiating logic.

7.6.9.3.12 Indication of Bypass

Indication is provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either train of groundwater drainage has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. The ESF bypass indication panel is discussed in Section 7.8.3.

7.6.9.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the Groundwater Drainage System inoperable is controlled by administrative and security measures.

7.6.9.3.14 Multiple Setpoints

Multiple setpoints are not required for the Groundwater Drainage System.

7.6.9.3.15 Completion of Protective Action Once it is Initiated

The groundwater drainage sump pumps will continue to operate until the condition requiring their operation has been eliminated.

7.6.9.3.16 Manual Initiation

The groundwater drainage sump pumps can be manually operated locally in the Auxiliary Building.

7.6.9.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points is controlled by administrative measures.

7.6.9.3.18 Identification of Protective Action

The safety-related instrumentation and controls for the Groundwater Drainage System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.9.3.19 Information Read-Out

Information read-outs are provided in the control room to monitor the operation of the Groundwater Drainage System.

7.6.9.3.20 System Repair

The Groundwater Drainage System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.9.3.21 Identification

The safety-related instrumentation and control equipment of the Groundwater Drainage System is physically identified as described in Section 7.1.2.3.

7.6.10 Containment Air Return, Hydrogen Skimmer and Hydrogen Recombiner System

7.6.10.1 Description

The containment air return fans provide for the rapid return of air to the lower containment after the initial LOCA blowdown. The hydrogen skimmer system fans prevent hydrogen pocketing in closed containment spaces. ESFAS actuates the air return and hydrogen skimmers automatically upon receipt of an Sp signal. Permissives from the containment pressure control system, described in Section 7.6.4, must also be present for automatic operation of the air return fans and isolation dampers. The two trains of the air return and hydrogen skimmer are redundant.

The hydrogen recombiner system consists of two independent and redundant recombiner units, with associated banks of electric heaters and controls. A two position maintained switch is provided for each recombiner unit to energize the recombiner heaters manually from their local control panels. Hydrogen generation is only a risk during beyond design basis (severe) accidents. Therefore the hydrogen recombiners are not required to mitigate any design basis accident including a loss of cooling accident.

The Containment Air Return, Hydrogen Skimmer and Hydrogen Recombiner System receives electrical power from the Essential Auxiliary Power System. The Containment Air Return, Hydrogen Skimmer, and Hydrogen Recombiner System is discussed in Section 6.2.5.

7.6.10.2 Design Bases

The instrumentation and controls of the Containment Air Return and Hydrogen Skimmer System are designed to assure proper systems operation for containment atmosphere control after a LOCA. The instrumentation and controls of the Hydrogen Recombiner System are designed to assure proper system operation if required as a backup for the hydrogen igniters.

7.6.10.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to these controls. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.6.10.3.1 General Functional Requirements

The instrumentation and controls associated with the containment air return and hydrogen skimmer systems are designed with reliability and redundancy to automatically initiate their safety functions upon receipt of a signal from the ESFAS. The Hydrogen Recombiners are available as a backup for the hydrogen igniters and can be manually initiated to reduce hydrogen content within containment.

7.6.10.3.2 Single Failure Criterion

The containment air return, hydrogen skimmer and hydrogen recombiner system instrumentation and controls are designed such that no single failure can prevent the system from performing its safety function.

7.6.10.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.10.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.10.3.5 Channel Integrity

The redundant trains of the safety related instrumentation and controls of the Containment Air Return, Hydrogen Skimmer and Hydrogen Recombiner System are designed to maintain their functional capability.

7.6.10.3.6 Channel Independence

The safety-related instrumentation and controls for the containment air return, hydrogen skimmer, and hydrogen recombiner system are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.6.10.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls for the containment air return, hydrogen skimmer, and hydrogen recombiner system are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate this system are part of the ESFAS and are described in Section 7.3.

7.6.10.3.8 Derivation of System Inputs

System inputs are provided by the ESFAS or are derived from direct measurement of the desired variables.

7.6.10.3.9 Capability for Test, Calibration, and Sensor Checks

The containment air return, hydrogen skimmer, and hydrogen recombiner system safety-related instrumentation and controls are designed to facilitate testing and calibration.

7.6.10.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls for the containment air return, hydrogen skimmer, and hydrogen recombiner system are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate this system are part of the ESFAS and are described in Section 7.3.

7.6.10.3.11 Operating Bypasses

The containment air return, hydrogen skimmer, and hydrogen recombiner system instrumentation and controls do not employ operating bypasses in their initiating logic. The protection channels that actuate the system are part of the ESFAS and are described in Section 7.3.

7.6.10.3.12 Indication of Bypasses

Indication is provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either train of the containment air return or hydrogen skimmer system has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. No OAC 1.47 bypass indication is provided for the hydrogen recombiner system. The ESF bypass indication panel is discussed in Section 7.8.3.

7.6.10.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the containment air return, hydrogen skimmer, and hydrogen recombiner system inoperable is controlled by administrative and security measures.

7.6.10.3.14 Multiple Setpoints

Multiple setpoints are not required for the containment air return, hydrogen skimmer, and hydrogen recombiner system.

7.6.10.3.15 Completion of Protective Action Once it is Initiated

Once initiated by a protective signal, the containment air return system will continue to operate within the containment pressure limits controlled by the Containment Pressure Control System as described in Section 7.6.4. Once initiated by a protective signal, the hydrogen skimmer system will continue to operate until operation is manually terminated by the operator. Operator action is required to manually initiate and terminate operation of the hydrogen recombiner system.

7.6.10.3.16 Manual Initiation

The containment air return fans, hydrogen skimmer fans, containment air return isolation dampers, and hydrogen skimmer fan isolation valves can be manually operated from the control room. The hydrogen recombiners are manually operated from their local control panels.

7.6.10.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points are controlled by administrative and security measures.

7.6.10.3.18 Identification of Protective Action

The safety-related instrumentation and controls for the containment air return, hydrogen skimmer, and hydrogen recombiner system are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate this system are part of the ESFAS and are described in Section 7.3.

7.6.10.3.19 Information Read-Out

Information read-outs related to the operation of the containment air return and hydrogen skimmer fans and associated dampers and valves are provided in the control room. Information read-outs for the hydrogen recombiners are provided on their local control panel.

7.6.10.3.20 System Repair

The containment air return, hydrogen skimmer, and hydrogen recombiner system is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.10.3.21 Identification

The safety-related instrumentation and control equipment of the containment air return, hydrogen skimmer, and hydrogen recombiner system is physically identified as described in Section 7.1.2.3.

7.6.11 Spent Fuel Pool Cooling System

7.6.11.1 Description

The Spent Fuel Pool Cooling System is designed to remove heat from the spent fuel pool and maintain the purity and optical clarity of the pool water during fuel handling operations. The fuel pool cooling pumps and refueling water storage tank isolation valves are controlled from the control room. ESFAS provides permissives to automatically trip the spent fuel pool cooling pumps, and close the refueling water storage tank isolation valves. The Spent Fuel Pool Cooling System has two separate and redundant trains. The Spent Fuel Pool Cooling System instrumentation and controls receive electrical power from the Essential Auxiliary Power System which is described in Section 8.3.

7.6.11.2 Design Bases

The Spent Fuel Pool Cooling System instrumentation and controls are designed to provide reliable manual and automatic control of the Spent Fuel Pool Cooling System.

7.6.11.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to these controls. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.6.11.3.1 General Functional Requirements

The spent fuel cooling system instrumentation and controls are designed for the normal plant operating environment, and are not required during a LOCA. However, the instrumentation and controls are required to perform a safety function in the event of a spent fuel accident and are designed accordingly.

7.6.11.3.2 Single Failure Criterion

No single failure within the safety-related instrumentation and control of the spent fuel pool cooling system can prevent the system from performing its safety function.

7.6.11.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.11.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.11.3.5 Channel Integrity

The redundant trains of the safety-related instrumentation and controls of this system are designed to maintain their functional capability.

7.6.11.3.6 Channel Independence

The safety-related instrumentation and controls for the Spent Fuel Pool Cooling System are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.6.11.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls for the Spent Fuel Pool Cooling System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the system are part of the ESFAS and are described in Section 7.3.

7.6.11.3.8 Derivation of System Inputs

Input signals to the Spent Fuel Cooling System instrumentation and controls, are provided by the ESFAS or are derived from direct measurements of the desired variables.

7.6.11.3.9 Capability for Test, Calibration, and Sensor Checks

The Spent Fuel Pool Cooling System safety-related instrumentation and controls are designed to facilitate testing and calibration.

7.6.11.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls of the Spent Fuel Pool Cooling system are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate this system are part of the ESFAS and are described in Section 7.3.

7.6.11.3.11 Operating Bypasses

The Spent Fuel Pool Cooling System instrumentation and controls do not employ operating bypasses in their initiating logic. The protection channels that actuate the system are part of the ESFAS and are described in Section 7.3.

7.6.11.3.12 Indication of Bypass

Indication is provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either train of the Spent Fuel Pool Cooling System has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. The ESF bypass indication panel is discussed in Section 7.8.3.

7.6.11.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the Spent Fuel Pool Cooling System inoperable is controlled by administrative and security measures.

7.6.11.3.14 Multiple Setpoints

Multiple setpoints are not required for the Spent Fuel Pool Cooling System.

7.6.11.3.15 Completion of Protective Action Once it is Initiated

Once initiated by a protective signal, the Spent Fuel Pool Cooling System instrumentation and controls continue to perform their safety function until deliberate action is taken by the operator.

7.6.11.3.16 Manual Initiation

The Spent Fuel Pool Cooling system can be manually operated from the control room.

7.6.11.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points of the Spent Fuel Pool Cooling System is controlled by administrative and security measures.

7.6.11.3.18 Identification of Protective Action

The safety-related instrumentation and controls of the Spent Fuel Pool Cooling System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate this system are part of the ESFAS and are described in Section 7.3.

7.6.11.3.19 Information Read-Out

Information read-outs related to the operation of the Spent Fuel Pool Cooling system for safety-related functions are provided in the control room.

7.6.11.3.20 System Repair

The Spent Fuel Pool Cooling System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.11.3.21 Identification

The safety-related instrumentation and control equipment of the Spent Fuel Pool Cooling System is physically identified as described in Section 7.1.2.3.

7.6.12 Auxiliary Building Ventilation System

7.6.12.1 Description

The Auxiliary Building Ventilation System provides adequate capacity to assure that proper temperatures are maintained in the Auxiliary Building during normal operating and shutdown conditions. During normal plant operations, the supply and exhaust systems are balanced such that all areas of the building are at a slightly negative pressure with respect to the atmosphere. This system also provides filtering for potentially contaminated areas of the auxiliary building and cooling air for the auxiliary shutdown panel rooms.

During normal operation, the Auxiliary Building Filtered Exhaust System is aligned to operate with the exhaust filter trains in the filter bypassed mode. In the event of high radiation upstream of the filter units (0EMF41) or in the Unit Vent Stack (EMF35, 36); these alarm in the control room and automatically realigns the system to exhaust through the filter units.

The Auxiliary Building Filtered Exhaust System and the Auxiliary Shutdown Panel Room Supply System have two separate and redundant trains. A single failure analysis of the Filtered Exhaust System and the auxiliary shutdown panel air handling units is provided in Table 9-28. Capability to start the Auxilairy Building Filtered Exhaust System is provided in the control room. The ESFAS provides signals to automatically shutdown non-essential Auxiliary Building ventilation system components and start the Auxiliary Building Filtered Exhaust System.

In the Unit Vent radiation monitors are provided to detect radiation. Upon high radiation, the Auxiliary Building Supply Units and Unfiltered Exhaust Units are shutdown automatically. An ESFAS or blackout sequencer signal bypasses these permissives in the Filtered Exhaust Unit controls in order to maintain their safety function.

7.6.12.2 Design Bases

The Auxiliary Building Ventilation System instrumentation and controls are designed to provide reliable control of the Auxiliary Building Ventilation System during normal and accident conditions.

7.6.12.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to the controls of this ESF support system. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.6.12.3.1 General Functional Requirements

The Auxiliary Building Ventilation System safety-related instrumentation and controls monitor and provide manual and automatic control of the Auxiliary Building Ventilation.

7.6.12.3.2 Single Failure Criterion

No single failure within the safety-related instrumentation and control of the Auxiliary Building Ventilation System can prevent the system from performing its safety function.

7.6.12.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.12.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.12.3.5 Channel Integrity

The redundant trains of safety-related instrumentation and controls for the Auxiliary Building Ventilation System are designed to assure system functional capability.

7.6.12.3.6 Channel Independence

The safety-related instrumentation and controls of the Auxiliary Building Ventilation System are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.6.12.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls for the Auxiliary Building Ventilation System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate this system are part of the ESFAS and are described in Section 7.3.

7.6.12.3.8 Derivation of System Inputs

Input signals to the Auxiliary Building Ventilation System instrumentation and controls are provided by the ESFAS or are derived from direct measurement of the desired variable.

7.6.12.3.9 Capability for Test, Calibration, and Sensor Checks

The Auxiliary Building Ventilation System safety-related instrumentation and controls are designed to facilitate testing and calibration as required by the Technical Specifications.

7.6.12.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls of the Auxiliary Building Ventilation System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate this system are part of the ESFAS and are described in Section 7.3.

7.6.12.3.11 Operating Bypasses

The Auxiliary Building Ventilation System instrumentation and controls do not employ operating bypasses in their initiating logic. The protection channels that actuate the Auxiliary Building Ventilation System are part of the ESFAS and are described in Section 7.3.

7.6.12.3.12 Indication of Bypass

Indication is provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either train of the Auxiliary Building Ventilation System has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. The ESF bypass indication panel is discussed in Section 7.8.3.

7.6.12.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the Auxiliary Building Ventilation System inoperable is controlled by administrative and security measures.

7.6.12.3.14 Multiple Setpoints

Multiple setpoints are not required for the Auxiliary Building Ventilation System.

7.6.12.3.15 Completion of Protective Action Once it is Initiated

Once initiated by a protective signal, the Auxiliary Building Ventilation System continues to perform its safety function until deliberate action is taken by the operator.

7.6.12.3.16 Manual Initiation

The Auxiliary Building Ventilation System can be manually operated.

7.6.12.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points of the Auxiliary Building Ventilation System instrumentation and controls is controlled by administrative and security measures.

7.6.12.3.18 Identification of Protective Action

The safety-related instrumentation and controls of the Auxiliary Building Ventilation System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate this system are part of the ESFAS and are described in Section 7.3.

7.6.12.3.19 Information Read-Out

Information read-outs are provided in the control room to monitor the safety functions of the Auxiliary Building Ventilation System.

7.6.12.3.20 System Repair

The Auxiliary Building Ventilation System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.12.3.21 Identification

The safety-related instrumentation and control equipment of the Auxiliary Building Ventilation System is physically identified as described in Section 7.1.2.3.

7.6.13 Control Room Area Heating, Ventilation and Air Conditioning Instrumentation and Control

7.6.13.1 Description

The Control Room Area HVAC consists of three subsystems:

1. Control Room Ventilation System
2. Control Room Area Ventilation System
3. Control Room Area Chilled Water System

These systems maintain the environment in the control room and control room area within acceptable limits for equipment operation and post-accident habitability. The Control Room Area HVAC systems are discussed in Section 9.4.1.

The Control Room Area HVAC systems are divided into two 100 percent capacity redundant trains that are interlocked such that only one train at a time is operating. During normal operation the systems are manually controlled with one train operating and the other train in standby. An ESFAS or blackout provides an automatic start signal to assure that one train of the system is operating and, if necessary, sequentially loads the Control Room Area HVAC equipment onto the Essential Auxiliary Power System as described in Section 8.3.1. Controls are provided in the main control room to allow the operator to switch the operating and standby trains. In the event the control room must be evacuated, controls for these systems are provided in the HVAC equipment room.

Chlorine detectors, radiation monitors, and smoke detectors are provided in each of the control room area ventilation intake ducts to provide control room alarms.

Interlocks are provided to shutdown a chiller compressor on any of the following:

a) High condenser refrigerant pressure

b) Low chilled water temperature

c) Low evaporator chilled water flow

d) High compressor discharge refrigerant temperature

e) Low compressor differential oil pressure

f) High compressor bearing oil discharge

The instrumentation and controls for these systems are powered from the same train of essential auxiliary power as their associated train of HVAC.

The monitoring of variables necessary to provide the required protective action is not performed directly by the Control Room Area HVAC System instrumentation; instead, this function is performed by the ESFAS and power monitoring circuits as described in Sections 7.3 and 8.3, respectively.

7.6.13.2 Design Bases

The instrumentation and controls for the Control Room Area HVAC Systems are designed to provide continuous reliable control of system equipment under all normal and accident conditions. The controls provide for manual operation under normal conditions with an automatic safety signal to assure system operation in the event of an accident.

7.6.13.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to the controls of this ESF support system. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.6.13.3.1 General Functional Requirements

The Control Room Area HVAC safety-related instrumentation and controls monitor and provide manual and automatic control of the control room area HVAC systems.

7.6.13.3.2 Single Failure Criterion

No single failure in the Control Room Area HVAC instrumentation and controls can prevent the system from performing its required safety function.

7.6.13.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.13.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.13.3.5 Channel Integrity

The safety-related instrumentation and controls for the redundant trains of Control Room Area HVAC are designed to assure system functional capability.

7.6.13.3.6 Channel Independence

The safety-related instrumentation and controls for the redundant trains of Control Room Area HVAC are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.6.13.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls of the Control Room Area HVAC System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate this system are part of the ESFAS and are described in Section 7.3.

7.6.13.3.8 Derivation of System Inputs

Input signals to the Control Room Area HVAC instrumentation and controls are provided by the ESFAS or are derived from direct measurement of the desired variables.

7.6.13.3.9 Capability for Test, Calibration, and Sensor Checks

The Control Room Area HVAC System safety-related instrumentation and controls are designed to facilitate testing and calibration as required by the Technical Specifications.

7.6.13.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls of the Control Room Area HVAC System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the system are part of the ESFAS and are described in Section 7.3.

7.6.13.3.11 Operating Bypasses

The Control Room Area HVAC System instrumentation and controls do not employ operating bypasses in their initiating logic. The protection channels that actuate the system are part of the ESFAS and are described in Section 7.3.

7.6.13.3.12 Indication of Bypass

Indication is provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either train of the Control Room Area HVAC System has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. The ESF bypass indication panel is discussed in Section 7.8.3.

7.6.13.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the Control Room Area HVAC System inoperable is controlled by administrative and security measures.

7.6.13.3.14 Multiple Setpoints

Multiple setpoints are not required for the Control Room Area HVAC System.

7.6.13.3.15 Completion of Protective Action Once it is Initiated

Once initiated by a protective signal, the Control Room Area HVAC System continues to perform its safety function until deliberate action is taken by the operator.

7.6.13.3.16 Manual Initiation

The Control Room Area HVAC System can be manually operated from the control room.

7.6.13.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration and test points for the Control Room Area HVAC System safety-related instrumentation and controls is controlled by administrative and security measures.

7.6.13.3.18 Identification of Protective Action

The safety-related instrumentation and controls of the Control Room Area HVAC System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate this system are part of the ESFAS and are described in Section 7.3.

7.6.13.3.19 Information Read-Out

Information read-outs are provided in the control room to monitor the safety functions of the Control Room Area HVAC System.

7.6.13.3.20 System Repair

The Control Room Area HVAC System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.13.3.21 Identification

The safety-related instrumentation and control equipment of the Control Room Area HVAC System is physically identified as described in Section 7.1.2.3.

7.6.14 Annulus Ventilation System Instrumentation and Control

7.6.14.1 Description

Two redundant 100 percent capacity trains of annulus ventilation collect and filter gaseous leakage during accident conditions, and relieve the post accident pressure buildup in the Containment/Reactor Building annulus. The Annulus Ventilation System is discussed in Section 9.4.9.

The Annulus Ventilation System is not normally in operation. In the event of an accident, a safety injection signal from the ESFAS automatically starts and aligns the system to maintain a negative pressure in the annulus. The recirculation and exhaust dampers are regulated automatically by annulus pressure signals to maintain the designed negative pressure of ≈-1.5"

w.g. at the instrument point in the annulus. This design setpoint assures that under all conditions, all points in the annulus will be at least 0.5" w.g. negative which exceeds the –0.25" w.g. design basis minimum value. Manual controls for the Annulus Ventilation System are provided in the control room.

The instrumentation and controls for the Annulus Ventilation System are powered from the same train of essential auxiliary power as their associated trained ventilation equipment.

7.6.14.2 Design Bases

The Annulus Ventilation System instrumentation and controls are designed to provide reliable automatic and manual control of the Annulus Ventilation System under normal and accident conditions.

7.6.14.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to these controls. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.6.14.3.1 General Functional Requirements

The Annulus Ventilation System instrumentation and controls automatically start the Annulus Ventilation System on safety injection signal (Ss) and control the operation of the system to maintain sub-atmospheric pressure in the annulus.

7.6.14.3.2 Single Failure Criterion

No single failure in the Annulus Ventilation System instrumentation and controls can prevent the system from performing its required safety function.

7.6.14.3.3 Quality of Components

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.14.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.14.3.5 Channel Integrity

The safety-related instrumentation and controls for the redundant trains of annulus ventilation are designed to assure system functional capability.

7.6.14.3.6 Channel Independence

The safety-related instrumentation and controls for the redundant trains of annulus ventilation are physically separated and electrically isolated as described in Section 8.3.1.4.

7.6.14.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls of the Annulus Ventilation System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the Annulus Ventilation System are part of the ESFAS and are described in Section 7.3.

7.6.14.3.8 Derivation of System Inputs

Input signals to the Annulus Ventilation System instrumentation and controls are from the ESFAS or are derived from direct measurement of the desired variables.

7.6.14.3.9 Capability for Test, Calibration, and Sensor Checks

The Annulus Ventilation System safety-related instrumentation and controls are designed to facilitate testing and calibration as required by Technical Specifications.

7.6.14.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls of the Annulus Ventilation System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the system are part of the ESFAS and are described in Section 7.3.

7.6.14.3.11 Operating Bypasses

The Annulus Ventilation System instrumentation and controls do not employ operating bypasses in their initiating logic. The protection channels that actuate the system are part of the ESFAS and are described in Section 7.3.

7.6.14.3.12 Indication of Bypass

Indication is provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either train of the Annulus Ventilation System has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. The ESF bypass indication panel is discussed in Section 7.8.3.

7.6.14.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the Annulus Ventilation System inoperable is controlled by administrative and security measures.

7.6.14.3.14 Multiple Setpoints

Multiple setpoints are not required for the Annulus Ventilation System.

7.6.14.3.15 Completion of Protective Action Once it is Initiated

Once initiated by a protective signal, the Annulus Ventilation System continues to perform its safety function until deliberate action is taken by the operator.

7.6.14.3.16 Manual Initiation

The Annulus Ventilation System can be manually operated from the control room.

7.6.14.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points for the safety-related instrumentation and controls of the Annulus Ventilation System are controlled by administrative and security measures.

7.6.14.3.18 Identification of Protective Action

The safety-related instrumentation and controls of the Annulus Ventilation System are train related and do not include protection channels as defined in IEEE 279-1971. The protection channels that actuate the Annulus Ventilation System are part of the ESFAS and are described in Section 7.3.

7.6.14.3.19 Information Read-Out

Information read-outs are provided in the control room to monitor the safety functions of the Annulus Ventilation System.

7.6.14.3.20 System Repair

The Annulus Ventilation System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.14.3.21 Identification

The safety-related instrumentation and control equipment of the Annulus Ventilation System is physically identified as described in Section 7.1.2.3.

7.6.15 Diesel Generator Fuel Oil System Instrumentation and Controls

7.6.15.1 Description

Each emergency diesel generator is provided a separate fuel oil system as described in Section 9.5.4.

For each diesel, fuel oil is gravity fed from the main storage tank to the day tank through a fail-closed solenoid operated fuel oil transfer valve. Level switches in the day tank automatically open the fuel oil transfer valve at a preselected low level. The valve is automatically closed when the day tank level reaches a preselected level. Level switches also monitor the day tank and main storage tank to provide high and low level alarms.

A dc fuel oil booster pump is provided for each diesel to supply fuel oil as necessary during maintenance. The motor driven fuel oil booster pump is normally isolated and its circuit breaker locked open.

A pressure switch is connected across each filter and strainer in the Diesel Fuel Oil System. These pressure switches provide alarms to alert the operator of a high filter or strainer differential pressure.

The fuel oil day tank is surrounded by a 5 foot retaining wall to contain any leakage that may occur in the day tank or its piping. In the event fuel oil is collected inside the retaining wall, a solenoid operated drain valve is provided to automatically drain the fuel oil to the dirty lube oil tank. A high level sensed inside the retaining wall initiates an alarm in the control room and on the local annunciator. A high-high level automatically opens the drain valve and starts the diesel lube oil transfer pump. When the level inside the retaining wall is reduced to the low level

setpoint, the drain valve is automatically closed and the diesel lube oil transfer pump is stopped. Controls are also provided to allow manual operation of the retaining wall drain valve.

Important parameters of the Diesel Generator Fuel Oil System are monitored and provide alarms on the diesel control panels to indicate system abnormal conditions. A common alarm is provided in the control room to alert the operator to an abnormal fuel oil system condition in sufficient time to take the appropriate corrective action. The following system parameters are alarmed:

1. Main fuel tank low level
2. Main fuel tank high level
3. Fuel day tank low level
4. Fuel day tank high level
5. Main fuel oil tank Tech. Spec. level warning
6. Fuel oil pressure low
7. Fuel filter high differential pressure
8. Fuel pump strainer high differential pressure
9. DC pump strainer high differential pressure
10. Day tank retaining wall high level

7.6.15.2 Design Bases

The Diesel Generator Fuel Oil System instrumentation and controls are designed to control and monitor the operation of the diesel fuel oil system for proper emergency diesel generator operation under accident conditions and during testing.

7.6.15.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to the controls of this ESF support system. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.6.15.3.1 General Functional Requirements

The Diesel Generator Fuel Oil System safety-related instrumentation and controls monitor and control the fuel oil system during diesel generator operation.

7.6.15.3.2 Single Failure Criterion

No single failure in the Diesel Generator Fuel Oil System instrumentation and controls can affect more than one emergency diesel generator.

7.6.15.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.15.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.15.3.5 Channel Integrity

The redundant trains of safety-related instrumentation and controls for the Diesel Generator Fuel Oil System are designed to assure system functional capability.

7.6.15.3.6 Channel Independence

The safety-related instrumentation and controls of the redundant Diesel Generator Fuel Oil System are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.6.15.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls for the Diesel Generator Fuel Oil System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.15.3.8 Derivation of System Inputs

Input signals to the Diesel Generator Fuel Oil System instrumentation and controls are derived from direct measurement of the desired variable.

7.6.15.3.9 Capability for Test, Calibration, and Sensor Checks

The Diesel Generator Fuel Oil System safety-related instrumentation and controls are designed to facilitate testing and calibration as required by the Technical Specifications.

7.6.15.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls for the Diesel Generator Fuel Oil System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.15.3.11 Operating Bypasses

The Diesel Generator Fuel Oil System instrumentation and controls do not employ operating bypasses in their initiating logic.

7.6.15.3.12 Indication of Bypass

No system level ESF bypass indication is required for the Diesel Generator Fuel Oil System per Table 7-14. There are no direct logic inputs from the Diesel Generator Fuel Oil System System provided to the OAC 1.47 Bypass Panel Graphic Display. The ESF bypass indication panel is discussed in Section 7.8.3.

7.6.15.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the Diesel Generator Fuel Oil System inoperable is controlled by administrative and security measures.

7.6.15.3.14 Multiple Setpoints

Multiple setpoints are not required for the Diesel Generator Fuel Oil System.

7.6.15.3.15 Completion of Protective Action Once it is Initiated

Once initiated by a protective signal, the Diesel Generator Fuel Oil System continues to perform its safety function until the conditions requiring its operation have been eliminated.

7.6.15.3.16 Manual Initiation

The Diesel Generator Fuel Oil System can be manually operated locally from the diesel room.

7.6.15.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points for the Diesel Generator Fuel Oil System safety-related instrumentation and controls is controlled by administrative and security measures.

7.6.15.3.18 Identification of Protective Action

The safety-related instrumentation and controls for the Diesel Generator Fuel Oil System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.15.3.19 Information Read-Out

Alarms are provided in the control room to monitor the safety functions of the Diesel Generator Fuel Oil System.

7.6.15.3.20 System Repair

The Diesel Generator Fuel Oil System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.15.3.21 Identification

The safety-related instrumentation and control equipment for the Diesel Generator Fuel Oil System is physically identified as described in Section 7.1.2.3.

7.6.16 Diesel Generator Cooling Water System Instrumentation and Control

7.6.16.1 Description

The Diesel Generator Cooling Water System is discussed in Section 9.5.5.

The Diesel Generator Cooling Water System instrumentation and controls automatically control the operation of the system to maintain diesel engine temperature within the designed operating range. During standby operation the jacket water heater circulating pump circulates cooling water through the thermostatically controlled jacket water heater. The diesel starting circuit automatically deenergizes the jacket water heater and jacket water heater circulating pump. During diesel operation cooling water temperature is regulated by a temperature controlled valve that adjusts the amount of water circulated through the system heat exchanger.

The diesel engine is interlocked to automatically shutdown if the cooling water temperature exceeds a predetermined value; however, this interlock is automatically bypassed by a diesel emergency start signal.

Diesel Generator Cooling Water System instrumentation provides alarms locally and at a common alarm point in the control room for the following conditions:

1. Cooling water effluent temperature high
2. Cooling water effluent temperature low
3. Cooling water influent temperature high
4. Cooling water influent temperature low

5. Intercooler influent temperature high
6. Cooling water pressure low
7. Standpipe level low

7.6.16.2 Design Bases

The Diesel Generator Cooling Water System safety-related instrumentation and controls are designed to monitor and control the operation of the Diesel Generator Cooling Water System for proper diesel engine operation under accident conditions and during testing.

7.6.16.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to the controls of this ESF support system. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.6.16.3.1 General Functional Requirements

These safety-related instrumentation and controls monitor and control the Diesel Generator Cooling Water System to assure proper diesel engine operation on receipt of an emergency start signal.

7.6.16.3.2 Single Failure Criterion

Any failure of the Diesel Generator Cooling Water System instrumentation and controls affects only its associated cooling water system and can in no way affect the operation of the redundant diesel generator.

7.6.16.3.3 Quality of Components

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.16.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.16.3.5 Channel Integrity

The redundant trains of Diesel Generator Cooling Water System safety-related instrumentation and controls are designed to assure system functional capability.

7.6.16.3.6 Channel Independence

The safety-related instrumentation and controls of the redundant Diesel Generator Cooling Water System are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.6.16.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls for the Diesel Generator Cooling Water System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.16.3.8 Derivation of System Inputs

Input signals to the Diesel Generator Cooling Water System instrumentation and controls are derived from direct measurement of the desired variable.

7.6.16.3.9 Capability for Test, Calibration, and Sensor Checks

The Diesel Generator Cooling Water System safety-related instrumentation and controls are designed to facilitate testing and calibration.

7.6.16.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls for the Diesel Generator Cooling Water System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.16.3.11 Operating Bypasses

The Diesel Generator Cooling Water System instrumentation and controls do not employ operating bypasses in their initiating logic.

7.6.16.3.12 Indication of Bypass

No system level ESF bypass indication is required for the Diesel Generator Cooling Water System per Table 7-14. There are no direct logic inputs from the Diesel Generator Cooling Water System System provided to the OAC 1.47 Bypass Panel Graphic Display. The ESF bypass indication panel is discussed in Section 7.8.3.

7.6.16.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the Diesel Generator Cooling Water System inoperable is controlled by administrative and security measures.

7.6.16.3.14 Multiple Setpoints

Multiple setpoints are not required for the Diesel Generator Cooling Water System.

7.6.16.3.15 Completion of Protective Action Once it is Initiated

Once initiated by a protective signal, the Diesel Generator Cooling Water System continues to perform its safety function until the condition requiring its operation has been eliminated.

7.6.16.3.16 Manual Initiation

The Diesel Generator Cooling Water System can be manually operated locally in the diesel room.

7.6.16.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points for the safety-related instrumentation and controls of the Diesel Generator Cooling Water System is controlled by administrative and security measures.

7.6.16.3.18 Identification of Protective Action

The safety-related instrumentation and controls for the Diesel Generator Cooling Water System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.16.3.19 Information Read-Out

Alarms are provided in the control room to monitor the safety functions of the Diesel Generator Cooling Water System.

7.6.16.3.20 System Repair

The Diesel Generator Cooling Water System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.16.3.21 Identification

The safety-related instrumentation and control equipment for the Diesel Generator Cooling Water System is physically identified as described in Section 7.1.2.3.

7.6.17 Diesel Generator Starting Air System Instrumentation and Control

7.6.17.1 Description

The Diesel Generator Starting Air System is discussed in Section 9.5.6.

Each diesel generator is provided with two, independent starting air systems, each including an air compressor and an air receiver. A pressure switch on each air receiver controls the operation of its associated air compressor.

Diesel Generator Starting Air System instrumentation provides local alarms for low air pressure at the engine and for low control air pressure. The operator is alerted to these conditons by a common alarm in the control room.

7.6.17.2 Design Bases

The Diesel Generator Engine Starting Air System is designed to provide fast start capability for the diesel generator engine by using compressed air to rotate the engine until combustion begins and it accelerates under its own power.

The design basis of the Diesel Generator Engine Starting Air System is the ability of the system to support 5 successful engine starts without use of the air compressors.

7.6.17.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to the controls of this ESF support system. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.6.17.3.1 General Functional Requirements

The Diesel Generator Starting Air System instrumentation and controls monitor the system air pressure and control the system air compressors to assure adequate air pressure is available to allow at least two automatic start attempts of each diesel generator. If the diesel starting air

pressure drops to ≤ 150 psig, automatic engine start lockout will occur. At 150 psig there is enough starting air remaining in the air receivers for at least three manual start attempts.

7.6.17.3.2 Single Failure Criterion

Any failure of the Diesel Generator Starting Air System instrumentation and controls affects only its associated starting air system and can in no way affect the operation of the redundant diesel generator.

7.6.17.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.17.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.17.3.5 Channel Integrity

The redundant trains of Diesel Generator Starting Air System safety-related instrumentation and controls are designed to assure system functional capability.

7.6.17.3.6 Channel Independence

The safety-related instrumentation and controls of the Diesel Generator Starting Air System are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.6.17.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls for the Diesel Generator Starting Air System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.17.3.8 Derivation of System Inputs

Input signals to the Diesel Generator Starting Air System instrumentation and controls are derived from direct measurement of the desired variable.

7.6.17.3.9 Capability for Test, Calibration, and Sensor Checks

The Diesel Generator Starting Air System safety-related instrumentation and controls are designed to facilitate testing and calibration as required by the Technical Specifications.

7.6.17.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls of the Diesel Generator Starting Air System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.17.3.11 Operating Bypasses

The Diesel Generator Starting Air System instrumentation and controls do not employ operating bypasses in their initiating logic.

7.6.17.3.12 Indication of Bypass

Indication is provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either train of the Diesel Generator Starting Air System has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. The ESF bypass indication panel is discussed in Section 7.8.3.

7.6.17.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the Diesel Starting Air System inoperable is controlled by administrative and security measures.

7.6.17.3.14 Multiple Setpoints

Multiple setpoints are not required for the Diesel Generator Starting Air System.

7.6.17.3.15 Completion of Protective Action Once it is Initiated

Once initiated by a protective signal, the Diesel Generator Starting Air System continues to perform its safety function until the condition requiring its operation has been eliminated.

7.6.17.3.16 Manual Initiation

The Diesel Generator Starting Air System can be manually operated locally in the diesel room.

7.6.17.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points for the safety-related instrumentation and controls of the Diesel Generator Starting Air System are controlled by administrative and security measures.

7.6.17.3.18 Identification of Protective Action

The safety-related instrumentation and controls of the Diesel Generator Starting Air System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.17.3.19 Information Read-Out

Alarms are provided in the control room to monitor the safety functions of the Diesel Generator Starting Air System.

7.6.17.3.20 System Repair

The Diesel Generator Starting Air System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.17.3.21 Identification

The safety-related instrumentation and control equipment of the Diesel Generator Starting Air System is physically identified as described in Section 7.1.2.3.

7.6.18 Diesel Generator Lubricating Oil System Instrumentation and Control

7.6.18.1 Description

The diesel lube oil system pumps lubricating oil from the lube oil sump tank to the diesel generator and provides a path for the engine crankcase to gravity drain the lube oil back to the sump tank. The Diesel Generator Lubricating Oil System is discussed in Section 9.5.7.

The diesel lube oil system instrumentation and controls provide engine protecting interlocks that prevent starting and shutdown the engine on the following conditions:

1. Low lube oil pressure
2. Low-low lube oil pressure
3. Low turbo oil pressure
4. High lube oil outlet temperature
5. High main bearing temperature

All of these interlocks except low-low lube oil pressure are automatically bypassed by an emergency start signal.

The low-low lube oil pressure trip employs three separate pressure sensors with contact outputs arranged in a two-out-of-three logic. The trip is bypassed for a sufficient time during engine starting to allow the engine driven lube oil pump to provide adequate oil pressure. In the event adequate oil pressure is not achieved within the allotted time, the engine is automatically shutdown.

Diesel generator lube oil system instrumentation provides alarms locally and at a common alarm point in the control room for the following conditions:

1. High lube oil inlet temperature
2. Low lube oil inlet temperature
3. High lube oil outlet temperature
4. Low lube oil outlet temperature
5. Low lube oil pressure
6. Low lube oil sump tank level

7.6.18.2 Design Bases

The Diesel Generator Lubricating Oil System safety-related instrumentation and controls are designed to monitor and control the diesel lube oil system for proper engine lubrication and protection.

7.6.18.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to the controls of this ESF support system. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.6.18.3.1 General Functional Requirements

These safety-related instrumentation and controls monitor and control the Diesel Generator Lubricating Oil System to assure proper lubrication during engine operation.

7.6.18.3.2 Single Failure Criterion

Any failure in the Diesel Generator Lubricating Oil System instrumentation and controls affects only its associated lube oil system and can in no way affect the operation of the redundant diesel generator.

7.6.18.3.3 Quality of Components

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.18.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.18.3.5 Channel Integrity

The redundant trains of Diesel Lube Oil System safety-related instrumentation and controls are designed to assure system functional capability.

7.6.18.3.6 Channel Independence

The safety-related instrumentation and controls of the Diesel Generator Lube Oil System are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.6.18.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls of the Diesel Lube Oil System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.18.3.8 Derivation of System Inputs

Input signals to the Diesel Generator Lubricating Oil System instrumentation and controls are derived from direct measurement of the desired variable.

7.6.18.3.9 Capability for Test, Calibration, and Sensor Checks

The Diesel Generator Lube Oil System safety-related instrumentation and controls are designed to facilitate testing and calibration as required by the Technical Specifications.

7.6.18.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls of the Diesel Generator Lube Oil System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.18.3.11 Operating Bypasses

The Diesel Generator Lube Oil System instrumentation and controls do not employ operating bypasses in their initiating logic.

7.6.18.3.12 Indication of Bypass

Indication is provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either train of the Diesel Generator Lube Oil System has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. The ESF bypass indication panel is discussed in Section 7.8.3.

7.6.18.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the Diesel Generator Lube Oil System inoperable is controlled by administrative and security measures.

7.6.18.3.14 Multiple Setpoints

Multiple setpoints are not required for the Diesel Generator Lube Oil System.

7.6.18.3.15 Completion of Protective Action Once it is Initiated

Once initiated by a protective signal, the Diesel Generator Lube Oil System continues to perform its safety function until the condition requiring its operation has been eliminated.

7.6.18.3.16 Manual Initiation

The Diesel Generator Lube Oil System can be manually operated locally in the diesel room.

7.6.18.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points for the safety-related instrumentation and controls of the Diesel Generator Lube Oil System are controlled by administrative and security measures.

7.6.18.3.18 Identification of Protective Action

The safety-related instrumentation and controls of the Diesel Generator Lube Oil System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.18.3.19 Information Read-Out

Alarms are provided in the control room to monitor the safety functions of the Diesel Generator Lube Oil System.

7.6.18.3.20 System Repair

The Diesel Generator Lube Oil System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.18.3.21 Identification

The safety-related instrumentation and control equipment of the Diesel Generator Lube Oil System is physically identified as described in Section 7.1.2.3.

7.6.19 Fuel Handling Area Ventilation System Instrumentation and Control

7.6.19.1 Description

The Fuel Handling Area Ventilation System supplies outside air to clean areas and exhausts air from potentially contaminated areas of the fuel handling and storage building. The system consists of a 100 percent capacity air supply system and two redundant 100 percent capacity trains of air exhaust system. Each train of the exhaust system consists of two 50 percent capacity exhaust fans with associated 50 percent capacity filter trains. Only the exhaust portion of the Fuel Handling Area Ventilation System provides a safety function. The Fuel Handling Area Ventilation System is discussed in Section 9.4.2.

During normal plant operation the Fuel Handling Area Ventilation System is aligned to operate with the exhaust filter trains bypassed. In the event of high radioactivity in the fuel handling area exhaust, gaseous radioactivity monitors upstream of the exhaust filters provide an alarm in the main control room and automatically realign the system to exhaust through the filter trains.

Prior to fuel handling operations involving recently irradiated fuel, the Fuel Handling Area Ventilation System is manually aligned to exhaust through the filter trains.

The fuel handling area exhaust fans are interlocked such that only one train can operate at a time. In the event of a blackout or a LOCA, the exhaust fans are load shed from their Class 1E power source. A blackout signal to the diesel sequencer allows the previously operating fan to be sequenced back on after the diesel starts; however, an SIAS signal to the diesel sequencer blocks further exhaust fan operation.

7.6.19.2 Design Bases

The Fuel Handling Area Ventilation System instrumentation and controls are designed to provide filtration of the fuel pool environment in the event that high radiation levels are detected in the area.

7.6.19.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to these controls. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.6.19.3.1 General Functional Requirements

The Fuel Handling Area Ventilation System safety-related instrumentation and controls automatically control the exhaust portion of the system to prevent the release of contaminated fuel handling area exhaust.

7.6.19.3.2 Single Failure Criterion

When the Fuel Handling Area Ventilation System is in operation, no single failure of its safety-related instrumentation and controls can prevent the performance of the system safety function.

7.6.19.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review,

procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.19.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.19.3.5 Channel Integrity

The redundant trains of safety-related instrumentation and controls for the Fuel Handling Area Ventilation System are designed to assure system functional capability.

7.6.19.3.6 Channel Independence

The redundant trains of Fuel Handling Area Ventilation System safety-related instrumentation and controls are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.6.19.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls of the Fuel Handling Area Ventilation System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.19.3.8 Derivation of System Inputs

Inputs to the Fuel Handling Area Ventilation System safety-related instrumentation and controls are derived from direct measurement of the desired variable.

7.6.19.3.9 Capability for Test, Calibration, and Sensor Checks

The Fuel Handling Area Ventilation System safety-related instrumentation and controls are designed to facilitate testing and calibration as required by the Technical Specifications.

7.6.19.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls of the Fuel Handling Area Ventilation System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.19.3.11 Operating Bypasses

The Fuel Handling Area Ventilation System instrumentation and controls do not employ operating bypasses in their initiating logic.

7.6.19.3.12 Indication of Bypass

Bypass indication is not required for the Fuel Handling Area Ventilation System.

7.6.19.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the Fuel Handling Area Ventilation System inoperable is controlled by administrative and security measures.

7.6.19.3.14 Multiple Setpoints

Multiple setpoints are not required for the Fuel Handling Area Ventilation System.

7.6.19.3.15 Completion of Protective Action Once it is Initiated

Once initiated by a protective signal, the Fuel Handling Area Ventilation System continues to perform its safety function until deliberate action is taken by the operator.

7.6.19.3.16 Manual Initiation

The fuel handling area exhaust fans can be manually operated from the control room.

7.6.19.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points for the safety-related instrumentation and controls of the Fuel Handling Area Ventilation System are controlled by administrative and security measures.

7.6.19.3.18 Identification of Protective Action

The safety-related instrumentation and controls of the Fuel Handling Area Ventilation System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.19.3.19 Information Read-Out

Information read-outs related are provided in the control room to monitor the safety functions of the Fuel Handling Area Ventilation System.

7.6.19.3.20 System Repair

The Fuel Handling Area Ventilation System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.19.3.21 Identification

The safety-related instrumentation and control equipment of the Fuel Handling Area Ventilation System is physically identified as described in Section 7.1.2.3.

7.6.20 Reactor Coolant System Overpressure Protection System for Low Pressure/Temperature, Water Solid Conditions

7.6.20.1 Description

The Reactor Coolant System Overpressure Protection System prevents the Reactor Coolant System from exceeding the pressure/temperature limits of 10CFR 50, Appendix G, for periods of water solid operation during startup and shutdown. The maximum RCS pressure is limited by providing a low pressure setpoint interlocked with reactor coolant temperature to actuate the pressurizer power operated relief valves (PORV). Refer to Section 5.4.13.2 for a description of the PORVs.

The protection provided by this system is required for periods of water solid operation during startup and shutdown. Therefore, the PORV low pressure set-point is enabled by the operator as plant conditions dictate. A key-lock switch, located on the main control board, is provided for each train of PORVs to enable the low pressure setpoint.

A logic diagram for the Reactor Coolant System Overpressure Protection System is provided in Figure 7-17.

As RCS temperature approaches the temperature setpoint during plant cooldown, but before collapse of the pressurizer steam bubble, an annunciator alerts the operator that plant conditions require low temperature overpressure protection. The operator places each key-lock switch to the LOW PRESSURE position to enable the PORV low pressure setpoint.

Should a pressure excursion occur while in the low pressure mode with plant temperature below the temperature setpoint, system pressure in excess of the PORV low pressure setpoint would be relieved to the pressurizer relief tank (refer to Section 5.2.2.1). An annunciator in the control room would alert the operator to system overpressure in this condition.

When system temperature rises above the temperature setpoint during plant heatup, the RCS Overpressure Protection System is automatically disarmed, and an annunciator alerts the operator that low temperature overpressure protection is no longer required. The operator then returns each key-lock switch to the NORMAL position.

The permissive signal which allows the operator to enable the PORV to respond to the low pressure setpoint and the annunciator which alerts the operator that the low pressure mode is required are derived from the RCS wide range temperature instrument. Additionally, the temperature permissive signal functions as an interlock to prevent inadvertent actuation of the PORVs during normal operation and, also, to automatically remove the low pressure setpoint when system temperature is above the low temperature setpoint.

7.6.20.2 Design Bases

The RCS Overpressure Protection System is designed to protect the Reactor Coolant System from exceeding the pressure/temperature limits of 10CFR 50, Appendix G, as defined in the Technical Specifications. Overpressure protection for low pressure/temperature conditions is designed to be functional only when RCS temperature is below a predetermined value.

7.6.20.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to these controls. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.6.20.3.1 General Functional Requirements

The low pressure/temperature overpressure protection system is enabled manually upon receipt of an alarm indicating the approach of plant conditions requiring protection. Once enabled the system operates automatically to relieve excessive pressure through the PORVs.

7.6.20.3.2 Single Failure Criterion

No single failure of the RCS Overpressure Protection System instrumentation and controls can prevent the operation of more than one train of PORVs.

7.6.20.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.20.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.20.3.5 Channel Integrity

The safety-related instrumentation and controls of the low pressure/temperature overpressure protection system are designed to assure system functional capability.

7.6.20.3.6 Channel Independence

The redundant trains of safety-related instrumentation and control for low pressure/temperature overpressure protection are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.6.20.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls of the low pressure/temperature overpressure protection system do not include protection channels as defined in IEEE 279-1971.

7.6.20.3.8 Derivation of System Inputs

The inputs to the low pressure/temperature overpressure protection are derived from direct measurement of the desired variables.

7.6.20.3.9 Capability for Test, Calibration, and Sensor Checks

The low pressure/temperature overpressure protection system safety-related instrumentation and controls are designed to facilitate testing and calibration.

7.6.20.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls of the low pressure/temperature overpressure protection system do not include protection channels as defined in IEEE 279-1971.

7.6.20.3.11 Operating Bypasses

The low pressure/temperature overpressure protection system instrumentation and controls are manually actuated and do not employ operating bypasses in their initiating logic.

7.6.20.3.12 Indication of Bypass

Bypass indication is not required for the low pressure/temperature overpressure protection system.

7.6.20.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the low pressure/temperature overpressure protection system inoperable is controlled by administrative and security measures.

7.6.20.3.14 Multiple Setpoints

Multiple setpoints are not required for the low pressure/temperature overpressure protection system.

7.6.20.3.15 Completion of Protective Action Once it is Initiated

Once initiated the low pressure/temperature overpressure protection system continues to perform its safety function until the condition requiring its operation has been eliminated.

7.6.20.3.16 Manual Initiation

The low pressure/temperature overpressure protection system can be manually operated from the control room.

7.6.20.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points for the safety-related instrumentation and controls of the low pressure/temperature overpressure protection system is controlled by administrative and security measures.

7.6.20.3.18 Identification of Protective Action

The safety-related instrumentation and controls of the low pressure/temperature overpressure protection system do not include protection channels as defined in IEEE 279-1971.

7.6.20.3.19 Information Read-Out

Annunciators are provided in the control room to allow monitoring of the system safety functions.

7.6.20.3.20 System Repair

The low pressure/temperature overpressure protection system is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.20.3.21 Identification

The safety-related instrumentation and control equipment of the low pressure/temperature overpressure protection system is physically identified as described in Section 7.1.2.3.

7.6.21 Nuclear Service Water Pump Structure Ventilation System

7.6.21.1 Description

The Nuclear Service Water (NSW) Pump Structure Ventilation System provides a suitable environment for the operation of the safety-related equipment, instrumentation, and controls located in the NSW pump structure.

The NSW Pump Structure Ventilation System consists of the following safety-related equipment:

1. Two 100% capacity fans in each of the two NSW pump compartments. One fan in each compartment is powered and controlled from Unit 1, while the other fan in each compartment is powered and controlled from Unit 2.
2. Two thermostatically controlled dampers regulate the mixing of fresh air flow from outside with return air flow from inside.
3. Four Hi Limit and four Lo limit thermostats (two of each type per pumphouse) that will initiate an annunciator alarm in the control room if the temperature in the pumphouse exceeds the Hi or Lo setpoints.

Additionally, the following non-safety equipment is provided:

1. Two thermostatically controlled heaters in each of the two NSW pump compartments to limit the minimum ambient temperature. One heater in each compartment is powered from Unit 1, the other from Unit 2.
2. Two air recirculation fans are provided for ventilation near the sump area during maintenance.

During normal operation the NSW Pump Structure Ventilation System is controlled manually from the NSW Pump Structure; however, upon receipt of an safety injection actuation signal (SIAS) by the diesel generator load sequencer of either unit, one fan in each NSW pump compartment is automatically started. Electrical interlocks allow operation of only one fan in each pump compartment to prevent exceeding the ventilation duct capacity.

The NSW Pump Structure Ventilation System safety-related instrumentation and controls are powered from the same train of essential auxiliary power as their associated train of NSW pump.

7.6.21.2 Design Basis

The NSW Pump Structure Ventilation System instrumentation and controls are designed to provide a suitable environment for NSW pump operation.

7.6.21.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to these controls. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279-1971, Section 4, is provided below.

7.6.21.3.1 General Functional Requirement

The NSW Pump Structure Ventilation System safety-related instrumentation and controls automatically control the environment inside the pump structure when initiated by a signal from the diesel generator load sequencer or whenever an NSW pump is running.

7.6.21.3.2 Single Failure

No single failure of the safety-related instrumentation and controls of the NSW Pump Structure Ventilation System can prevent the system from performing its safety function.

7.6.21.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.21.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Section 3.10 and 3.11.

7.6.21.3.5 Channel Integrity

The redundant trains of safety-related instrumentation and controls for the NSW Pump Structure Ventilation System are designed to assure system functional capability.

7.6.21.3.6 Channel Independence

The safety-related instrumentation and controls of the NSW Pump Structure Ventilation System are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.6.21.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls of the NSW Pump Structure Ventilation System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.21.3.8 Derivation of System Inputs

Input signals to the NSW Pump Structure Ventilation System instrumentation and controls are provided by the diesel generator load sequencers or are derived from direct measurement of the desired variables.

7.6.21.3.9 Capability for Test, Calibration, and Sensor Checks

The NSW Pump Structure Ventilation System safety-related instrumentation and controls are designed to facilitate testing and calibration.

7.6.21.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls of the NSW Pump Structure Ventilation System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.21.3.11 Operating Bypasses

The NSW Pump Structure Ventilation System instrumentation and controls do not employ operating bypasses in their initiating logic.

7.6.21.3.12 Indication of Bypass

Indication is provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either train of the NSW Pump Structure Ventilation System has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell. The ESF bypass indication panel is discussed in Section 7.8.3.

7.6.21.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the NSW Pump Structure Ventilation System inoperable is controlled by administrative and security measures.

7.6.21.3.14 Multiple Setpoints

Multiple setpoints are not required for the NSW Pump Structure Ventilation System.

7.6.21.3.15 Completion of Protective Action Once it is Initiated

Once initiated the NSW Pump Structure Ventilation System continues to perform its safety function until the condition requiring its operation has been eliminated.

7.6.21.3.16 Manual Initiation

The NSW Pump Structure Ventilation System can be manually operated from local control panels located in the NSW Pump Structure.

7.6.21.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points for the safety-related instrumentation and controls of the NSW Pump Structure Ventilation System is controlled by administrative and security measures.

7.6.21.3.18 Identification of Protective Action

The safety-related instrumentation and controls of the NSW Pump Structure Ventilation System are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.21.3.19 Information Read-Out

Information read-outs are provided in the control room to allow monitoring of system safety functions.

7.6.21.3.20 System Repair

The NSW Pump Structure Ventilation System is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.21.3.21 Identification

The safety-related instrumentation and control equipment of the NSW Pump Structure Ventilation System is physically identified as described in Section 7.1.2.3.

7.6.22 Main Feedwater Flow Isolation on High Doghouse Water Level Instrumentation

7.6.22.1 Description

The doghouse water level instrumentation provides for the termination of forward feedwater flow in the event of a postulated pipe break in the main feedwater piping in the doghouses to prevent flooding safety-related equipment essential to the safe shutdown of the plant.

The level instrumentation consists of two independent and redundant trains of level switches which monitor level in each of the doghouses. These switches are powered from the vital instrumentation and control power system as described in Section 8.3.2.

Each doghouse contains six level switches, with three switches assigned to each train. Within each train, contacts of the three level switches are connected in two-out-of-three (2/3) logic for a HI-HI level trip and alarm. Within each train, contacts of the three level switches are also connected in one-out-of-three (1/3) logic for a HI level alarm.

Annunciator and computer alarms are provided on HI doghouse level to alert the operator to a potential flooding condition. Each train of doghouse level instrumentation provides inputs to its own annunciator window and computer alarm through an appropriate isolation device.

Any doghouse level switch that senses a HI-HI level condition will initiate an alarm on the plant computer. Should two-out-of-three doghouse level switches in any train sense a HI-HI level condition, the following actions will be initiated:

At an 11 inch setpoint the following occurs:

1. Trip Main Feedwater Pump Turbines (MFWPT)
2. Close the S/G Temper Flow to Auxiliary Feedwater Nozzles Valve
3. Close the S/G Temper Flow to Auxiliary Feedwater Nozzle Valve Bypass Valve

Also, dependent on whether the flooding has occurred in the inner or the outer doghouse, the following devices will close to isolate feedwater flow to the affected doghouse.

1. S/G Feedwater Flow Control Valves
2. S/G Feedwater Flow Control Bypass Control Valves
3. S/G Main Feedwater Containment Isolation Valves
4. S/G Main Feedwater Reverse Purge Isolation Valves
5. S/G Main Feedwater Bypass to Auxiliary Feedwater Nozzle Valves
6. S/G Tempering Flow to Auxiliary Feedwater Nozzle Valves

7.6.22.2 Design Bases

The doghouse water level switches and controls are designed to assure proper response to a postulated pipe break in a doghouse and availability of safety related equipment located in these areas.

7.6.22.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, these requirements are not directly applicable to these controls. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below.

7.6.22.3.1 General Functional Requirements

The instrumentation and controls associated with doghouse water level are designed with reliability and redundance to automatically initiate their safety function.

7.6.22.3.2 Single Failure Criterion

The doghouse water level instrumentation and controls are designed such that no single failure can prevent the safety function from being performed.

7.6.22.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.22.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.22.3.5 Channel Integrity

The redundant trains of the safety related instrumentation and controls associated with doghouse water level monitoring are designed to maintain their functional capability.

7.6.22.3.6 Channel Independence

The redundant trains of safety-related instrumentation and controls associated with doghouse water level monitoring are physically separated and electrically isolated as discussed in Section 8.3.1.4.

7.6.22.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls for doghouse water level monitoring are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.22.3.8 Derivation of System Inputs

System inputs are derived from direct measurement of the desired variables.

7.6.22.3.9 Capability for Test, Calibration, and Sensor Checks

The safety-related instrumentation and controls are designed to facilitate testing and calibration as required by the Technical Specifications.

7.6.22.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls associated with doghouse water level are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.22.3.11 Operating Bypasses

The doghouse water level instrumentation and controls do not employ operating bypasses in their initiating logic.

7.6.22.3.12 Indication of Bypass

The doghouse water level instrumentation has no designed bypass capability and therefore no indication of a bypass is provided.

7.6.22.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the doghouse water level instrumentation inoperable is controlled by administrative and security measures.

7.6.22.3.14 Multiple Setpoints

Annunciator alarms are initiated at the 5 inch water level in the doghouse while trip outputs are initiated at the 11 inch setpoint.

7.6.22.3.15 Completion of Protection Action Once it is Initiated

Once initiated the doghouse water level instrumentation and controls continue to perform their safety function until the condition requiring its operation has been eliminated.

7.6.22.3.16 Manual Initiation

There is no system level manual initiation associated with doghouse water level monitoring.

7.6.22.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points for the safety-related instrumentation and controls associated with doghouse level monitoring are controlled by administrative and security measures.

7.6.22.3.18 Identification of Protective Action

The safety-related instrumentation and controls associated with doghouse level monitoring are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.22.3.19 Information Read-Out

Information read-outs are provided in the control room to allow confirmation of system safety functions.

7.6.22.3.20 System Repair

The doghouse water level instrumentation and controls are designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.22.3.21 Identification

The safety-related instrumentation and control equipment associated with doghouse level monitoring is physically identified as described in Section 7.1.2.3.

7.6.23 Boron Dilution Mitigation System

7.6.23.1 Description

The shutdown margin monitor portion of the Boron Dilution Mitigation System (BDMS) measures the count rate from a neutron counting instrument. It performs a statistical time average of the neutron count rate and displays this average if in the source range (from 0.1 counts per second (cps) to 10,000 cps). It also provides an alarm output to indicate a decrease in reactor shutdown margin when the count rate increases by an amount determined by the preset alarm ratio. The shutdown monitor alarm setpoint is continuously recalculated and automatically reduced as the reactor is shutdown and the neutron flux is reduced. When the neutron count rate achieves a steady value and then eventually increases, the alarm setpoint remains at its lowest value unless it is manually reset. An alarm will occur when the time averaged neutron count rate increases due to a reactivity addition to a value determined by the preset alarm setpoint. The response time for the alarm depends on the initial count rate and the rate of change of neutron flux. The preset alarm ratio is chosen to ensure an early alarm will occur during an inadvertent boron dilution event. Analysis of inadvertent boron dilution events is discussed in Section 15.4.6. There are two redundant alarm channels. In addition to providing an alarm on the main control boards, an alarm in either channel will automatically: 1) Close the

respective train related valve, NV188A or NV189B (if valves NV252A or NV253B, respectively, have begun to open), in the charging pump suction line from the volume control tank (see Figure 9-90) thereby isolating the pumps from sources of water for boron dilution; and 2) Stop both reactor makeup water pumps (see Figure 9-98) to provide added assurance that unborated water is not introduced into dilution pathways; and 3) Open the respective train related valve, NV252A or NV253B, (see Figure 9-96) in order to align the refueling water storage tank (a source of borated water) with the charging pumps.

7.6.23.2 Design Bases

The Boron Dilution Mitigation System is designed to protect the reactor from an inadvertent criticality by automatically stopping the flow of unborated water.

7.6.23.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard; therefore, those requirements are not directly applicable to these controls. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below.

7.6.23.3.1 General Functional Requirement

The BDMS functions reliably and automatically to prevent inadvertent recriticality due to boron dilution. The BDMS will also provide an alarm to indicate increasing count rate from any cause that might lead to inadvertent criticality.

7.6.23.3.2 Single Failure Criterion

Controls for the BDMS are designed such that a single failure can not prevent proper action at the system level. The single failure criterion is met by assuring physical and electrical separation between the redundant trains.

7.6.23.3.3 Quality of Components

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.23.3.4 Equipment Qualification

Qualification of this electrical equipment is discussed in Reference 1.

7.6.23.3.5 Channel Integrity

The redundant trains of safety-related controls for the BDMS are designed to assure system functional capability.

7.6.23.3.6 Channel Independence

The safety-related instrumentation and controls for the BDMS are physically separated trains and electrically isolated as discussed in Section 8.3.1.4.

7.6.23.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls of the BDMS are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.23.3.8 Derivation of System Inputs

The inputs to the BDMS are derived from direct measurements of neutron flux (excore).

7.6.23.3.9 Capability for Test, Calibration, and Sensor Checks

The BDMS safety-related instrumentation and controls are designed to facilitate testing and calibration as required by the Technical Specifications.

7.6.23.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls of the BDMS are train related and do not include protection channels as defined in IEEE 279-1971.

System redundancy is reduced when the BDMS is tested; however, testing requires only a short period during the modes of operation when the BDMS is operational.

BDMS interlock defeat is provided to facilitate on-line maintenance and to prevent inadvertent equipment operation at extremely low and extremely high count-rates.

Indication is provided in the main control room when either train of the BDMS has been made inoperable at a system level by loss of electrical power.

7.6.23.3.11 Operating Bypasses

The BDMS instrumentation and controls employ operating bypasses in their initiating logic. The automatic equipment operation described in Section 7.6.23.1 may be defeated via control board mounted key operated switches. The control room alarm for a sudden increase in count-rate remains in service.

7.6.23.3.12 Indication of Bypass

The automatic operation defeat is indicated on the control board mounted shutdown monitors.

7.6.23.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the BDMS inoperable is controlled by administrative and security measures.

7.6.23.3.14 Multiple Setpoints

Multiple setpoints are not required for the Boron Dilution Mitigation System.

7.6.23.3.15 Completion of Protection Action Once it is Initiated

Once initiated the Boron Dilution Mitigation System will actuate the pumps and valves described in Section 7.6.23.1 to their safe position. Any repositioning must be done manually by the operator.

7.6.23.3.16 Manual Initiation

The valves and pumps described in Section 7.6.23.1 can be manually operated from the control room.

7.6.23.3.17 Access to Setpoint Adjustments, Calibration, and Test Point

Access to setpoint adjustments, calibration, and test points is controlled by administrative and security measures.

7.6.23.3.18 Identification of Protective Action

The safety-related instrumentation and controls of the BDMS are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.23.3.19 Information Read-Out

Indication of the status of the Boron Dilution Mitigation System is provided on safety grade displays in the control room. Control room annunciators alarm actuation of the BDMS and (on separate windows) loss of power to the BDMS.

7.6.23.3.20 System Repair

The BDMS is designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.23.3.21 Identification

The BDMS safety-related instrumentation and control equipment is physically identified as described in Section 7.1.2.3.

7.6.24 References

1. "Gamma-Metrics RCS Series Neutron Flux Monitoring System Qualification Test Report N0-010, Rev-1", June 1983 (Proprietary).

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.6.

THIS PAGE LEFT BLANK INTENTIONALLY.

7.7 Control Systems Not Required for Safety

The general design objectives of the Plant Control Systems are:

1. To establish and maintain power equilibrium between primary and secondary system during steady state unit operation;
2. To constrain operational transients so as to preclude unit trip and re-establish steady state unit operation;
3. To provide the reactor operator with monitoring instrumentation that indicates all required input and output control parameters of the systems and provides the operator the capability of assuming manual control of the system.

7.7.1 Description

The Plant Control Systems described in this section perform the following functions:

1. Reactor Control System
   a. Enables the nuclear plant to accept a step load increase or decrease of 10 percent and a ramp increase or decrease of 5 percent per minute within the load range of 15 percent to 100 percent without reactor trip, steam dump, or pressurizer relief actuation, subject to possible xenon limitations.
   b. Maintains reactor coolant average temperature (T_{avg}) within prescribed limits by creating the bank demand signals for moving groups of full length rod cluster control assemblies during normal operation and operational transients. The T_{avg} control also supplies a signal to pressurizer water level control, and steam dump control.
2. Rod Control System
   a. Provides for reactor power modulation by manual or automatic control of full length control rod banks in a preselected sequence and for manual operation of individual banks.
   b. Systems for monitoring and indicating
      1) Provide alarms to alert the operator if the required core reactivity shutdown margin is not available due to excessive control rod insertion.
      2) Display control rod position.
      3) Provide alarms to alert the operator in the event of control rod deviation exceeding a preset limit.
3. Plant Control System Interlocks
   a. Prevent further withdrawal of the control banks when signal limits are approached that predict the approach of a DNBR limit or kw/ft limit.
   b. Inhibit automatic turbine load change as required by the Nuclear Steam Supply System.
4. Pressurizer Pressure Control

   Maintains or restores the pressurizer pressure to the design pressure ±30 psi (which is well within reactor trip and relief and safety valve actuation setpoint limits) following normal operational transients that induce pressure changes by control (manual or automatic) of

heaters and spray in the pressurizer. Provides steam relief by controlling the power relief valves.

5. Pressurizer Water Level Control

   Establishes, maintains, and restores pressurizer water level within specified limits as a function of the average coolant temperature. Changes in level are caused by coolant density changes induced by loading, operational, and unloading transients. Level changes are produced by means of charging flow control (manual or automatic) as well as by manual selection of letdown orifices. Maintaining coolant level in the pressurizer within prescribed limits by actuating the charging and letdown system thus provides control of the reactor coolant water inventory.

6. Steam Generator Water Level Control

   a. Establishes and maintains the steam generator water level to within predetermined physical limits during normal operating transients.

   b. The Steam Generator Water Level Control System also restores the steam generator water level to within predetermined limits at unit trip conditions. It regulates the feedwater flow rate such that under operational transients the heat sink for the Reactor Coolant System does not decrease below a minimum. Steam generator water inventory control is manual or automatic through the use of feed water control valves.

7. Steam Dump Control

   a. Permits the nuclear plant to accept a sudden loss of load without incurring reactor trip. Steam is dumped to the condenser and/or the atmosphere as necessary to accommodate excess power generation in the reactor during turbine load reduction transients.

   b. Insures that stored energy and residual heat are removed following a reactor trip to bring the plant to equilibrium no-load conditions without actuation of the steam generator safety valves.

   c. Maintains the plant at no-load conditions and permit a manually controlled cooldown of the plant.

8. Incore Instrumentation

   Provides information on the neutron flux distribution and on the core outlet temperatures at selected core locations.

7.7.1.1 Reactor Control System

The Reactor Control System enables the nuclear plant to follow load changes automatically including the acceptance of step load increases or decreases of 10 percent and ramp increases or decreases of 5 percent per minute within the load range of 15 percent to 100 percent without reactor trip, steam dump, or pressure relief (subject to possible xenon limitations). The system is also capable of restoring coolant average temperature to within the programmed temperature deadband following a change in load. Manual control rod operation may be performed at any time.

The Reactor Control System controls the reactor coolant average temperature by regulation of control rod bank position. The reactor coolant loop average temperatures are determined from hot leg and cold leg measurements in each reactor coolant loop. There is an average coolant temperature (T_{avg}) computed for each loop, where:

$$T_{avg} = \frac{T_{hot} + T_{cold}}{2}$$

The error between the programmed reference temperature (based on turbine impulse chamber pressure) and the second highest of the T_{avg} measured temperatures (which is processed through a lead-lag compensation unit) from each of the reactor coolant loops constitutes the primary control signal as shown in general on Figure 7-18 and in more detail on the instrumentation and control system diagrams shown in Figure 7-2, pages 11 and 12. The system is capable of restoring coolant average temperature to the programmed value following a change in load. The programmed coolant temperature increases linearly with turbine load from zero power to the full power condition. The T_{avg} also supplies a signal to pressurizer level control and steam dump control and rod insertion limit monitoring.

The temperature channels needed to derive the temperature input signals for the Reactor Control System are fed from protection channels via isolation amplifiers.

An additional control input signal is derived from the reactor power versus turbine load mismatch signal. This additional control input signal improves system performance by enhancing response and reducing transient peaks.

The core axial power distribution is controlled during load follow maneuvers by changing (a manual operator action) the boron concentration in the reactor coolant system. The control board $\Delta\Phi$ displays (Section 7.7.1.3.1) indicate the need for an adjustment in the axial power distribution. Adding boron to the reactor coolant will reduce T_{avg} and cause the rods (through the rod control system) to move toward the top of the core. This action will reduce power peaks in the bottom of the core. Likewise, removing boron from the reactor coolant will move the rods further into the core to control power peaks in the top of the core.

7.7.1.2 Rod Control System

7.7.1.2.1 Full Length Rod Control System

The full length rod control system receives rod speed and direction signals from the T_{avg} control system. The rod speed demand signal varies over the corresponding range of 3.75 to 45 inches per minute (6 to 72 steps/minute) depending on magnitude of the input signal. Manual control is provided to move a control bank in or out at a prescribed fixed speed.

When the turbine load reaches approximately 15 percent of rated load, the operator may select the "AUTOMATIC" mode, and rod motion is then controlled by the reactor control systems. A permissive interlock C-5 (See Table 7-12) derived from measurements of turbine impulse chamber pressure prevents automatic control when the turbine load is below 15 percent. In the "AUTOMATIC" mode, the rods are again withdrawn (or inserted) in a predetermined programmed sequence by the automatic programming with the control interlocks (See Table 7-12).

The shutdown banks are moved to the fully withdrawn position at a constant speed by manual control prior to criticality. During normal operations the shutdown banks are kept in the fully withdrawn position, except during the rod movement surveillance required by technical specifications. A reactor trip signal causes them to fall by gravity into the core. There are five shutdown banks.

The control banks are the only rods that can be manipulated under automatic control. Each control bank is divided into two groups to obtain smaller incremental reactivity changes per step.

All rod control cluster assemblies in a group are electrically paralleled to move simultaneously. There is individual position indication for each rod cluster control assembly.

Power to rod drive mechanisms is supplied by two motor-generator sets operating from two separate 600 volt, three-phase buses. Each generator is the synchronous type and is driven by a 150 Hp induction motor. The ac power is distributed to the rod control power cabinets through the two series connected reactor trip breakers.

The variable speed rod drive programmer affords the ability to insert small amounts of reactivity at low speed to accomplish fine control of reactor coolant average temperature about a small temperature deadband, as well as furnishing control at high speed. A summary of the rod cluster control assembly sequencing characteristics is given below.

1. Two groups within the same bank are stepped such that the relative position of the groups will not differ by more than one step.
2. The control banks are programmed such that withdrawal of the banks is sequenced in the following order; control bank A, control bank B, control bank C, and control bank D. The programmed insertion sequence is the opposite of the withdrawal sequence, i.e., the last control bank withdrawn (bank D) is the first control bank inserted.
3. The control bank withdrawals are programmed such that when the first bank reaches a preset position, the second bank begins to move out simultaneously with the first bank. The first bank continues to move until it reaches its fully withdrawn position. When the second bank reaches a preset position, the third bank begins to move out, and so on (these bank overlaps of movement at most permit simultaneous movement of two banks. This withdrawal sequence continues until the unit reaches the desired power level. The control bank insertion sequence is the opposite.
4. Overlap between successive control banks is adjustable between 0 to 50 percent (0 and 116 steps), with an accuracy of ±1 step.
5. Rod speeds for automatic operation of the control banks are capable of being controlled between a minimum of 8 steps per minute and a maximum of 72 steps per minute. Normally, in manual operation, the control bank speeds are fixed at 48 steps per minute and the shutdown banks speed at 64 steps per minute. During special tests (such as Dynamic Rodworth Measurement) the speed of the control and shutdown banks may be increased up to 64 steps per minute for control banks and 72 steps per minute for shutdown banks.

7.7.1.2.2 Rod Control System Failures

Credible rod control equipment malfunctions which could potentially cause inadvertent positive reactivity insertions due to inadvertent rod withdrawal, incorrect overlap or malpositioning of the rods are the following:

1. Failures in the manual rod controls:
   a. Rod Motion Control Switch (In-Hold-Out)
   b. Bank Selector Switch
2. Failures in the overlap and bank sequence program control:
   a. Logic Cabinet Systems
   b. Power Supply Systems

1. Failures in the Manual Rod Controls

The Rod Motion Control switch is a three position lever switch. The three positions are "In," "Hold," and "Out." These positions are effective when the bank selector switch is in manual. Failure of the rod motion control switch (contacts failing short or activated relay failures) would have the potential, in the worst case, to produce positive reactivity insertion by rod withdrawal when the bank selector switch is in the manual position or in a position which selects one of the banks.

When the bank selector switch is in the automatic position, the rods would obey the automatic commands and failures in the rod motion control switch would have no effect on the rod motion regardless of whether the rod motion control switch is in "In," "Hold," or "Out."

In the case where the Bank Selector switch is selecting a bank and a failure occurs in the Rod Motion switch that would command the bank "out" even when the Rod Motion Control switch was in an "In" or "Hold" position the selected bank could inadvertently withdraw. This failure is bounded in the safety analysis (Chapter 15) by the reactivity insertion rate assumptions utilized in the uncontrolled bank withdrawal from subcritical and at power transients. The reactivity insertion rate assumptions are consistent with the withdrawal of two banks.

Failure that can cause more than one group of four mechanisms to be moved at one time within a power cabinet is not a credible event because the circuit arrangement for the movable and lift coils would cause the current available to the mechanisms to divide equally between coils in the two groups (in a power supply). The drive mechanism is designed such that it will not operate on half current. A second feature in this scenario would be the multiplexing failure detection circuit included in each power cabinet. This circuit would stop rod withdrawal (or insertion).

The second case considered in the potential for inadvertent reactivity insertion due to possible failures is when the selector switch is in the manual position. Such a case could produce, with a failure in the rod motion control switch, a scenario where the rods could inadvertently withdraw in a programmed sequence. The overlap and bank sequence are programmed when the selection is in either automatic or manual. This scenario is also bounded by the reactivity values assumed in the SAR accident analysis. In this case, the operator can trip the reactor, or the protection system would trip the reactor via Power Range Neutron Flux-High, or overtemperature ΔT.

Failure of the Bank Selector Switch

A failure of the bank selector switch produces no consequences when the "in-hold-out" manual switch is in the "Hold" position. This is due to the following design feature:

The bank selector switch is series wired with the in-hold-out lever switch for manual and individual control rod bank operation. With the "in-hold-out" lever switch in the "hold" position, the bank selector switch can be positioned without rod movement.

2. Failures in the Overlap and Bank Sequence Program Control

The Rod Control System design prevents the movement of the groups out of sequence as well as limiting the rate of reactivity insertion. The main feature that performs the function of preventing malpositioning produced by groups out of sequence is included in the Block Supervisory Memory Buffer and Control. This circuitry accepts and stores the externally generated command signals. In the event of out of sequence input command to the rods while they are in movement, this circuit will inhibit the buffer memory from accepting the command. If a change of signal command appears, this circuit would stop the system after allowing the slave cyclers to finish their current sequencing. Failure of the components

related to this system will also produce a Rod deviation alarm and insertion limit alarm (see Section 7.7). Failures within the system such as failures of supervisory logic cards, pulser cards, etc., will also cause an urgent alarm. An urgent alarm will be followed by the following actions:

a. Automatic de-energizing of the lift coil and reduced current energizing of the stationary gripper coils and movable gripper coils.

b. Activation of the alarm light on the affected cabinet front panel.

c. Activation of ROD CONTROL URGENT FAILURE annunciation window on the plant annunciator.

The urgent alarm is produced in general by:

d. Regulation failure detector

e. Phase failure detector

f. Logic error detector

g. Multiplexing error detector

h. Interlock failure detector.

i. Logic Cabinet Failures

The rod control system is designed to limit the rod speed control signal output to a value that causes the pulser (logic cabinet) to drive the control rod driving mechanism at 72 steps per minute. If a failure should occur in the pulser or the reactor control system, the highest stepping rate possible is 77 steps per minute, which corresponds to one step every 780 milliseconds. A commanded stepping rate higher than 77 steps per minute would result in "GO" pulses entering a slave cycler while it is sequencing its mechanisms through a 780 millisecond step. This condition stops the control bank motion automatically and alarms are activated locally and in the control room. It also causes the affected slave cycler to reject further "GO" pulses until it is reset.

Failures that cause the 780 millisecond step sequence time to shorten will not result in higher rod speeds since the stepping rate is proportional to the pulsing rate. Simultaneous failures in the pulser or rod control system and in the clock circuits that determine the 780 millisecond stepping sequence could result in higher CRDM speed, however, in the unlikely event of these simultaneous multiple failures the maximum CRDM operation speed would be no more than approximately 100 steps per minute due to mechanical limitation. This speed has been verified by tests conducted on the CRDM's.

Failures Causing Movement Of The Rods Out Of Sequence

No single failure was discovered (Reference 2) that would cause a rapid uncontrolled withdrawal of Control Bank D (taken as worst case) when operating in the automatic bank overlap control mode with the reactor at, or near, full power output. The analysis revealed that many of the failures postulated were in a safe direction and that rod movement is blocked by the rod Urgent Alarm.

j. Power Supply System Failures

Analysis of the power cabinet disclosed no single component failures that would cause the uncontrolled withdrawal of a group of rods serviced by the power cabinet. The

analysis substantiates that the design of a power cabinet is "fail-preferred" in regards to a rod withdrawal accident if a component fails. The end results of the failure is either that of blocking rod movement or that of dropping an individual rod or rods or a group of rods. No failure, within the power cabinet, which could cause erroneous drive mechanism operation will remain undetected. Sufficient alarm monitoring (including "urgent" alarm) is provided in the design of the power cabinet for fault detection of those failures which could cause erroneous operation of a group of mechanisms. As noted in the foregoing, diverse monitoring systems are available for detection of failures that cause the erroneous operation of an individual control rod drive mechanism. Conclusion

In summary, no single failure within the rod control system can cause either reactivity insertions or mal-positioning of the control rods resulting in core thermal conditions not bounded by analyses contained in Chapter 15.

7.7.1.3 Plant Control Signals for Monitoring and Indicating

7.7.1.3.1 Monitoring Functions Provided by the Nuclear Instrumentation System

The power range channels are important because of their use in monitoring power distribution in the core within specified safe limits. They are used to measure power level, axial flux imbalance, and radial flux imbalance. These channels are capable of recording overpower excursions up to 200 percent of full power. Suitable alarms are derived from these signals as described below.

Basic power range signals are:

1. Total current from a power range detector (four such signals from separate detectors); these detectors are vertical and have a total active length of 10 feet.
2. Current from the upper half of each power range detector (four signals).
3. Current from the lower half of each power range detector (four signals).

   Derived from these basic signals are the following (including standard signal processing for calibration).

4. Indicated nuclear power (four signals).
5. Indicated axial flux imbalance ($\Delta\Phi$), derived from upper half flux minus lower half flux (four signals).

   Alarm functions derived are as follows:

6. Deviation (maximum minus minimum of four) in indicated nuclear power.
7. Upper radial tilt (maximum to average of four) on upper-half currents.
8. Lower radial tilt (maximum to average of four) on lower-half currents.

Provision is made to continuously record, on the control board, the eight ion chamber signals, i.e. upper and lower currents for each detector. Nuclear power and axial unbalance are recorded as well. Indicators are provided on the control board for nuclear power and for axial flux imbalance. The axial flux difference imbalance deviation $\Delta\Phi$ alarms are derived from the plant process computer which determines the one minute averages of the excore detector outputs to monitor $\Delta\Phi$ in the reactor core and alerts the operator where $\Delta\Phi$ alarm conditions exist. Two types of alarm messages are output. Above a preset (50 percent) power level, an alarm message is output immediately upon determining a delta flux exceeding the Technical Specification limits. When the alarm on flux difference becomes inoperable and in Mode 1 at

50% rated power or greater, the axial flux difference is logged within one hour and every hour thereafter, until the alarm is available. No power reduction is required during this period of manual surveillance.

Additional background information on the Nuclear Instrumentation System can be found in Reference 1.

7.7.1.3.2 Rod Position Monitoring of Full Length Rods

Two separate systems are provided to sense and display control rod position as described below:

1. Digital Rod Position Indication System

   The digital rod position indication system measures the actual position of each full length rod using a detector which consists of discrete coils mounted concentrically with the rod drive pressure housing. The coils are located axially along the pressure housing and electro-magnetically sense the entry and presence of the rod drive shaft through its centerline. For each detector, the coils are interlaced into two data channels and are connected to the containment electronics (Data A and B) by separate multiconductor cables. By employing two separate channels of information, the digital rod position indication (DRPI) system can continue to function (at reduced accuracy) if one channel fails. Multiplexing is then used to transmit the digital position signals from the containment electronics to the control room area DRPI cabinet. The control room area DRPI process cabinet contains two separate, redundant computer nodes, each receiving the data from one of the containment data cabinets.

   The nodes calculate rod position and communicate with each other to produce a ±4 step composite rod position when operating at full accuracy. The composite rod position is provided to two independent monitors in a display unit on the main control board. Each monitor is capable of displaying the position of all control rods; however, the default arrangement will be to typically display all control banks on one monitor and all shutdown banks on the other. Additional optional display screens are available on each display for diagnostic and testing purposes.

   The composite rod position data is also supplied to the operator aid computer (OAC), which has the same display capabilities as the control board displays.

   The DRPI system provides a rod at bottom indication for each rod, as well as an alarm when any rod is at bottom.

   The DRPI system is split into independent A and B ‘trains’ that are powered from separate 120vac regulated power sources. The B train is powered through a power transfer switch such that the normal source of power is from the unit it is monitoring, and alternate power is provided from the other nuclear unit.

2. Demand Position System - The demand position system counts pulses generated in the rod drive control system to provide a digital readout of the demanded bank position.

The demand position and digital rod position indication systems are separate systems, but safety criteria were not involved in the separation, which was the result only of operational requirements. Operating procedures require the reactor operator to compare the demand and indicated (actual) reading from the rod position indication system so as to verify operation of the rod control system.

7.7.1.3.3 Control Bank Rod Insertion Monitoring

When the reactor is critical, the normal indication of reactivity status in the core is the position of the control bank in relation to reactor power (as indicated by the Reactor Coolant System loop ΔT) and coolant average temperature. These parameters are used to calculate insertion limits for the control banks. Two alarms are provided for each control bank.

1. The "low" alarm alerts the operator of an approach to the rod insertion limits requiring boron addition by following normal procedures with the Chemical and Volume Control System.
2. The "low-low" alarm alerts the operator to take immediate action to stop any dilution in progress. Shutdown margin is subsequently verified above the required minimum or boron is added, and the control bank(s) is restored above its insertion limit setpoint.

The purpose of the control bank rod insertion monitor is to give warning to the operator of excessive rod insertion. The insertion limit maintains sufficient core reactivity shutdown margin following reactor trip and provides a limit on the maximum inserted rod worth in the unlikely event of the hypothetical rod ejection, and limits rod insertion such that acceptable nuclear peaking factors are maintained. Since the amount of shutdown reactivity required for the design shutdown margin following a reactor trip increases with increasing power, the allowable rod insertion limits must be decreased (the rods must be withdrawn further) with increasing power. Two parameters which are proportional to power are used as inputs to the insertion monitor. These are the ΔT between the hot leg and the cold leg, which is a direct function of reactor power, and T_{avg}, which is programmed as a function of power. The rod insertion monitor uses parameters for each control rod bank as follows:

$$Z_{LL} = A(\Delta T)_{auct} + B(T_{avg})_{auct} + C$$

where:

Z_{LL}	=	Maximum permissible insertion limit for affected control bank
$(\Delta T)_{auct}$	2^{nd} Highest ΔT of all loops	
$(T_{avg})_{auct}$	2^{nd} Highest T_{avg} of all loops	
A,B,C	= Constants chosen to maintain $Z_{LL} \geq$ actual limit based on physics calculations	

The control rod bank demand position (Z) is compared to Z_{LL} as follows:

$$\text{If } Z - Z_{LL} \leq D \text{ a low alarm is actuated}$$

$$\text{If } Z - Z_{LL} \leq E \text{ a low} - \text{low alarm is actuated.}$$

Since the 2^{nd} highest value of T_{avg} and ΔT are chosen by auctioneering, a conservatively high representation of power is used in the insertion limit calculation.

Actuation of the low alarm alerts the operator of an approach to a reduced shutdown reactivity situation. Administrative procedures require the operator to add boron through the Chemical and Volume Control System. Actuation of the low-low alarm requires the operator to stop any dilution in progress. Shutdown margin is subsequently verified above the required minimum or boron is added, and the control bank(s) is restored above its insertion limit setpoint. The value for "E" is chosen such that the low-low alarm would normally be actuated before the insertion limit is exceeded. The value for "D" is chosen to allow the operator to follow normal boration procedures. Figure 7-19 shows a block diagram representation of the control rod bank insertion monitor. The monitor is shown in more detail on the functional diagrams shown in Figure 7-2,

pages 11 and 12. In addition to the rod insertion monitor for the control banks, the plant computer, which monitors individual rod positions, provides an alarm that is associated with the rod deviation alarm discussed in Section 7.7.1.3.4. This alarm warns the operator if any shutdown rod cluster control assembly leaves the fully withdrawn position.

Rod insertion limits are established by:

1. Establishing the allowed rod reactivity insertion at full power consistent with the purposes given above.
2. Establishing the differential reactivity worth of the control rods when moved in normal sequence.
3. Establishing the change in reactivity with power level by relating power level to rod position.
4. Linearizing the resultant limit curve. All key nuclear parameters in this procedure are measured as part of the initial and periodic physics testing program.

Any unexpected change in the position of the control bank under automatic control, or a change in coolant temperature under manual control, provides a direct and immediate indication of a change in the reactivity status of the reactor. In addition, samples are taken periodically of coolant boron concentration. Variations in concentration during core life provide an additional check on the reactivity status of the reactor, including core depletion.

7.7.1.3.4 Rod Deviation Alarm

The demanded and measured rod position signals are displayed on the control board. These signals are also monitored by the plant computer which provides a visual printout and an audible alarm if an individual rod position signal deviates from the bank demand position by 12 steps. (This rod to bank comparison deviation limit is such that the 24 step rod to rod deviation limit within a bank is enveloped.) The alarm can be set with appropriate allowance for instrument error and within sufficiently narrow limits to preclude exceeding core design hot channel factors. The deviation alarm of a shutdown rod is based on a Preset insertion limit belong exceeded.

Figure 7-20 is a block diagram of the rod deviation comparator and alarm system implemented by the plant computer.

7.7.1.3.5 Rod Bottom Alarm

A rod bottom signal for the rods in the digital rod position system is used to operate a control relay, which generates the "RPI AT BOTTOM ROD DROP" alarm.

7.7.1.4 Plant Control System Interlocks

The listing of the plant control system interlocks, along with the description of their derivations and functions, is presented in Table 7-12. It is noted that the designation numbers for these interlocks are preceded by "C". The development of these logic functions is shown in the instrumentation and control diagrams (Figure 7-2 pages 11 through 25).

7.7.1.4.1 Rod Stops

Rod stops are provided to prevent abnormal power conditions which could result from excessive control rod withdrawal initiated by either a control system malfunction or operator violation of administrative procedures.

Rod stops are the C_1, C_2, C_3, C_4, and C_5 control interlocks identified in Table 7-12. The C_3 rod stop, derived from overtemperature ΔT, and the C_4 rod stop, derived from overpower ΔT, are also used for turbine runback, which is discussed below.

7.7.1.4.2 Automatic Turbine Load Runback

Automatic turbine load runback is initiated by an approach to an overpower or overtemperature condition. This will prevent high power operation that might lead to an undesirable condition, which, if reached, will be protected by reactor trip.

Turbine load reference reduction is initiated by either an overtemperature or overpower ΔT signal. Two out of four coincidence logic is used.

A rod stop and turbine runback are initiated when

$$\Delta T > \Delta T_{\text{rod stop}}$$

for both the overtemperature and the overpower condition.

For either condition in general

$$\Delta T_{\text{rod stop}} = \Delta T_{\text{setpoint}}{}^{-B}p$$

Where:

$$B_p = \text{a setpoint bias}$$

where ΔT setpoint refers to the overtemperature ΔT reactor trip value and the overpower ΔT reactor trip value for the two conditions.

The turbine runback is continued until ΔT is equal to or less than $\Delta T_{\text{rod stop}}$.

This function serves to maintain an essentially constant margin to trip.

7.7.1.4.3 Turbine Loading Stop

An interlock (C-16) is provided to limit turbine loading during a rapid return to power transient when a reduction in reactor coolant temperature is used to increase reactor power (through the negative moderator coefficient). This interlock limits the drop in coolant temperature to prevent exceeding cooldown accident limits and preserves satisfactory steam generator operating conditions. Subsequent automatic turbine loading can begin after the interlock has been cleared by an increase in coolant temperature which is accomplished by reducing the boron concentration in the coolant.

7.7.1.5 Pressurizer Pressure Control

The Reactor Coolant System pressure is controlled by using either the heaters (in the water region) or the spray (in the steam region) of the pressurizer plus steam relief for large transients. The electrical immersion heaters are located near the bottom of the pressurizer. A portion of the heater group is proportionally controlled to correct small pressure variations. These variations are due to heat losses, including heat losses due to a small continuous spray. The remaining (backup) heaters are turned on when the pressurizer pressure controlled signal demands approximately 100 percent proportional heater power.

The spray nozzles are located on the top of the pressurizer. Spray is initiated when the pressure controller spray demand signal is above a given setpoint. The spray rate increases proportionally with increasing spray demand signal until it reaches a maximum value.

Steam condensed by the spray reduces the pressurizer pressure. A small continuous spray is normally maintained to reduce thermal stresses and thermal shock and to help maintain uniform water chemistry and temperature in the pressurizer.

Power relief valves limit system pressure for large positive pressure transients. In the event of a large load reduction, not exceeding the design plant load rejection capability, the pressurizer power operated relief valves might be actuated for the most adverse conditions, e.g., the most negative Doppler coefficient, and the maximum incremental rod worth. The relief capacity of the power operated relief valves is sized large enough to limit the system pressure to prevent actuation of high pressure reactor trip for the above condition.

A block diagram of the Pressurizer Pressure Control System is shown on Figure 7-21.

7.7.1.6 Pressurizer Water Level Control

The pressurizer operates by maintaining a steam cushion over the reactor coolant. As the density of the reactor coolant adjusts to the various temperatures, the steam water interface moves to absorb the variations with relatively small pressure disturbances.

The water inventory in the Reactor Coolant System is maintained by the Chemical and Volume Control System. During normal plant operation, the charging flow varies to produce the flow demanded by the pressurizer water level controller.

The pressurizer water level is programmed as function of coolant average temperature with second highest being used. The pressurizer water level decreases as the load is reduced from full load. This is a result of coolant contraction following programmed coolant temperature reduction from full power to low power. The programmed level is designed to match as nearly as possible the level changes resulting from the coolant temperature changes.

To control pressurizer water level during startup and shutdown operations, the charging flow is manually regulated from the main control room.

A block diagram of the Pressurizer Water Level Control System is shown on Figure 7-22.

7.7.1.7 Steam Generator Water Level Control

Each steam generator is equipped with a three element feedwater flow controller which receives inputs of Steam Flow, Feed Flow, Steam Pressure, Nuclear Instrumentation System, Steam Generator Narrow Range Level, Steam Generator Wide Range Level, and Feedwater Temperature. In the Feedwater Control System (FCS), these inputs are used to calculate a feedwater control demand.

This demand is sent to a calculator where the appropriate position for both the feedwater control valve (FCV) and the feedwater control bypass valve (FCBV) and feedpump demand is determined.

Feedwater temperature is used to determine the gain of the controller. Feedwater pump speed is set to a programmed value based on a calculation of whichever S/G has the highest demand for feedwater. Adjustments to the programmed speed are made if feedwater is being supplied via the upper nozzles or if a low pressure diffeential condition exists between the Steam Header and the Feedwater Header.

Continued delivery of feedwater to the steam generators is required as a sink for the heat stored and generated in the reactor following a reactor trip and turbine trip. An override signal closes all feedwater valves when the average coolant temperature is below a given temperature and the reactor has tripped. Manual overide of the feedwater control system is available at all times.

Block diagrams of the Steam Generator Water Level Control System and the Main Feedwater Pump Speed Control System are shown in Figure 7-23 and Figure 7-24.

When the nuclear plant is operating at very low power levels (as during startup), the steam and feedwater flow signals will not be usable for control. The FCS uses a low power strategy which is based on narrow range level, but with wide range used as a feedforward signal. Feedwater temperature is also used at low power to change the gain of the controller, but not by the same algorithm used at high power. Feedwater temperature has a larger impact at low power.

The low power control strategy also uses the feedwater control demand calculator and controls both the feedwater control valve (FCV) and the feedwater control bypass valve (FCBV) and the feedwater pump speed.

FCS receives multiple inputs for each process variable. The following signals are used for control, second highest narrow range level, second highest nuclear power, second highest feedwater temperature, median selected wide range level, median feedwater flow and arbitrated steam flow. Two channels of steam flow are arbitrated against second highest delta temperature. FCS will maintain a steady control function during the switch to manual operation. Steam line pressure inputs to FCS originate in the 7300 protection system. The protection functions include: Steam Line Pressure-Low and Steam Line Pressure-Negative Rate functions, which are 2/3 logic.

Because of the median select function in FCS, Section 4.7 of IEEE 279-1971 and GDC 24 requirements concerning Control and Protection Systems interaction are satisfied. Although control signals for Steam Pressures are derived from protection sets, a 2/3 coincidence logic exists. Two out of four coincidence logic is required where a single random failure can cause a control system action that results in a condition requiring protective action. 2/4 coincidence logic is also required if a single random failure can prevent proper action of a protective system channel designed to protect against the condition. The remaining three redundant protection channels would be capable of providing the protective action even if degraded by a second random failure.

7.7.1.8 Steam Dump Control

The steam dump system is designed to accept sudden loss of load without tripping the reactor. The automatic steam dump system is able to accommodate load rejection and to reduce the effects of the transient imposed upon the Reactor Coolant System. By bypassing main steam directly to the condenser, an artificial load is maintained on the primary system. In the event load rejection exceeds 30 percent step or 15 percent/min, main steam is dumped to the atmosphere also. The Rod Control System can then reduce the reactor temperature to a new equilibrium value without causing overtemperature and/or overpressure conditions.

If the difference between the reference T_{avg} (T_{ref}), based on median turbine impulse chamber pressure and the lead/lag compensated second highest T_{avg} exceeds a predetermined amount, and the interlock mentioned below is satisfied, a demand signal will actuate the steam dump to maintain Reactor Coolant System temperature within control range until a new equilibrium temperature is reached. This occurs only if the load rejection is sensed by a falling T_{ref}. Increasing T_{avg} alone will not activate the steam dumps. Since T_{ref} is developed using the

median signal of the three turbine impulse pressure transmitters, the loss of one transmitter will not cause an inadvertent steam dump actuation. T_{avg} is based on the second highest of the four T_{avg} signals (in lieu of the auctioneered high) which will minimize the impact to control should T_{avg} signal failure occur. To prevent actuation of the steam dump on small load perturbations, an independent load rejection sensing circuit is provided. This circuit senses the rate of decrease in the turbine load as detected by the turbine impulse chamber pressure. It is provided to unblock the dump valves when the rate of load rejection exceeds a preset value corresponding to a 10 percent step load decrease or a sustained ramp load decrease of 5 percent/min.

The setpoints were based on maintaining adequate control system performance over the entire range of the predicted plant operating conditions.

The steam dump control system allows for a sequential operation of the six (6) individual valves in the first two modulating banks. After the first two modulating banks have opened, the remaining dump valves are modulated sequentially, one bank at a time. The third bank does not begin to modulate open until the first two banks have received a signal to modulate fully open; the fourth bank does not begin to modulate open until the first, second and third banks have received signals to modulate fully open, etc. The sequence for modulating the valves closed shall be the reverse of the opening; i.e., the fifth bank to open is the first bank to close, etc.

The following process signals are used in the steam dump control system:

- Selected Steam Pressure
  - 2^{nd} Highest of the median steam pressure from each loop 12 transmitters (3 per loop)
  - Alternate steam pressure signal is steam header pressure transmitter
- Selected T_{avg}
  - 2^{nd} Highest
- Median Selected Turbine Impulse Pressure
  - 2 channels for Reactor Protection Control System
  - 1 channel wired directly to the steam dump control system
  - Used to develop T_{ref} for load rejection controller
  - C-5 interlock
- Turbine Impulse Pressure for C7 - A&B
  - Developed independent of median selected turbine impulse pressure
  - Developed by taking 2 of 3 rate of change > than 10 and 30%

A block diagram of the Steam Dump Control System is shown in Figure 7-25.

Deleted Per 2012 Update.

7.7.1.8.1 Load Rejection Steam Dump Controller

This circuit prevents large increase in reactor coolant temperature following a large, sudden load decrease. The error signal is a difference between the second highest T_{avg} and the reference T_{avg} as based on turbine impulse chamber pressure.

The T_{avg} signal used in steam dump control is diverse from the signal used in the Reactor Coolant System. The lead/lag compensation for the T_{avg} signal is to compensate for lags in the plant thermal response and in valve positioning. Following a sudden load decrease, T_{ref} is immediately decreased and T_{avg} increases, thus generating an immediate demand signal for steam dump. Since control rods are available, in this situation steam dump terminates as the error comes within the maneuvering capability of the control rods.

7.7.1.8.2 Plant Trip Steam Dump Controller

Following a reactor trip, the load rejection steam dump controller is defeated, and the plant trip steam dump controller becomes active. Since control rods are not available in this situation, the demand signal is the error signal between the second highest T_{avg} and the no-load reference T_{avg}.. When the error signal exceeds a predetermined setpoint, the dump valves are tripped open in a prescribed sequence. As the error signal reduces in magnitude indicating that the Reactor Coolant System T_{avg} is being reduced toward the reference no-load value, the dump valves are modulated by the plant trip controller to regulate the rate of decay heat removal and thus gradually establish the equilibrium hot shutdown condition.

Following a reactor trip the steam dump capacity requirement is only that necessary to maintain steam pressure below the steam generator relief valve setpoint (≅40 percent capacity to the condenser); therefore, only the first two groups of valves are opened. The error signal determines whether a group is to be tripped open or modulated open. In either case, they are modulated when the error is below the trip-open setpoints.

7.7.1.8.3 Steam Header Pressure Controller

Residual heat removal is maintained by the steam generator pressure controller (manually selected) which controls the amount of steam flow to the condensers. This controller operates a portion of the same steam dump valves to the condensers which are used during the initial transient following turbine reactor trip on load rejection.

7.7.1.9 Incore Instrumentation

The Incore Instrumentation System consists of chromel-alumel thermocouples at fixed core outlet positions and movable miniature neutron detectors which can be positioned at the center of selected fuel assemblies, anywhere along the length of the fuel assembly vertical axis. The basic system for insertion of these detectors is shown in Figure 7-26.

7.7.1.9.1 Thermocouples

Chromel-alumel thermocouples are threaded into guide tubes that penetrate the reactor vessel head through seal assemblies, and terminate at the exit flow end of the fuel assemblies. The thermocouples are provided with two primary seals, a conoseal and swage type seal from conduit to head. Thermocouple readings are monitored by the computer with backup readout provided by a precision indicator with manual point selection located in the control room. Information from the incore instrumentation is available even if the computer is not in service.

7.7.1.9.2 Movable Neutron Flux Detector Drive System

Miniature fission chamber detectors can be remotely positioned in retractable guide thimbles to provide flux mapping of the core. The stainless steel detector shell is welded to the leading end of helical wrap drive cable and to stainless steel sheathed coaxial cable. The retractable thimbles, into which the miniature detectors are driven, are pushed into the reactor core through

conduits which extend from the bottom of the reactor vessel down through the concrete shield area and then up to a thimble seal table. Their distribution over the core is nearly uniform with about the same number of thimbles located in each quadrant.

The thimbles are closed at the leading ends, and dry inside, and serve as the pressure barrier between the reactor water pressure and the atmosphere. Mechanical seals between the retractable thimbles and the conduits are provided at the seal line. During reactor operation, the retractable thimbles are stationary. They are extracted downward from the core during refueling to avoid interference within the core. A space above the seal line is provided for the retraction operation.

The drive system for the insertion of the miniature detectors consists basically of drive assemblies, five path rotary transfer assemblies, and ten path rotary transfer assemblies, as shown in Figure 7-26. The drive system pushes hollow helical wrap drive cables into the core with the miniature detectors attached to the leading ends of the cables and small diameter sheathed coaxial cables threaded through the hollow centers back to the ends of the drive cables. Each drive assembly consists of a gear motor which pushes a helical wrap drive cable and a detector through a selective thimble path by means of a special drive box and includes a storage device that accommodates the total drive cable length.

Manual isolation valves (one for each thimble) are provided for closing the thimbles. When closed, the valves form a 2500 psig barrier. The manual isolation valves are not designed to isolate a thimble while a detector/drive cable is inserted into the thimble. The detector/drive cable must be retracted to a position above the isolation valve prior to closing the valve.

A small leak would probably not prevent access to the isolation valves and thus a leaking thimble could be isolated during a hot shutdown. A large leak might require cold shutdown for access to the isolation valve.

The NRC issued IE Bulletin 88-09, "Thimble Tube Thinning in Westinghouse Reactors," on July 26, 1988. The purpose of this bulletin was to request that licensees establish an inspection program to periodically confirm incore neutron monitoring system thimble tube integrity. Subsequently, inspections and evaluations were performed on the Unit 1 and Unit 2 neutron monitoring system thimble tubes, and the requested program to periodically verify thimble tube integrity was established (letters from H.B. Tucker to the NRC, dated March 16, 1989, April 18, 1989, and October 1, 1990; and letter from M.S. Tuckman to the NRC, dated December 6, 1990). Specifically, inspections will be periodically performed based on estimations from the data obtained in the above and future inspections, and that future action to assure thimble tube integrity (e.g., repositioning, capping or replacement) will be determined by the results of future re- inspections and the recommendations of the Westinghouse Owners Group Report of the subject. NRC approval of the DPC responses for IE Bulletin 88-09 was issued in a letter to M.S. Tuckman on May 16, 1991.

7.7.1.9.3 Control and Readout Description

The control and readout system provides means for inserting the miniature neutron detectors into the reactor core and withdrawing the detectors while plotting neutron flux versus detector position. The control system is located in the control room. Limit switches in each transfer device provide feedback of path selection operation. Each gear box drives an encoder for position feedback. One five path operation selector is provided for each drive unit that is then used to route a detector into any one of up to ten selectable paths. A common path is provided to permit cross calibration of the detectors.

The control room contains the necessary equipment for control, position indication, and flux recording for each detector.

A "flux-mapping" consists, briefly, of selecting (by panel switches) flux thimbles in given fuel assemblies at various core quadrant locations. The detectors are driven to the top of the core and stopped automatically. An x-y plot (position versus flux level) is initiated with the slow withdrawal of the detectors through the core from the top to a point below the bottom. In a similar manner other core locations are selected and plotted. Each detector provides axial flux distribution data along the center of a fuel assembly.

Various radial positions of detectors are then compared to obtain a flux map for a region of the core.

The number and location of these thimbles have been chosen to permit measurement of local to average peaking factors to an accuracy of ±5 percent (95 percent confidence). Measured nuclear peaking factors will be increased by 5 percent to allow for this accuracy. If the measured power peaking is larger than acceptable, reduced power capability will be indicated.

Operating plant experience has demonstrated the adequacy of the Incore Instrumentation in meeting the design bases stated.

7.7.1.10 Boron Concentration Measurement System

This system is not currently used at Catawba due to maintenance problems that have not been resolved satisfactorily. In its place, Catawba relies on sampling of the Reactor Coolant System for soluble boron concentration.

The Boron Concentration Measurement System was designed for use as an advisory system. It was not designed as a safeguards system or component of safeguards system. The Boron Concentration Measurement System was not part of a control element or control system, nor was it designed for this use. No credit is taken for this system in any accident analysis.

7.7.1.11 ATWS Mitigation Actuation Circuitry

An Anticipated Transient Without Scram (ATWS) is an anticipated occurrence (such as loss of feedwater, condenser vacuum, or offset power) which is accompanied by a failure of the Reactor Trip System (RTS) to shut down the reactor.

The ATWS Mitigation System and Actuation Circuitry (AMSAC) at Catawba Nuclear Station is based on the Westinghouse Owners Group WCAP-10858-PA, Rev. 1, Generic Design 3. The AMSAC design for Catawba is based on conditions that indicate a loss of main feedwater event, which if accompanied by a failure of the RPS to scram leads to overpressurization of the Reactor Coolant System (RCS). The system monitors the position of all Main Feedwater Control Valves, Feedwater Bypass Control Valves, and Feedwater Isolation Valves (Unit 1 only) and the operating status of both main feedwater pumps. The generic design and the Catawba specific AMSAC design have been approved by NRC as meeting the compliance requirements of the ATWS rule, 10CFR50.62 (References 3, 4, 5, 6).

Description

AMSAC actuation will occur when either both main feedwater pumps trip or when main feedwater flow to the steam generators is blocked due to valves closing in the line. When an actuation occurs, the AMSAC circuitry will perform the following:

1. Trip the main turbine
2. Start both motor driven auxiliary feedwater pumps

3. Close the steam generator blowdown and sampling valves

Annunciators, status indicators, and computer alarms in the control room are also available.

To monitor the operating status of the main feedwater pumps, pressure switches are used that monitor the hydraulic control oil pressure to the stop valves. Each of the feedwater pump turbine stop valves will close when the pump turbine trips. The pressure switches monitor the hydraulic oil pressure holding the stop valves open. When a loss of pressure is indicated by 2 of the 3 pressure switches on a pump, the logic circuit will enable the AMSAC circuitry for the tripped pump. If both pump logic circuits are enabled, the AMSAC circuitry will actuate and perform as outlined earlier.

Position of the main feedwater control valves, feedwater control valve bypass valves and main feedwater isolation valves (Unit 1 only) is monitored by limit switches on the valves. These switches are set to enable the AMSAC circuitry when a control valve in a main feedwater flow path is less than 25% open, with the associated control valve bypass valve less than 50% open or when a Feedwater Isolation Valve is closed (Unit 1 only). Minimum AMSAC flow requirements can be maintained with the control valve closed and the control valve bypass valve 50% open. Therefore, the control valve indication is interlocked with the bypass valve indication such that both the control valve and the bypass valve must be closed to the stated setpoints to indicate the blocked flow path.

If 3 out of 4 flow paths are blocked, the AMSAC circuitry will actuate and perform as outlined earlier. A bypass/reset pushbutton with a bypass indication light is installed on a control room control board. The bypass/reset pushbutton provides backup capability by the operator to bypass or reset the AMSAC circuitry should the 2/2 turbine impulse pressure logic (indicating % Reactor Power) fail to perform its automatic bypass/reset functions described below. This bypass is initiated automatically when Reactor Power is below 40% (as indicated by turbine impulse pressure) and after a 120 second time delay. This bypass resets automatically when the Reactor Power is above 40%. A 30 second delay is also installed for the control valve and control valve bypass valve portions of the AMSAC circuitry. This delay will prevent normal valve movements from causing spurious AMSAC actuations at all power levels.

The AMSAC circuitry responds to an ATWS event through new inputs to existing control circuitry. The turbine trip is initiated by an input to the Turbine Control System. Starting the motor driven auxiliary feedwater pumps and closing the blowdown and sampling valves is initiated by an input on the non-safety side of an existing isolation device in the auxiliary feedwater controls. The isolation device separates the non-safety signals from the safety related controls system.

Seismic reviews have been completed for mounting the bypass switch on the control board and for mounting the limit switches onto the control and isolation valves. A 10 CFR 50.48 review has also been performed.

A principal criteria applied to AMSAC is that the AMSAC functions be accomplished without relying on the existing reactor shut down system. Separate equipment is used for AMSAC and for the Reactor Protection System (RPS). The pressure switches which monitor the main feedwater pumps have no RPS interface. The limit switches which monitor the main feedwater control and isolation valves for AMSAC provide no signals to the RPS. The AMSAC logic circuitry has a non-interruptible non-safety 125 VDC power source. The Auxiliary Feedwater, Steam Generator Blowdown and Steam Generator Sampling are systems which are safety related or have safety related components and receive an AMSAC input. The interface with these systems is through an existing non-safety/safety isolation device and is designed so that

the safety related system will perform as designed coincident with a postulated failure of the non-safety AMSAC input.

Non-safety related equipment in the AMSAC circuitry is subject to specific quality assurance identified in NRC Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment that is Not Safety-Related", (Reference 13).

7.7.2 Analysis

The plant control systems are designed to assure high reliability in any anticipated operational occurrences. Equipment used in these system is designed and constructed with a high level of reliability.

Proper positioning of the control rods is monitored in the control room by bank arrangements of the individual position columns for each rod cluster control assembly. A rod deviation alarm alerts the operator of a deviation of one rod cluster control assembly from bank demand position. There are also insertion limit monitors with visual and audible annunciation. A rod bottom alarm signal is provided to the control room for each rod cluster control assembly. Four excore long ion chambers also detect asymmetrical flux distribution indicative of rod misalignment.

Overall reactivity control is achieved by the combination of soluble boron and rod cluster control assemblies. Long term regulation of core reactivity is accomplished by adjusting the concentration of boric acid in the reactor coolant. Short term reactivity control for power changes is accomplished by the Plant Control System which automatically moves rod cluster control assemblies. This system uses input signals including neutron flux, coolant temperature, and turbine load.

The axial core power distribution is controlled by moving the control rods through changes in reactor coolant system boron concentration. Adding boron causes the rods to move out thereby reducing the amount of power in the bottom of the core, this allows power to redistribute toward the top of the core. Reducing the boron concentration causes the rods to move into the core thereby reducing the power in the top of the core, the result redistributes power towards the bottom of the core.

The plant control systems will prevent an undesirable condition in the operation of the plant that, if reached, will be protected by reactor trip. The description and analysis of this protection is covered in Section 7.2. Worst case failure modes of the plant control systems are postulated in the analysis of off-design operational transients and accidents covered in Chapter 15, such as, the following:

1. Uncontrolled rod cluster control assembly withdrawal from a subcritical condition.
2. Uncontrolled rod cluster control assembly withdrawal at power
3. Rod cluster control assembly misalignment
4. Loss external electrical load and/or turbine trip
5. Loss of all AC power to the station auxiliaries (Station Blackout)
6. Excessive heat removal due to feedwater system malfunctions
7. Excessive load increase incident
8. Accidental depressurization of the Reactor Coolant System.

These analyses will show that a reactor trip setpoint is reached in time to protect the health and safety of the public under those postulated incidents and that the resulting coolant temperatures produce a DNBR well above the limiting value of (See Section 4.4.2.1). Thus, there will be no cladding damage and no release of fission products to the Reactor Coolant System under the assumption of these postulated worst case failure modes of the Plant Control System.

A review of IE Bulletin 79-27, Loss of Non-Class IE Instrumentation and Control Power System Bus During Power Operation, Actions 1 thru 3 has been performed and Catawba Nuclear Station was found to be in compliance. Loss of power to any instrumentation and control bus will be alarmed by an audible control room annunciator. Also, a computer point alarm will alert of the specific bus undervoltage condition. Voltmeters are provided in the control room for each DC instrumentation and control bus. Loss of power to any one instrumentation and control bus will not inhibit the ability to reach cold shutdown. Four redundant channels of indication are available for most control and protection system parameters, e.g., pressurizer pressure, S/G level, RCS flow, loop ΔT, Tavg. Other parameters have a minimum of two Control Room indications. Table 7-11 details the number and location of the various indicators. A single power supply failure could eliminate only one of the RPS display channels. Therefore, a loss of any one bus will not result in a loss of control indication in the control room. Relative to non-Class IE non-safety-related power supply inverters: 1) The non-Class IE auxiliary control inverters employ a time delay which is only used to delay an automatic transfer from the alternate source back to the inverter and prevents the transfer until the inverter has synchronized with the alternate source; and 2) The only input voltage to the auxiliary control inverters is a non-safety-related 125 VDC supply; and 3) The non-class IE inverters provide the normal source of power to the auxiliary power panelboards. Each inverter normally feeds its associated panelboard, but during inverter undervoltage or overcurrent conditions, or during an inverter failure, an automatic static switch transfers the affected panelboard to an alternate supply provided from the regulated power distribution centers. The inverter is designed to be current limited such that load exceeding approximately 125% of rated output current will cause a drop in output voltage which will initiate an automatic transfer to the alternate source. IE Circular 79-02 Item No. 2 is not applicable to the Catawba design.

The effect on safety systems of environmentally induced failures in non-safety control systems was addressed in H. B. Tucker's letter of November 23, 1982 to H.R. Denton. An analysis of major NSSS control systems failures has demonstrated that failures of individual sensors, losses of power to protection separation groups, to control groups, to control separation groups, or breaks in common instrument lines all result in events which are bounded by Chapter 15 analyses. Therefore, the FSAR adequately bounds the consequences of these fundamental failures.

7.7.2.1 Separation of Protection and Control System

In some cases, it is advantageous to employ control signals derived from individual protection channels through isolation amplifiers contained in the protection channel. As such, a failure in the control circuitry does not adversely affect the protection channel. Test results have shown that a short circuit or the application (credible fault voltage from within the cabinets) of 118 volts AC or 140 volts DC on the isolated output portion of the circuit (nonprotection side of the circuit) will not affect the input (protection) side of the circuit.

Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels are capable of providing the protective action even when degraded by a second random failure. This meets the applicable requirements of Section 4.7 of IEEE 279-1971.

The pressurizer pressure channels needed to derive the control signals are electrically isolated from control.

7.7.2.2 Response Considerations of Reactivity

Reactor shutdown with control rods is completely independent of the control functions since the trip breakers interrupt power to the rod drive mechanisms regardless of existing control signals. The design is such that the system can withstand accidental withdrawal of control groups or unplanned dilution of soluble boron without exceeding acceptable fuel design limits. The design meets the requirements of General Design Criterion 25.

No single electrical or mechanical failure in the rod control system could cause the accidental withdrawal of a single rod cluster control assembly from the partially inserted bank at full power operation. The operator could deliberately withdraw a single rod cluster control assembly in the control bank; this feature is necessary in order to retrieve a rod, should one be accidentally dropped. In the extremely unlikely event of simultaneous electrical failures which could result in single rod cluster control assembly withdrawal, rod deviation would be displayed on the plant annunciator, and the individual rod position readouts would indicate the relative positions of the rods in the bank. Withdrawal of a single rod cluster control assembly by operator action, whether deliberate or by a combination of errors, would result in activation of the same alarm and the same visual indications.

Each bank of control and shutdown rods in the system is divided into two groups (group 1 and group 2) of up to 4 or 5 mechanisms each. The rods comprising a group operate in parallel through multiplexing thyristors. The two groups in a bank move sequentially such that the first group is always within one step of the second group in the bank. The group 1 and group 2 power circuits are installed in different cabinets as shown in Figure 7-32, which also shows the one group is always within one step (5/8 inch) of the other group. A definite schedule of actuation or deactuation of the stationary gripper, movable gripper, and lift coils of a mechanism is required to withdraw the rod cluster control assembly attached to the mechanism. Since the stationary gripper, movable gripper, and lift coils associated with the rod cluster control assemblies of a rod group are driven in parallel, any single failure which could cause rod withdrawal would affect a minimum of one group of rod cluster control assemblies. Mechanical failures are in the direction of insertion, or immobility.

Figure 7-32 is provided for a discussion of design features that assure that no single electrical failure could cause the accidental withdrawal of a single rod cluster control assembly from the partially inserted bank at full power operation.

The Figure 7-32 shows the typical parallel connections on the lift, movable, and stationary coils for a group of rods. Since single failures in the stationary or movable circuits will result in dropping or preventing rod (or rods) motion, the discussion of single failure will be addressed to the lift coil circuits. 1) Due to the method of wiring the pulse transformers which fire the lift coil multiplex thyristors, three of the four thyristors in a rod group could remain turned off when required to fire, if for example the gate signal lead failed open at point X_1. Upon "up" demand, one rod in group 1 and 4 rods in group 2 would withdraw. A second failure at point X_2 in the group 2 circuit is required to withdraw one rod cluster control assembly, 2) Timing circuit failures will affect the four mechanisms of a group or the eight mechanisms of the bank and will not cause a single rod withdrawal; 3) More than two simultaneous component failures are required (other than the open wire failures) to allow withdrawal of a single rod.

The identified multiple failure involving the least number of components consists of open circuit failure of the proper two out of sixteen wires connected to the gate of the lift coil thyristors. The probability of open wire (or terminal) failure is 0.016E-6 per hour by MIL-HDB-217A. These wire

failures would have to be accompanied by failure, or disregard, of the indications mentioned above. The probability of this occurrence is therefore too low to have any significance.

Concerning the human element, to erroneously withdraw a single rod cluster control assembly, the operator would have to improperly set the bank selector switch, the lift coil disconnect switches, and the in-hold-out switch. In addition, the three indications would have to be disregarded or ineffective. Such series of errors would require a complete lack of understanding and administrative control. A probability number cannot be assigned to a series of errors such as these.

The Rod Position Indication System provides direct visual displays of each control rod assembly position. The plant computer alarms for deviation of rods from their banks. In addition a rod insertion limit monitor provides an audible and visual alarm to warn the operator of an approach to an abnormal condition due to dilution. The low-low insertion limit alarm alerts the operator to stop any dilution in progress. The facility reactivity control systems are such that acceptable fuel damage limits will not be exceeded even in the event of a single malfunction of either system.

An important feature of the control rod system is that insertion is provided by gravity fall of the rods.

In all analyses involving reactor trip, the single, highest worth rod cluster control assembly is postulated to remain untripped in its full out position.

One means of detecting a stuck control rod assembly is available from the actual rod position information displayed on the control board. The control board position readouts, one for each rod, give the plant operator the actual position of the rod in steps. The indications are grouped by banks (e.g., Control Bank A, Control Bank B, etc.) to indicate to the operator the deviation of one rod with respect to other rods in a bank. This serves as a means to identify rod deviation.

The plant computer monitors the actual position of all rods. In the event a rod is misaligned more than 12 steps from the bank demand position, the rod to bank deviation alarm is actuated. Plant Technical Specifications limit the position difference between any two rods in a bank to a maximum of 24 steps; this limit is enveloped by the rod to bank deviation alarm setpoint.

Misaligned rod cluster control assemblies are also detected and alarmed in the control room via the flux tilt monitoring system which is independent of the plant computer.

Isolated signals derived from the Nuclear Instrumentation System are compared with one another to determine if a preset amount of deviation of average power level has occurred. Should such a deviation occur, the comparator output will operate a bistable unit to actuate a control board annunciator. This alarm will alert the operator to a power imbalance caused by a misaligned rod. By use of individual rod position readouts, the operator can determine the deviating control rod and take corrective action. The design of the plant control systems meets the requirements of General Design Criterion 23.

Refer to Section 4.3 for additional information on response considerations due to reactivity.

7.7.2.3 Step Load Changes Without Steam Dump

The Plant Control System restores equilibrium conditions, without a trip, following a plus or minus 10 percent step change in load demand over the 15 to 100 percent power range for automatic control. Steam dump is blocked for load decrease less than or equal to 10 percent. A load demand greater than full power is prohibited by the turbine control load limit devices.

The Plant Control System minimizes the reactor coolant average temperature deviation during the transient within a given value and restores average temperature to the programmed

setpoint. Excessive pressurizer pressure variations are prevented by using spray and heaters and power relief valves in the pressurizer.

The control system must limit nuclear power overshoot to acceptable values following a 10 percent increase in load to 100 percent.

7.7.2.4 Loading and Unloading

Ramp loading and unloading of 5 percent per minute can be accepted over the 15 to 100 percent power range under automatic control without tripping the plant. The function of the control system is to maintain the coolant average temperature as a function of turbine-generator load.

The coolant average temperature increases during loading and causes a continuous insurge to the pressurizer as a result of coolant expansion. The sprays limit the resulting pressure increase. Conversely, as the coolant average temperature is decreasing during unloading, there is a continuous outsurge from the pressurizer resulting from coolant contraction. The pressurizer heaters limit the resulting system pressure decrease. The pressurizer water level is programmed such that the water level is above the setpoint for heater cut out during the loading and unloading transients. The primary concern during loading is to limit the overshoot in nuclear power and to provide sufficient margin in the overtemperature ΔT setpoint.

The automatic load controls are designed to adjust the unit generation to match load requirements within the limits of the unit capability and licensed rating.

Load maneuvering is a managed evolution, with loading rates constrained by fuel thermal conditioning requirements. The fuel conditioning requirements vary with fuel type and manufacturer, varying from no limits to tightly controlled limits. The limits are evaulated during the core design evolution and promulgated to operating personnel through controlled documents and referenced in approved operating procedures.

Step increases in power are discouraged, and normal power increases are accomplished while maintaining the coolant average temperature close to the programmed reference temperature. A control room alarm provides the operator with a warning when the difference between the two temperatures exceeds established limits.

Excessive drops in coolant temperature are prevented by interlock C-16. This interlock circuit monitors the second lowest coolant temperature indications and the programmed reference temperature which is a function of turbine impulse pressure and causes a turbine loading stop when the temperature difference reaches the setpoint.

7.7.2.5 Load Rejection Furnished By Steam Dump System

When a load rejection occurs, if the difference between the required temperature setpoint of the Reactor Coolant System and the actual average temperature exceeds a predetermined amount, a signal will actuate the steam dump to maintain the Reactor Coolant System temperature within control range until a new equilibrium condition is reached.

The reactor power is reduced at a rate consistent with the capability of the rod control system. Reduction of the reactor power is automatic. The steam dump flow reduction is as fast as rod cluster control assemblies are capable of inserting negative reactivity.

The Rod Control System can then reduce the reactor temperature to a new equilibrium value without causing overtemperature and/or overpressure conditions. The steam dump steam flow capacity is approximately 70 percent of full-load steam flow at full-load steam pressure.

The steam dump flow reduces proportionally as the control rods act to reduce the average coolant temperature. The artificial load is therefore removed as the coolant average temperature is restored to its programmed equilibrium value.

The dump valves are modulated by the reactor coolant average temperature signal. The required number of steam dump valves can be tripped quickly to stroke full open or modulate, depending upon the magnitude of the temperature error signal resulting from loss of load.

7.7.2.6 Reactor Trip

The unit is operated with a programmed average temperature as a function of load, with the full load average temperature significantly greater than the equivalent saturation pressure of the safety valve setpoint. The thermal capacity of the Reactor Coolant System is greater than that of the secondary system, and because the full load average temperature is greater than the no load temperature, a heat sink is required to remove heat stored in the reactor coolant to prevent actuation of steam generator safety valves for a trip from full power. This heat sink is provided by the combination of controlled release of steam to the condenser and by makeup of cold feedwater to the steam generators.

The Steam Dump System is controlled by the reactor coolant average temperature signal whose setpoint values are programmed as a function of turbine load. Actuation of the steam dump is rapid to prevent actuation of the steam generator safety valves. With the dump valves open, the average coolant temperature starts to reduce quickly to the no-load setpoint. A direct feedback of temperature acts to proportionally close the valves to minimize the total amount of steam which is bypassed.

Following a reactor trip, the feedwater flow is cut off when the average coolant temperature decreases below a given temperature or when the steam generator water level reaches a given high level.

Additional feedwater makeup is then controlled manually to restore and maintain steam generator water level while assuring that the reactor coolant temperature is at the desired value. Residual heat removal is maintained by the steam header pressure controller (manually selected) which controls the amount of steam flow to the condensers. This controller operates a portion of the same steam dump valves to the condensers which are used during the initial transient following a reactor trip.

The pressurizer pressure and level fall rapidly during the transient because of coolant contraction.

If heaters become uncovered following the trip, the Chemical and Volume Control System provides full charging flow to restore water level in the pressurizer. Heaters are then turned on to restore pressurizer pressure to normal.

The steam dump and feedwater control systems are designed to prevent the average coolant temperature from falling below the programmed no-load temperature following the trip to ensure adequate reactivity shutdown margin.

7.7.3 References

1. Lipchak, J. B., "Nuclear Instrumentation System," WCAP-8255, January, 1974. (for background information only).
2. Shopsky, W. E., "Failure Mode and Effects Analysis (FMEA) of the Solid State Full Length Rod Control System," WCAP-8976, September 1977.

3. Safety Evaluation Report Regarding Compliance with ATWS Rule (10CFR50.62), September 22, 1986.
4. Adler, M.R., "AMSAC Generic Design Package," WCAP-10858P-A, Revision 1, July, 1987.
5. Nuclear Regulatory Commission, Letter to H.B. Tucker (Duke), November 6, 1987, re: ATWS Rule (10CFR 50.62) for McGuire and Catawba Nuclear Stations, Units 1 and 2 (TACs 59081/59111/59112/64535).
6. Nuclear Regulatory Commission, Letter to H.B. Tucker (Duke), August 3, 1989, re: Approval of Changes in ATWS/AMSAC Design, McGuire and Catawba Nuclear Stations, Units 1 and 2 (TACs 68427, 68428, 68429, and 68430).
7. Nuclear Regulatory Commission, Letter to All Holders of Operating Licenses or Construction Permits for Westinghouse (W)-Designed Nuclear Power Reactors That Utilize Bottom Mounted Instrumentation, from Charles E. Rossi, July 26, 1988, NRC Bulletin 88-09, "Thimble Tube Thinning in Westinghouse Reactors."
8. Duke Power Company, Letter from H.B. Tucker to NRC, March 16, 1989, re: Response to NRC Bulletin No. 88-09, "Thimble Tube Thinning in Westinghouse Reactors."
9. Duke Power Company, Letter from H.B. Tucker to NRC, April 18, 1989, re: Response to NRC Bulletin No. 88-09, "Thimble Tube Thinning in Westinghouse Reactors."
10. Duke Power Company, Letter from H.B. Tucker to NRC, October 1, 1990, re: Response to NRC Bulletin No. 88-09, "Thimble Tube Thinning in Westinghouse Reactors" - Incore Instrument Guide Thimble Wear Examination
11. Duke Power Company, Letter from M.S. Tuckman to NRC, December 6, 1990, re: Response to NRC Bulletin No. 88-09, "Thimble Tube Thinning in Westinghouse Reactors" - Incore Instrument Guide Thimble Wear Examination
12. Nuclear Regulatory Commission, Letter to M.S. Tuckman (DPC), May 16, 1991, re: Catawba Units 1 and 2 - Closeout of Bulletin 88-09, "Thimble Tube Thinning in Westinghouse Reactors" (TAC Nos. 72651 and 72652).
13. NRC Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment that is Not Safety-Related", April 16, 1985.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.7.

THIS PAGE LEFT BLANK INTENTIONALLY.

7.8 Operating Control Stations

Consistent with proven power station design philosophy, all controls, instrumentation displays, and alarms required for startup, operation, and shutdown of Units 1 and 2 are located in one centralized control room and are readily available to the operator. Remote control stations are provided for certain auxiliary systems which do not involve unit control or emergency functions.

7.8.1 General Layout

The control room design is such that one man can supervise operation of both units during normal steady state conditions; however, other qualified operators are always available to assist during normal and abnormal operating conditions.

7.8.2 Monitor Light Panels

Eight monitor light panels are provided in the control room to enable the operator to quickly assess the status of all remotely-operated engineered safety features valves, motors, fans, etc.

Each monitor light panel consist of an array of white lights, one for each engineered safety feature component monitored. The monitor lights are not energized when the monitored component is in the position or mode required for power operation. An energized light on a monitor light panel indicates that the monitored component is in its safety position or mode.

The eight monitor light panels are arranged to monitor particular groupings of components as follows:

Grouping One Panel	-	components that are normally in their safety positions and receive an ESFAS signal to insure correct positioning (containment isolation valves excepted).
Grouping Two Panel	-	components that are normally positioned for safety injection but are realigned for recirculation.
Grouping Three Panel	-	components that are aligned for safety injection by an ESFAS signal and are realigned for recirculation.
Grouping Four Panel	-	components that are aligned for safety injection by an ESFAS signal and are not realigned for recirculation (containment isolation valves excepted).
Grouping Five Panel	-	components that are normally aligned for safety injection and cold leg recirculation, but must be realigned for hot leg recirculation.
Grouping Six Panel	-	disabled due to deletion of upper head injection.
Grouping Seven Panel	-	redundant indication for components that are normally aligned for safety injection with power removed.
Grouping Eight Panel	-	containment isolation components that receive an ESFAS signal.

7.8.3 ESF Bypass Indication

An automatic function level bypass indication is provided in the control room for each safety-related function designed to perform automatically, if it is expected that the function will be bypassed or deliberately made inoperable more than once per year when it is normally required to be operable. This bypass indication is provided on the OAC 1.47 Bypass Panel Graphic Displays in the control room when either train has been made inoperable at the system level. Each time a bypass exists, an audible alarm is generated via the OAC alarm bell.

The function bypass alarms receive their inputs from valve position limit switches, circuit breaker auxiliary contacts, switch contacts, relays, etc. indicative of function inoperability. Means for manual actuation of each bypass alarm is also provided in the control room. The operator does not have the capability to disable any of the automatic function level bypass alarms.

A separate bypass alarm system is provided for each of the two Catawba units. The bypass alarm systems are interfaced with the unit specific plant computers for continuous control room indication. Alarm window terminology is explicit as to the safety function affected.

The design and installation of the bypass and inoperable status indication is such that a failure in an alarm circuit will have no adverse affects on the function monitored or on any of the other functions monitored by the bypass alarm system.

The indication of bypassed or inoperable status for safety-related functions conforms to the recommendations of Regulatory Guide 1.47, Revision 0. Functions for which bypass indication is provided are listed in Table 7-14.

7.8.4 Summary of Alarms

Visible and audible alarm units are incorporated into the control boards to inform the operator if limiting conditions are approached by any system. Audible Reactor Building evacuation alarms are initiated from the Radiation Monitoring System and from the source range nuclear instrumentation. Audible alarms are sounded in appropriate areas throughout the station if high radiation conditions are present in that area. Alarms for the nuclear systems are indicated in process diagrams in Chapter 6, Chapter 7, and Chapter 9.

7.8.5 Auxiliary Control Stations

Auxiliary control stations are provided where their use simplifies control of auxiliary systems equipment such as waste evaporator, sample valve selectors, chemical addition, etc. Sufficient indicators and alarms are provided so that the control room operator is made aware of abnormal conditions involving remote control stations.

7.8.6 Safety Features

Control room layouts provide the necessary controls to start, operate, and shut down the units with sufficient information display and alarm monitoring to assure safe and reliable operation under normal and accident conditions. Special emphasis is given to maintaining control during accident conditions. The layout of the Engineered Safety Feature devices of the control board is designed to minimize the time required for the operator to evaluate system performance under accident conditions.

7.8.7 Occupancy

Safe occupancy of the control room during abnormal conditions is provided for in the design of the Auxiliary Building. Adequate shielding is used to maintain tolerable radiation levels in the control rooms for maximum hypothetical accident conditions. Each control room ventilation system is provided with radiation detectors and appropriate alarms. Provisions are made for the control room air to be recirculated through absolute and carbon filters. Emergency lighting is provided.

7.8.8 Loose Parts Monitoring System

OVERVIEW:

The Loose Parts Monitoring System (LPMS) is an electronic system that monitors the Reactor Coolant System for metal-to-metal impacts in the primary coolant loop. Accelerometer sensors are mounted at various collection regions on the exterior surfaces of the upper reactor vessel, lower reactor vessel, reactor coolant pumps, and steam generators. The signal information from these sensors are amplified via charge-to-voltage converters and then routed out of containment to the LPMS cabinet mounted in the control room. The LPMS cabinet contains all the necessary electronics for processing the sensor signal data for alarming, data storage, data analysis, and remote annunciation to the main control board.

HARDWARE:

Field Equipment:

Twenty-two piezoelectric accelerometers are used to detect the presence of metallic impacts within the reactor coolant loops. Three sensors are located on the upper reactor head. Three lower reactor vessel sensors are mounted to the incore guide tubes approximately 120 degrees apart. One sensor is mounted on each reactor coolant pump. Three sensors are mounted on each steam Generator. All sensors are cabled to wall mounted enclosures where each signal passes through a charge converter/preamplifier before being routed out of containment to the LPMS cabinet. Each sensor is separately mounted and cabled via a high temperature, high radiation, low noise, hard-line cable to a splice box where the cable is coupled to a high radiation, low noise, soft-line cable. Each sensor's soft-line cable is then routed to one of six wall mounted enclosures where each signal passes separately amplified via a charge-to-voltage converter. The signal output from each charge-to-voltage converter is then routed via separate twisted, shielded pairs through a containment penetration to the LPMS cabinet.

Cabinet Equipment:

The LPMS cabinet is a seismically mounted cabinet which contains all the electronics for processing, storing, analyzing, and alarming any abnormal event as detected by the twenty-two primary loop sensors. The cabinet contains the following:

1. Signal processing to convert signal data to appropriate levels for use by cabinet components.
2. Detection and alarming of each signal input.
3. Post event data analysis.
4. Recording all twenty two channels when an alarm is detected.
5. Audio monitoring to select and listen to any channel or recorded channel.
6. Visual alarming and operator acknowledge capability.

OPERATION:

A metal-to-metal impact in the primary reactor coolant loop will be detected by the field mounted sensors, amplified, and then routed to the LPMS cabinet for processing. The system amplifies, filters, and converts the incoming signals into the appropriate analog or digital data for processing by the rest of the system. The system develops a relative alarm threshold which is compared to fixed and relative thresholds for burst detection. When an event is detected the system records the event data for all channels, and alerts the Control Room Operator of a possible loose part event. The Control Room Operator may then take the appropriate measures to further identify the severity of the event. This can be accomplished by immediately listening to the on-line audible signal from each sensor or by notifying the LPMS System Engineer who can analyze the data. Once a loose part is detected and is identified as an authentic loose part analysis is performed to estimate the mass and location of the part. Further analysis can be performed by knowledgeable individuals, including but not limited to industry experts or knowledgeable vendors. With the mass and location information, damage estimates can be evaluated to determine the correct course of action that will minimize damage while maximizing plant efficiency.

SYSTEM CHARACTERISTICS:

The LPMS is designed to a non-safety system. Since the entire reactor coolant system is designed to withstand all hypothetical seismic events including the OBE, the presence of any loose part due to seismic is highly unlikely. Therefore, it is not essential that the LPMS equipment itself be safety qualified. The LPMS is designed to meet the basic functional requirements as specified in Regulatory Guide 1.133 as discussed in Section 1.7. While not designed safety the system does employ many redundant and enhanced features, such as:

1. Multiple sensors per collection region
2. Sensor cabling is armored and routed in cable trays that are bought and mounted the same as safety equipment.
3. On-line sensor health monitoring is employed.
4. Per channel frequency filtering is employed.
5. Per channel event alarm discrimination techniques that minimizes false/nuisance alarms.
6. A 100 kHz per channel sampling rate.
7. On-line audio monitoring of each channel.
8. Event data analysis capability.
9. A Backup Alarm Panel.
10. A seismically mounted cabinet.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.8.