# CHAPTER 7.0 - INSTRUMENTATION AND CONTROLS

## TABLE OF CONTENTS


| | PAGE |
|---|---|
| 7.0 INSTRUMENTATION AND CONTROLS | 7.1-1 |
| 7.1 INTRODUCTION | 7.1-1 |
| 7.1.1 Identification of Safety-Related Systems | 7.1-4 |
| 7.1.1.1 General | 7.1-4 |
| 7.1.1.1.1 Reactor Trip System | 7.1-4 |
| 7.1.1.1.2 Engineered Safety Features Actuation System | 7.1-5 |
| 7.1.1.1.3 Instrumentation and Control Power Supply System | 7.1-5 |
| 7.1.1.2 Safety-Related Display Instrumentation | 7.1-5 |
| 7.1.1.3 Instrumentation and Control System Designers | 7.1-5 |
| 7.1.1.4 Plant Comparison | 7.1-5 |
| 7.1.2 Identification of Safety Criteria | 7.1-5 |
| 7.1.2.1 Design Bases | 7.1-6 |
| 7.1.2.1.1 Reactor Trip System | 7.1-6 |
| 7.1.2.1.2 Engineered Safety Features Actuation System | 7.1-7 |
| 7.1.2.1.3 Instrumentation and Control Power Supply System | 7.1-7 |
| 7.1.2.1.3.1 Loss of Power Alarm or Indication in the Control Room for Class 1E and Non-Class 1E Buses | 7.1-8 |
| 7.1.2.1.4 Emergency Power System | 7.1-9 |
| 7.1.2.1.5 Interlocks | 7.1-9 |
| 7.1.2.1.6 Bypasses | 7.1-9 |
| 7.1.2.1.7 Equipment Protection | 7.1-9 |
| 7.1.2.1.8 Diversity | 7.1-10 |
| 7.1.2.1.9 Bistable Trip Setpoints | 7.1-10 |
| 7.1.2.1.10 Engineered Safety Features Motor Specifications | 7.1-12 |
| 7.1.2.1.11 Other Safety-Related Systems | 7.1-12 |
| 7.1.2.2 Independence of Redundant Safety-Related Systems | 7.1-13 |
| 7.1.2.2.1 General | 7.1-13 |
| 7.1.2.2.2 Specific Systems | 7.1-15 |
| 7.1.2.2.3 Fire Protection | 7.1-16 |
| 7.1.2.3 Physical Identification of Safety-Related Equipment | 7.1-16 |
| 7.1.2.4 Conformance to Criteria | 7.1-17 |
| 7.1.2.5 Instrument Lines Penetrating Primary Reactor Containment | 7.1-17 |

TABLE OF CONTENTS (Cont'd)


| | | PAGE |
|---|---|---|
| 7.1.2.6 | Periodic Testing of Protection System Actuation Functions (Regulatory Guide 1.22) | 7.1-17a |
| 7.1.2.7 | Seismic Design Classification | 7.1-23 |
| 7.1.2.8 | Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment | 7.1-23 |
| 7.1.2.9 | Qualification Tests of Continuous Duty Motors Installed Inside the Containment of Water-Cooled Nuclear Power Plants | 7.1-23 |
| 7.1.2.10 | Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems (Regulatory Guide 1.47) | 7.1-24 |
| 7.1.2.11 | Application of the Single Failure Criterion to Nuclear Power Plant Protection System (Regulatory Guide 1.53) | 7.1-26 |
| 7.1.2.12 | Manual Initiation of Protective Actions | 7.1-27 |
| 7.1.2.12.1 | Manual Initiation of Protective Actions Required by Regulatory Guide 1.62 | 7.1-27 |
| 7.1.2.13 | Electric Penetration Assemblies in Containment Structures for Light-Water-Cooled Nuclear Power Plants | 7.1-28 |
| 7.1.2.14 | Initial Test Programs for Water-Cooled Reactor Power Plants | 7.1-28 |
| 7.1.2.15 | Qualification Tests of Electric Valve Operators Installed Inside the Containment of Nuclear Power Plants | 7.1-28 |
| 7.1.2.16 | Physical Independence of Electric Systems | 7.1-28 |
| 7.1.2.17 | Preoperational Testing of Instrument Air Systems | 7.1-28 |
| 7.1.2.18 | Qualification Program | 7.1-29 |
| 7.1.2.19 | Conformance to IEEE Standard 338-1987 | 7.1-29 |
| 7.1.3 | References | 7.1-30 |
| 7.2 | REACTOR TRIP SYSTEM | 7.2-1 |
| 7.2.1 | Description | 7.2-1 |
| 7.2.1.1 | System Description | 7.2-1 |
| 7.2.1.1.1 | Functional Performance Requirements | 7.2-2 |
| 7.2.1.1.2 | Reactor Trips | 7.2-2 |
| 7.2.1.1.3 | Reactor Trip System Interlocks | 7.2-11 |
| 7.2.1.1.4 | Coolant Temperature Sensor Arrangement | 7.2-12 |
| 7.2.1.1.5 | Pressurizer Water Level Reference Leg Arrangement | 7.2-13 |
| 7.2.1.1.6 | Analog System | 7.2-13 |
| 7.2.1.1.7 | Solid-State Logic Protection System | 7.2-15 |
| 7.2.1.1.8 | Isolation Amplifiers | 7.2-15 |
| 7.2.1.1.9 | Energy Supply and Environmental Variations | 7.2-15 |

TABLE OF CONTENTS (Cont'd)


| | PAGE |
|---|---|
| 7.2.1.1.10 Setpoints | 7.2-16 |
| 7.2.1.1.11 Seismic Design | 7.2-16 |
| 7.2.1.2 Design Basis Information | 7.2-16 |
| 7.2.1.2.1 Unit Conditions | 7.2-16 |
| 7.2.1.2.2 Unit Variables | 7.2-16 |
| 7.2.1.2.3 Spatially Dependent Variables | 7.2-17 |
| 7.2.1.2.4 Limits, Margins, and Setpoints | 7.2-17 |
| 7.2.1.2.5 Abnormal Events | 7.2-17 |
| 7.2.1.2.6 Minimum Performance Requirements | 7.2-18 |
| 7.2.1.3 System Drawings | 7.2-18 |
| 7.2.2 Analysis | 7.2-18 |
| 7.2.2.1 Failure Mode and Effects Analyses | 7.2-18 |
| 7.2.2.2 Evaluation of Design Limits | 7.2-19 |
| 7.2.2.2.1 Trip Setpoint Discussion | 7.2-19 |
| 7.2.2.2.2 Reactor Coolant Flow Measurement | 7.2-21 |
| 7.2.2.2.3 Evaluation of Compliance to Applicable Codes and Standards | 7.2-21 |
| 7.2.2.3 Specific Control and Protection Interactions | 7.2-34 |
| 7.2.2.3.1 Neutron Flux | 7.2-34 |
| 7.2.2.3.2 Coolant Temperature | 7.2-34 |
| 7.2.2.3.3 Pressurizer Pressure | 7.2-35 |
| 7.2.2.3.4 Pressurizer Water Level | 7.2-36 |
| 7.2.2.3.5 Steam Generator Water Level | 7.2-36 |
| 7.2.2.3.6 Main Steamline Pressure Instrumentation | 7.2-38 |
| 7.2.2.3.7 Effect of an Adverse Environment on Four Reactor Protection Control Systems | 7.2-38 |
| 7.2.2.4 Additional Postulated Accidents | 7.2-42 |
| 7.2.2.4.1 Loss of Any Single Instrument | 7.2-43 |
| 7.2.2.4.2 Loss of Power to an Inverter, Control Group, or Protection Set | 7.2-43 |
| 7.2.2.4.3 Loss of Common Instrument Lines | 7.2-44 |
| 7.2.3 Tests and Inspections | 7.2-45 |
| 7.2.4 References | 7.2-46 |
| 7.3 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM | 7.3-1 |
| 7.3.1 Description | 7.3-1 |
| 7.3.1.1 System Description | 7.3-1 |
| 7.3.1.1.1 Function Initiation | 7.3-2 |
| 7.3.1.1.2 Analog Circuitry | 7.3-4 |
| 7.3.1.1.3 Digital Circuitry | 7.3-4 |
| 7.3.1.1.4 Final Actuation Circuitry | 7.3-5 |
| 7.3.1.1.5 Support Systems | 7.3-6 |
| 7.3.1.1.6 Auxiliary Feedwater System Operation | 7.3-6 |
| 7.3.1.1.7 Essential Service Water System Operation | 7.3-10 |
| 7.3.1.1.8 Auxiliary Building HVAC System Instrumentation and Controls | 7.3-13 |

TABLE OF CONTENTS (Cont'd)


| | | PAGE |
|---|---|---|
| 7.3.1.1.8.1 | System Identification | 7.3-13 |
| 7.3.1.1.8.2 | Identification of Safety Criteria | 7.3-14 |
| 7.3.1.1.8.2.1 | Safety Design Bases | 7.3-14 |
| 7.3.1.1.8.2.2 | Power Generation Design Basis | 7.3-14 |
| 7.3.1.1.8.2.3 | Indication and Annunciation | 7.3-14 |
| 7.3.1.1.8.2.3.1 | Indication | 7.3-14 |
| 7.3.1.1.8.2.3.2 | Alarms | 7.3-15 |
| 7.3.1.1.8.3 | System Description | 7.3-15 |
| 7.3.1.1.8.3.1 | Power Supply | 7.3-15 |
| 7.3.1.1.8.3.2 | Initiating Circuits, Logic, and Sequencing | 7.3-16 |
| 7.3.1.1.8.3.3 | Bypasses and Interlocks | 7.3-16 |
| 7.3.1.1.8.3.4 | Redundancy/Diversity | 7.3-17 |
| 7.3.1.1.8.3.5 | Separation | 7.3-17 |
| 7.3.1.1.8.3.6 | Testability | 7.3-17 |
| 7.3.1.1.8.3.7 | System Drawings | 7.3-17 |
| 7.3.1.1.8.3.8 | Environmental Considerations | 7.3-17 |
| 7.3.1.1.8.3.9 | Operational Considerations | 7.3-17 |
| 7.3.1.1.8.4 | Design-Bases Information | 7.3-17 |
| 7.3.1.1.9 | Main Control Room Heating, Ventilation, and Air Conditioning Instrumentation Controls | 7.3-18 |
| 7.3.1.1.9.1 | System Identification | 7.3-18 |
| 7.3.1.1.9.2 | Identification of Safety Criteria | 7.3-18 |
| 7.3.1.1.9.2.1 | Safety Design-Bases | 7.3-18 |
| 7.3.1.1.9.2.2 | Power Generation Design-Bases | 7.3-19 |
| 7.3.1.1.9.2.3 | Indication and Annunciation | 7.3-19 |
| 7.3.1.1.9.2.3.1 | Indication | 7.3-19 |
| 7.3.1.1.9.2.3.2 | Annunciation | 7.3-19 |
| 7.3.1.1.9.3 | System Description - Main Control Room HVAC Control System | 7.3-19 |
| 7.3.1.1.9.3.1 | Power Supply | 7.3-20 |
| 7.3.1.1.9.3.2 | Initiating Circuits, Logic, and Sequencing | 7.3-20 |
| 7.3.1.1.9.3.3 | Bypass and Interlocks | 7.3-21 |
| 7.3.1.1.9.3.4 | Redundancy/Diversity | 7.3-21 |
| 7.3.1.1.9.3.5 | Separation | 7.3-22 |
| 7.3.1.1.9.3.6 | Testability | 7.3-22 |
| 7.3.1.1.9.3.7 | System Drawings | 7.3-22 |
| 7.3.1.1.9.3.8 | Environmental Considerations | 7.3-22 |
| 7.3.1.1.9.3.9 | Operational Considerations | 7.3-22 |
| 7.3.1.1.9.4 | Design-Bases Information | 7.3-22 |
| 7.3.1.1.9.4.1 | Outdoor Air Intake Radiation Protection Portion of Control Room HVAC System | 7.3-22 |
| 7.3.1.1.9.4.2 | Outdoor Air Intake Chlorine Protection Portion of Control Room HVAC System (Braidwood only) | 7.3-23 |

TABLE OF CONTENTS (Cont'd)


| | PAGE |
|---|---|
| 7.3.1.1.9.4.3 Ionization Detection Portion of Control Room HVAC System | 7.3-23 |
| 7.3.1.1.9.4.4 Ionization Detection Portion of Control Room HVAC System | 7.3-23a |
| 7.3.1.1.10 Diesel-Generator Room Ventilation System Instrumentation and Controls | 7.3-24 |
| 7.3.1.1.10.1 System Identification | 7.3-24 |
| 7.3.1.1.10.2 Identification of Safety Criteria | 7.3-24 |
| 7.3.1.1.10.2.1 Safety Design-Bases | 7.3-24 |
| 7.3.1.1.10.2.2 Power Generation Bases | 7.3-24 |
| 7.3.1.1.10.2.3 Indication and Annunciation | 7.3-25 |
| 7.3.1.1.10.2.3.1 Indication | 7.3-25 |
| 7.3.1.1.10.2.3.2 Annunciation | 7.3-25 |
| 7.3.1.1.10.3 System Description | 7.3-26 |
| 7.3.1.1.10.3.1 Power Supply | 7.3-26 |
| 7.3.1.1.10.3.2 Initiating Circuits, Logic, and Sequencing | 7.3-26 |
| 7.3.1.1.10.3.3 Bypasses and Interlocks | 7.3-26 |
| 7.3.1.1.10.3.4 Redundancy/Diversity | 7.3-27 |
| 7.3.1.1.10.3.5 Separation | 7.3-27 |
| 7.3.1.1.10.3.6 Testability | 7.3-27 |
| 7.3.1.1.10.3.7 System Drawings | 7.3-27 |
| 7.3.1.1.10.3.8 Environmental Considerations | 7.3-27 |
| 7.3.1.1.10.3.9 Operational Considerations | 7.3-27 |
| 7.3.1.1.10.3.10 Supporting Systems | 7.3-27 |
| 7.3.1.1.10.4 Design Bases Information | 7.3-28 |
| 7.3.1.1.11 Essential Switchgear Rooms, Miscellaneous Electrical Equipment Rooms and Battery Rooms Ventilation Systems Instrumentation and Controls | 7.3-28 |
| 7.3.1.1.11.1 System Identification | 7.3-28 |
| 7.3.1.1.11.2 Identification of Safety Criteria | 7.3-29 |
| 7.3.1.1.11.2.1 Safety Design-Bases | 7.3-29 |
| 7.3.1.1.11.2.2 Power Generation Bases | 7.3-29 |
| 7.3.1.1.11.2.3 Indication and Annunciation | 7.3-30 |
| 7.3.1.1.11.2.3.1 Indication | 7.3-30 |
| 7.3.1.1.11.2.3.2 Annunciation | 7.3-30 |
| 7.3.1.1.11.3 System Description | 7.3-31 |
| 7.3.1.1.11.3.1 Power Supply | 7.3-31 |
| 7.3.1.1.11.3.2 Initiating Circuits, Logic and Sequencing | 7.3-31 |
| 7.3.1.1.11.3.3 Bypasses and Interlocks | 7.3-31 |
| 7.3.1.1.11.3.4 Redundancy/Diversity | 7.3-31 |
| 7.3.1.1.11.3.5 Separation | 7.3-31 |
| 7.3.1.1.11.3.6 Testability | 7.3-31 |
| 7.3.1.1.11.3.7 System Drawings | 7.3-32 |
| 7.3.1.1.11.3.8 Environmental Considerations | 7.3-32 |
| 7.3.1.1.11.3.9 Operational Considerations | 7.3-32 |
| 7.3.1.1.11.4 Design Bases Information | 7.3-32 |
| 7.3.1.1.12 Reactor Containment Fan Coolers Instrumentation and Controls | 7.3-32 |

TABLE OF CONTENTS (Cont'd)


| | PAGE |
|---|---|
| 7.3.1.1.12.1 System Identification | 7.3-32 |
| 7.3.1.1.12.2 Identification of Safety Criteria | 7.3-32 |
| 7.3.1.1.12.2.1 Safety Design-Bases | 7.3-32 |
| 7.3.1.1.12.2.2 Power Generation Bases | 7.3-33 |
| 7.3.1.1.12.2.3 Indication and Alarms | 7.3-33 |
| 7.3.1.1.12.2.3.1 Indication | 7.3-33 |
| 7.3.1.1.12.2.3.2 Alarms | 7.3-33 |
| 7.3.1.1.12.3 System Description | 7.3-34 |
| 7.3.1.1.12.3.1 Power Supply | 7.3-34 |
| 7.3.1.1.12.3.2 Initiating Circuits, Logic, and Sequencing | 7.3-34 |
| 7.3.1.1.12.3.3 Bypasses and Interlocks | 7.3-34 |
| 7.3.1.1.12.3.4 Redundancy/Diversity | 7.3-34 |
| 7.3.1.1.12.3.5 Separation | 7.3-34 |
| 7.3.1.1.12.3.6 Testability | 7.3-34 |
| 7.3.1.1.12.3.7 System Drawings | 7.3-34 |
| 7.3.1.1.12.3.8 Environmental Considerations | 7.3-35 |
| 7.3.1.1.12.3.9 Operational Considerations | 7.3-35 |
| 7.3.1.1.12.4 Design Basis | 7.3-35 |
| 7.3.1.1.13 Containment Spray System Operation | 7.3-35 |
| 7.3.1.1.14 Diesel Fuel Oil System | 7.3-38 |
| 7.3.1.1.15 Emergency Core Cooling System (ECCS) | 7.3-39 |
| 7.3.1.1.15.1 Initiating Circuits and Logic | 7.3-39 |
| 7.3.1.1.15.2 Bypasses, Interlocks, and Sequencing | 7.3-39 |
| 7.3.1.1.15.3 Redundancy and Diversity | 7.3-39 |
| 7.3.1.1.16 Combustible Gas Control in Containment | 7.3-40 |
| 7.3.1.1.17 Containment Isolation | 7.3-40 |
| 7.3.1.2 Design Bases Information | 7.3-40 |
| 7.3.1.2.1 Generating Station Conditions | 7.3-41 |
| 7.3.1.2.2 Generating Station Variables | 7.3-41 |
| 7.3.1.2.3 Limits, Margins, and Setpoints | 7.3-41 |
| 7.3.1.2.4 Abnormal Events | 7.3-42 |
| 7.3.1.2.5 Minimum Performance Requirements | 7.3-42 |
| 7.3.1.3 System Drawings | 7.3-43 |
| 7.3.2 Analysis of ESF Actuation System | 7.3-43 |
| 7.3.2.1 Failure Mode and Effects Analyses | 7.3-43 |
| 7.3.2.2 Compliance With Standards and Design Criteria | 7.3-44 |
| 7.3.2.2.1 Single Failure Criteria | 7.3-44 |
| 7.3.2.2.2 Equipment Qualification | 7.3-45 |
| 7.3.2.2.3 Channel Independence | 7.3-45 |
| 7.3.2.2.4 Control and Protection System Interaction | 7.3-45 |
| 7.3.2.2.5 Capability for Sensor Checks and Equipment Test and Calibration | 7.3-45 |
| 7.3.2.2.6 Manual Resets and Blocking Features | 7.3-50 |
| 7.3.2.2.7 Manual Initiation of Protective Actions (Regulatory Guide 1.62) | 7.3-50 |
| 7.3.2.2.8 Analysis of Auxiliary Building HVAC System | 7.3-51 |

TABLE OF CONTENTS (Cont'd)


| | | PAGE |
|---|---|---|
| 7.3.2.2.8.1 | General | 7.3-51 |
| 7.3.2.2.8.2 | Specific Conformance of the Instrumentation and Controls to IEEE 279-1971 | 7.3-51 |
| 7.3.2.2.8.3 | Specific Conformance of the Instrumentation and Controls to General Design Criteria, 10 CFR 50 Appendix A | 7.3-52 |
| 7.3.2.2.9 | Analysis of Main Control Room HVAC System | 7.3-52 |
| 7.3.2.2.9.1 | General | 7.3-53 |
| 7.3.2.2.9.2 | Specific Conformance of the Instrumentation and Controls to IEEE 279-1971 | 7.3-53 |
| 7.3.2.2.9.3 | Specific Conformance of Instrumentation and Controls to General Design Criteria 10 CFR 50 Appendix A | 7.3-54 |
| 7.3.2.2.10 | Analysis of Diesel-Generator Room Ventilation System | 7.3-54 |
| 7.3.2.2.10.1 | General | 7.3-54 |
| 7.3.2.2.10.2 | Specific Conformance of the Instrumentation and Controls to IEEE 279-1971 | 7.3-55 |
| 7.3.2.2.10.3 | Specific Conformance of the Instrumentation and Controls to General Design Criteria of 10 CFR 50 Appendix A | 7.3-55 |
| 7.3.2.2.11 | Analysis of Ventilation Systems for Redundant ESF Switchgear Rooms, Cable Spreading Rooms, Miscellaneous Electrical Equipment Rooms, Battery Rooms, and Cooling Tower Electrical Substation Rooms | 7.3-56 |
| 7.3.2.2.11.1 | General | 7.3-56 |
| 7.3.2.2.11.2 | Specific Conformance of the Instrumentation and Controls to IEEE 279-1971 | 7.3-56 |
| 7.3.2.2.11.3 | Specific Conformance of the Instrumentation and Controls to General Design Criteria, 10 CFR 50 Appendix A | 7.3-57 |
| 7.3.2.2.12 | Analysis of Reactor Containment Fan Cooler (RCFC) Units | 7.3-58 |
| 7.3.2.2.12.1 | General | 7.3-58 |
| 7.3.2.2.12.2 | Specific Conformance of the Instrumentation and Controls to IEEE 279-1971 | 7.3-58 |
| 7.3.2.2.12.3 | Specific Conformance of the Instrumentation and Controls to General Design Criteria, 10 CFR 50 Appendix A | 7.3-59 |

TABLE OF CONTENTS (Cont'd)


| | PAGE |
|---|---|
| 7.3.2.3 Further Considerations | 7.3-60 |
| 7.3.2.4 Summary | 7.3-64 |
| 7.3.2.4.1 Loss-of-Coolant Protection | 7.3-64 |
| 7.3.2.4.2 Steamline Break Protection | 7.3-65 |
| 7.3.3 References | 7.3-66 |
| 7.4 SYSTEMS REQUIRED FOR SAFE SHUTDOWN | 7.4-1 |
| 7.4.1 Description | 7.4-1 |
| 7.4.1.1 Monitoring Indicators | 7.4-2 |
| 7.4.1.2 Controls | 7.4-3 |
| 7.4.1.2.1 General Considerations | 7.4-3 |
| 7.4.1.2.2 Pumps and Fans | 7.4-3 |
| 7.4.1.2.3 Diesel Generators | 7.4-3 |
| 7.4.1.2.4 Valves and Heaters | 7.4-4 |
| 7.4.1.3 Control Room Evacuation | 7.4-4 |
| 7.4.1.4 Equipment and Systems Available for Cold Shutdown | 7.4-5 |
| 7.4.2 Analysis | 7.4-8 |
| 7.5 SAFETY-RELATED DISPLAY INSTRUMENTATION (Regulatory Guide 1.97) | 7.5-1 |
| 7.5.1 Description | 7.5-1 |
| 7.5.2 Analyses | 7.5-3 |
| 7.5.3 Design Criteria | 7.5-4 |
| 7.5.3.1 Scope | 7.5-4 |
| 7.5.3.2 Definitions | 7.5-4 |
| 7.5.3.3 Requirements | 7.5-5 |
| 7.5.3.3.1 General Functional Requirements | 7.5-5 |
| 7.5.3.3.2 Information Readout | 7.5-5 |
| 7.5.3.3.3 Single-Failure Criterion | 7.5-5 |
| 7.5.3.3.4 Quality of Components and Modules | 7.5-5 |
| 7.5.3.3.5 Equipment Qualification | 7.5-6 |
| 7.5.3.3.6 Channel Integrity | 7.5-6 |
| 7.5.3.3.7 Channel Independence | 7.5-6 |
| 7.5.3.3.8 Power Source | 7.5-6 |
| 7.5.3.3.9 Postaccident Monitoring System and Control System Interaction | 7.5-6 |
| 7.5.3.3.10 Deviation of System Inputs | 7.5-7 |
| 7.5.3.3.11 Capability for Sensor Checks | 7.5-7 |
| 7.5.3.3.12 Capability for Verifying Operability | 7.5-7 |
| 7.5.3.3.13 Channel Bypass or Removal from Operation (RG 1.47) | 7.5-7 |
| 7.5.3.3.14 Access to Means of Bypassing | 7.5-7 |
| 7.5.3.3.15 Access to Setpoint Adjustments, Calibration, and Test Points | 7.5-7 |
| 7.5.3.3.16 Identification of Monitoring Functions | 7.5-8 |

TABLE OF CONTENTS (Cont'd)


| | PAGE |
|---|---|
| 7.5.3.3.17 System Repair | 7.5-8 |
| 7.5.3.3.18 Identification | 7.5-8 |
| 7.6 OTHER SAFETY-RELATED INSTRUMENTATION SYSTEMS | 7.6-1 |
| 7.6.1 Description | 7.6-1 |
| 7.6.2 Analysis | 7.6-1 |
| 7.6.3 Instrumentation and Control Power Supply System | 7.6-1 |
| 7.6.4 Residual Heat Removal Isolation Valves | 7.6-1 |
| 7.6.4.1 Description | 7.6-1 |
| 7.6.4.2 Analysis | 7.6-1 |
| 7.6.5 Refueling Interlocks | 7.6-2 |
| 7.6.6 Accumulator Motor-Operated Valves | 7.6-2 |
| 7.6.7 Switchover from Injection to Recirculation | 7.6-3 |
| 7.6.8 Reactor Coolant System Loop Isolation Valve Interlocks | 7.6-3 |
| 7.6.8.1 Description | 7.6-3 |
| 7.6.9 Interlocks for RCS Pressure Control During Low Temperature Operation | 7.6-3 |
| 7.6.9.1 Analysis of Interlock | 7.6-5 |
| 7.6.10 Instrumentation for Mitigating Consequences of Inadvertent Boron Dilution | 7.6-6 |
| 7.6.10.1 Description | 7.6-6 |
| 7.6.10.2 Analysis | 7.6-6 |
| 7.6.10.3 Qualification | 7.6-7 |
| 7.6.11 Charging Pump Miniflow Valve Interlocks | 7.6-7 |
| 7.6.12 References | 7.6-7 |
| 7.7 CONTROL SYSTEMS NOT REQUIRED FOR SAFETY | 7.7-1 |
| 7.7.1 Description of Control Systems Not Required for Safety | 7.7-1 |
| 7.7.1.1 Reactor Control System | 7.7-3 |
| 7.7.1.2 Full Length Rod Control System | 7.7-4 |
| 7.7.1.2.1 Description | 7.7-4 |
| 7.7.1.2.2 Features | 7.7-6 |
| 7.7.1.3 Plant Control Signals for Monitoring and Indicating | 7.7-9 |
| 7.7.1.3.1 Monitoring Functions Provided by the Nuclear Instrumentation System | 7.7-9 |
| 7.7.1.3.2 Rod Position Monitoring | 7.7-11 |
| 7.7.1.3.3 Control Bank Rod Insertion Monitoring | 7.7-12 |
| 7.7.1.3.4 Rod Deviation Alarm | 7.7-14 |
| 7.7.1.3.5 Rod Bottom Alarm | 7.7-14 |
| 7.7.1.4 Plant Control System Interlocks | 7.7-14 |
| 7.7.1.4.1 Rod Stops | 7.7-14 |
| 7.7.1.4.2 Automatic Turbine Load Runback | 7.7-15 |

TABLE OF CONTENTS (Cont'd)


| | | PAGE |
|---|---|---|
| 7.7.1.5 | Pressurizer Pressure Control | 7.7-15 |
| 7.7.1.6 | Pressurizer Water Level Control | 7.7-16 |
| 7.7.1.7 | Steam Generator Water Level Control | 7.7-16 |
| 7.7.1.8 | Steam Dump Control | 7.7-17 |
| 7.7.1.8.1 | Load Rejection Steam Dump Controller | 7.7-17 |
| 7.7.1.8.2 | Plant Trip Steam Dump Controller | 7.7-18 |
| 7.7.1.8.3 | Steam Header Pressure Controller | 7.7-18 |
| 7.7.1.9 | Incore Instrumentation | 7.7-18 |
| 7.7.1.9.1 | Thermocouples | 7.7-18 |
| 7.7.1.9.2 | Movable Neutron Flux Detector Drive System | 7.7-19 |
| 7.7.1.9.3 | Control and Readout Description | 7.7-20 |
| 7.7.1.10 | Boron Concentration Measurement System Braidwood only | 7.7-20 |
| 7.7.1.11 | Main Steam Isolation Control | 7.7-21 |
| 7.7.1.12 | Turbine-Generator Controls | 7.7-21 |
| 7.7.1.13 | Main Condenser Water Level Control | 7.7-22 |
| 7.7.1.14 | Main Condenser Vacuum Control | 7.7-23 |
| 7.7.1.15 | Circulating Water System Controls | 7.7-23 |
| 7.7.1.16 | Condensate/Condensate Booster and Feedwater System Controls | 7.7-24 |
| 7.7.1.17 | Process Radiation Monitoring Instruments and Controls | 7.7-24 |
| 7.7.1.18 | Area Radiation Monitoring Instruments and Controls | 7.7-25 |
| 7.7.1.19 | Liquid Radwaste System Instruments and Controls | 7.7-25 |
| 7.7.1.20 | Leak Detection Instrumentation and Control | 7.7-26 |
| 7.7.1.21 | Anticipated Transients Without Scram Mitigation System (AMS) | 7.7-27 |
| 7.7.1.21.1 | System Overview | 7.7-27 |
| 7.7.1.21.2 | Logic Power Supplies | 7.7-27b |
| 7.7.1.22 | Power Distribution Monitoring System (PDMS) | 7.7-27b |
| 7.7.1.22.1 | Determination of Core Power Distribution | 7.7-27b |
| 7.7.1.22.2 | Calibration of Core Power Distribution | 7.7-27b |
| 7.7.1.22.3 | BEACON Core Monitoring Methodology | 7.7-27c |
| 7.7.1.22.4 | System Configuration | 7.7-27c |
| 7.7.2 | Analysis of Control Systems Not Required for Safety | 7.7-27d |
| 7.7.2.1 | Separation of Protection and Control System | 7.7-28 |
| 7.7.2.2 | Response Considerations of Reactivity | 7.7-28 |
| 7.7.2.3 | Step Load Changes Without Steam Dump | 7.7-31 |
| 7.7.2.4 | Loading and Unloading | 7.7-31 |
| 7.7.2.5 | Load Rejection Furnished by Steam Dump System | 7.7-32 |
| 7.7.2.6 | Turbine-Generator Trip With Reactor Trip | 7.7-33 |
| 7.7.3 | References | 7.7-34 |

# CHAPTER 7.0 - INSTRUMENTATION AND CONTROLS

## LIST OF TABLES


| NUMBER | TITLE | PAGE |
|---|---|---|
| 7.1-1 | Listing of Applicable Criteria | 7.1-31 |
| 7.1-2 | Identification of Safety-Related Features | 7.1-39 |
| 7.2-1 | List of Reactor Trips | 7.2-47 |
| 7.2-2 | Protection System Interlocks | 7.2-50 |
| 7.2-3 | Reactor Trip System Instrumentation | 7.2-52 |
| 7.2-4 | Reactor Trip Correlation | 7.2-54 |
| 7.2-5 | Loss of Any Single Instrument | 7.2-59 |
| 7.2-6 | Loss of Power to Inverter I | 7.2-73 |
| 7.2-7 | Loss of Power to Inverter II | 7.2-75 |
| 7.2-8 | Loss of Power to Inverter III | 7.2-77 |
| 7.2-9 | Loss of Power to Inverter IV | 7.2-78 |
| 7.2-10 | Loss of Power to Protection Set I | 7.2-79 |
| 7.2-11 | Loss of Power to Protection Set II | 7.2-81 |
| 7.2-12 | Loss of Power to Protection Set III | 7.2-83 |
| 7.2-13 | Loss of Power to Protection Set IV | 7.2-85 |
| 7.2-14 | Loss of Power to Control Group 1 | 7.2-86 |
| 7.2-15 | Loss of Power to Control Group 2 | 7.2-87 |
| 7.2-16 | Loss of Power to Control Group 3 | 7.2-88 |
| 7.2-17 | Loss of Power to Control Group 4 | 7.2-89 |
| 7.2-18 | Loss of Common Instrument Lines | 7.2-90 |
| 7.2-19 | Reactor Trip System Instrumentation Maximum Allowable Response Times | 7.2-92 |
| 7.3-1 | Instrumentation Operating Conditions for Engineered Safety Features | 7.3-67 |
| 7.3-2 | Instrument Operating Conditions for Isolation Functions | 7.3-68 |
| 7.3-3 | Interlocks for Engineered Safety Features Actuation System | 7.3-70 |
| 7.3-4 | Conformance to IEEE 279-1971 | 7.3-72 |
| 7.3-5 | Conformance to General Criteria 10 CFR 50 Appendix A | 7.3-75 |
| 7.3-6 | Engineered Safety Features (ESF) Maximum Allowable Response Times | 7.3-77 |
| 7.4-1 | Remote Shutdown Monitoring Instrumentation | 7.4-11 |
| 7.5-1 | Main Control Board Indicators and/or Recorders Available to the Operator (Condition II, III, and IV Events) | 7.5-9 |
| 7.5-2 | Control Room Indicator and/or Recorders Available to the Operator to Monitor Significant Plant Parameters During Normal Operation | 7.5-13 |
| 7.7-1 | Plant Control System Interlocks | 7.7-35 |

# CHAPTER 7.0 - INSTRUMENTATION AND CONTROLS

## LIST OF FIGURES


| NUMBER | TITLE |
|---|---|
| 7.1-1 | Single Line Diagram of Reactor Trip System |
| 7.1-2 | Reactor Trip System Input Relay Bay |
| 7.1-3 | Deleted |
| 7.1-4 | Deleted |
| 7.1-4 | Block Diagram Turbine Protection System Overview |
| 7.1-5 | Reactor Trip/ESF Actuation Mechanical Linkage |
| 7.2-1 | Deleted |
| 7.2-2 | Reactor Trip/ESF Actuation Mechanical Linkage |
| 7.3-1 | Typical ESF Test Circuits |
| 7.3-2 | Engineered Safeguards Test Cabinet - Index, Notes, and Legend |
| 7.3-3 | Deleted |
| 7.3-4 | Deleted |
| 7.3-5 | Deleted |
| 7.6-1 | Logic Diagram For Outer RHR Isolation Valve |
| 7.6-2 | Logic Diagram For Inner RHR Isolation Valve |
| 7.6-3 | Functional Block Diagram of Accumulator Isolation Valve |
| 7.6-4 | Transfer Signal For SI System Recirculation Sump Isolation Valves and Charging Pump Miniflow Motor Operated Valve |
| 7.6-5 | Safety Injection System Recirculation Sump Isolation Valves |
| 7.6-6 | Functional Diagram For Motor Operated Charging Pump Miniflow Control Valves |
| 7.6-7 | Functional Diagram For Wide Range Pressure Signal For Solenoid Actuated Charging Pump Miniflow Control Valves |
| 7.6-8 | Functional Diagram For Solenoid Actuated Charging Pump Miniflow Control Valves |
| 7.6-9 | Reactor Coolant System Loop With Loop Stop Valves |
| 7.6-10 | Diagram Showing Generating Plant Variable Processing for Low Temperature Interlocks for RCS Pressure |
| 7.6-11 | Deleted |
| 7.7-1 | Simplified Block Diagram of Reactor Control System |
| 7.7-2 | Control Bank Rod Insertion Monitor |
| 7.7-3 | Rod Deviation Comparator |
| 7.7-4 | Block Diagram of Pressurizer Pressure Control System |
| 7.7-5 | Block Diagram of Pressurizer Level Control System |
| 7.7-6 | Block Diagram of Steam Generator Water Level Control System |

LIST OF FIGURES (Cont'd)


| NUMBER | TITLE |
|---|---|
| 7.7-7 | Block Diagram of Main Feedwater Pump Speed Control System |
| 7.7-8 | Block Diagram of Steam Dump Control System |
| 7.7-9 | Basic Flux - Mapping System |
| 7.7-10 | Simplified Block Diagram Rod Control System |
| 7.7-11 | Control Bank D Partial Simplified Schematic Diagram Power Cabinets 1BD and 2BD |
| 7.7-12 | ATWS Mitigation System Simplified Logic Diagram |

## CHAPTER 7.0 – INSTRUMENATION AND CONTROLS

## DRAWINGS CITED IN THIS CHAPTER*

*The listed drawings are included as "General References" only; i.e., refer to the drawings to obtain additional detail or to obtain background information. These drawings are not part of the UFSAR. They are controlled by the Controlled Documents Program.

| DRAWING* | SUBJECT |
|---|---|
| 108D685-1 | Index and Symbols Functional Diagrams |
| 108D685-2 | Reactor Trip Signals Diagram |
| 108D685-3 | Nuclear Instrumentation and Manual Trip Signals Diagram |
| 108D685-4 | Nuclear Instrumentation Permissives and Blocks Diagram |
| 108D685-5 | Primary Coolant System Trip Signals Diagram Units 1 & 2 |
| 108D685-6 | Pressurizer Trip Signals Diagram |
| 108D685-7 | Steam Generator Trip Signals Diagram |
| 108D685-8 | Safeguards Actuation Signals Diagram |
| 108D685-9 | Rod Controls and Rod Blocks Functional Diagrams Units 1 & 2 |
| 108D685-10 | Steam Dump Controls Diagram |
| 108D685-11 | Pressurizer Pressure and Level Controls Diagram |
| 108D685-12 | Pressurizer Heater Controls Diagram |
| 108D685-13 | Feedwater Controls and Isolation Units 1 & 2 |
| 108D685-14 | Feedwater Controls and Isolation Diagram |
| 108D685-15 | Auxiliary Feedwater Pumps Startup Diagram |
| 108D685-16 | Turbine Trips, Runbacks, and Other Signals Diagram |
| 108D685-17 | Loop Stop Valve Interlocks Diagram |
| 108D685-18 | Boron Dilution Protection Signals Diagram |
| M-37 | Diagram of Auxiliary Feedwater System Unit 1 |
| M-39 | Diagram of Condensate (Makeup and Overflow) System Unit 1 |
| M-48A | Composite Diagram of Liquid Radwaste Treatment Processing Units 1 & 2 |
| M-60 | Diagram of Reactor Coolant System Loops Units 1 |
| M-61 | Diagram of Safety Injection System Unit 1 |
| M-95 | Diagram of Auxiliary Building HVAC (VA) System Units 1 & 2 |
| M-96 | Diagram of Control Room HVAC System Units 1 & 2 |

DRAWINGS CITED IN THIS CHAPTER* (Cont'd)

| DRAWING* | SUBJECT |
|---|---|
| M-97 | Diagram of Diesel Generator Room 1A & 1B Ventilation System Unit 1 |
| M-98 | Diagram of Diesel Generator Room 2A & 2B Ventilation System Unit 2 |
| M-103 | Diagram of Primary Containment Ventilation (VP) System Unit 1 |
| M-104 | Diagram of Primary Containment Ventilation (VP) System Unit 2 |
| M-115 | Diagram of Essential and Non-Essential Switchgear and Miscellaneous Electrical Equipment Room Ventilation System Unit 1 |
| M-116 | Diagram of Essential and Non-Essential Switchgear and Miscellaneous Electrical Equipment Room Ventilation System Unit 2 |
| M-119 | Diagram of Cooling Tower OA/OB Electrical Substations Ventilation System Units 1 & 2 (Byron) |
| M-135 | Diagram of Reactor Coolant System Loops Unit 2 |
| M-2095 | HVAC/Controls and Instrumentation Diagram of Auxiliary Building HVAC (VA) System Units 1 & 2 |
| M-2104 | HVAC/Control and Instrumentation Diagram of Primary Containment Ventilation (VP) System Units 1 & 2 |
| M-2116 | HVAC/Controls and Instrumentation Diagram of Switchgear Heat Removal HVAC (VE, VX) Systems Units 1 & 2 |

# CHAPTER 7.0 - INSTRUMENTATION AND CONTROLS

## 7.1 INTRODUCTION

Instrumentation systems are used to monitor various process and environmental parameters throughout the plant. That information is displayed to the operator, or is transmitted to appropriate control systems during normal operation of the plant, and to reactor trip and engineered safety feature systems during abnormal and accident conditions.

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

This chapter presents the functional logic of the protection systems, which is shown in Drawings 108D685. All logic, interlocks, and associated circuitry are redundant where credit is taken in the accident analysis for their functioning to initiate the required protective action. The Westinghouse supplied systems conform to applicable criteria, such as IEEE-279 and IEEE-338, for electrical and physical separation, independence, and testing. Those interlocks required from systems located outside the protection system cabinets are required to meet Westinghouse interface requirements to assure that redundancy is not compromised and that protection system performance cannot be degraded by any single credible event.

The primary purpose of the instrumentation and control systems is to exercise proper control and provide automatic protection 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 15.0. 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.

Periodic surveillance tests on I and C protection systems identified in this section require the use of jumpers which bypass protective functions.

The use of jumpers and other temporary arrangements will be required during startup testing.

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 Table 7.1-1 for a listing of applicable criteria.

Definitions

Terminology used in this chapter is based on the definitions given in IEEE Standard 279-1971 which is listed in Subsection 7.1.2. 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 - Refer to Table 1.1-1 of the Technical Specifications.

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

Phase A Containment Isolation - Closure of all nonessential process lines which penetrate containment initiated by the safety injection signal or manually from the main control board.

Phase B Containment Isolation - Closure of remaining process lines, initiated by containment Hi-3 pressure signal (process lines do not include engineered safety features lines) or manually from the main control board.

Reactor Trip System Response Time

The reactor trip system response time shall be the time interval from when the monitored parameter exceeds its trip setpoint at the channel sensor until loss of stationary gripper coil voltage. The response time may be measured by means of any series of sequential overlapping, or total steps so that the entire response time is measured. In lieu of measurement, response time may be verified for selected components provided that the components and methodology for verification have been previously reviewed and approved by the NRC.

Nuclear Rate Trips

The nuclear rate trips are tested with simulated signals generated by switching between combinations of upper and lower detector test currents.

Engineered Safety Feature (ESF) Response Time

The ESF response time shall be that time interval from when the monitored parameter exceeds its ESF actuation setpoint at the channel sensor until the ESF equipment is capable of performing its safety function (i.e., the valves travel to their required positions, pump discharge pressures reach their required values, etc.). Times shall include diesel generator starting and sequence loading delays, where applicable. The response time may be measured by means of any series of sequential, overlapping, or total steps so that the entire response time is measured. In lieu of measurement, response time may be verified for selected components provided that the components and methodology for verification have been previously reviewed and approved by the NRC.

Engineered Safety Features Actuation System (ESFAS) Response Time

The ESFAS response time is defined as 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 Manufacturers Association PMC-20.1-1973 (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 Manufacturers 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 "postaccident" 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 element, 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 then includes 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 nonsteady-state condition.

## 7.1.1 Identification of Safety-Related Systems

### 7.1.1.1 General

The systems presented in this chapter have been grouped to agree with the grouping described in the NRC Standard Format (Regulatory Guide 1.70): reactor trip systems; engineered safety feature systems; systems required for safe shutdown; safety-related display instrumentation; other instrumentation systems required for safety; and control systems not required for safety. Table 7.1-2 lists the individual systems.

#### 7.1.1.1.1 Reactor Trip System

The reactor trip system is a functionally defined system described in Section 7.2. The equipment which provides the trip functions is identified and discussed in Section 7.2. Design bases for the reactor trip system are given in Subsection 7.1.2.1.1. Figure 7.1-1 includes a single line diagram of this system.

#### 7.1.1.1.2 Engineered Safety Features Actuation System

The engineered safety features actuation system is a functionally defined system described in Section 7.3. The

equipment which provides the actuation functions is identified and discussed in Section 7.3. Design bases for the engineered safety features actuation system are given in Subsection 7.1.2.1.2.

7.1.1.1.3 Instrumentation and Control Power Supply System

Design bases for the instrumentation and control power supply system are given in Subsection 7.1.2.3. Further description of this system is provided in Subsection 7.6.3.

7.1.1.2 Safety-Related Display Instrumentation

Display instrumentation provides the operator with information to enable him to monitor the status of the plant and the results of engineered safety features actuations following a Condition II, III, or IV event. Section 7.5, Table 7.5-1 lists indicators and records on the main control board available to the operator during Condition II, III, and IV events.

7.1.1.3 Instrumentation and Control System Designers

All systems discussed in Chapter 7.0 have definitive functional requirements developed on the basis of the Westinghouse NSSS design. Drawings 108D685 define scope interface. Regardless of the supplier, the functional requirements necessary to ensure plant safety and proper control are clearly delineated.

7.1.1.4 Plant Comparison

System functions for all NSSS discussed in Chapter 7.0 are similar to those of the SNUPPS Application. A comparison table is provided in Section 1.3. System function for non-NSSS are similar to systems provided for the Zion Station.

Chapter 7.0 identifies the safety-related systems, the reactor trip system (RTS), and the engineered safety features actuation system (ESFAS), required to shut the plant down safely. The functional performance requirements of these systems are identical at the system level to those provided for the SNUPPS application. Within these systems, minor hardware and/or control equipment supplier changes are recognized. There are also certain minor differences in ESF status indication circuitry which are unrelated to functional performance. The RTS and the ESFAS are designed and provided by Westinghouse.

7.1.2 Identification of Safety Criteria

Subsection 7.1.2.1 gives design bases for the systems given in Subsection 7.1.1.1. Design bases for non-safety-related systems are provided in the sections which describe the systems. Conservative considerations for instrument errors are included in the accident analyses presented in Chapter 15.0. 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, 7.5, and 7.6.

The documents listed in Table 7.1-1 were considered in the design of the systems given in Subsection 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. A discussion of compliance with each document for systems in its scope is provided in the referenced sections given in Table 7.1-1 for each criterion. Because some documents were issued after design and testing had been completed, the equipment documentation may not meet the format requirements of some standards. Justification, for any exceptions taken to each document for systems in its scope, is provided in the referenced sections.

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 Technical Requirements Manual (TRM) 2.0.a.

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 Standard 279-1971 are discussed in Subsection 7.2.1.2. The design limits specified by Westinghouse for the reactor trip system are:

a. Minimum DNBR shall not be less than 1.30 as a result of any anticipated transient or malfunction (Condition II faults).

b. Power density shall not exceed the rated linear power density for Condition II faults. See Chapter 4.0 for fuel design limits.

c. The stress limit of the reactor coolant system for the various conditions shall be as specified in Section 3.9.

d. 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.

e. 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 break 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 6.0 for the engineered safety features. Design bases requirements of IEEE Standard 279-1971 are addressed in Subsection 7.3.1.2. General design requirements are as follows:

a. 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 plant and containment, and automatically provide, as output, timely and effective signals to actuate the various components features systems.

b. Manual Actuation Requirements

The engineered safety features actuation system has provisions in the main control room for manually initiating the functions of the engineered safety features systems.

7.1.2.1.3 Instrumentation and Control Power Supply System

The instrumentation and control power supply system provides continuous, reliable, regulated single phase ac power to all instrumentation and control equipment required for plant safety. Details of this system are provided in Section 7.6. The design bases are as follows:

a. The inverter shall have the capacity and regulation required for the a-c output for proper operation of the equipment supplied.

b. Redundant loads shall be assigned to different distribution panels which are supplied from different inverters.

c. Auxiliary devices that are required to operate dependent equipment shall be supplied from the same distribution panel to prevent the loss of electric power in one protection set from causing the loss of equipment in another protection set. No single failure shall cause a loss of power supply to more than one distribution panel.

d. Each of the distribution panels shall have access only to its respective inverter supply and a standby power supply.

e. The system shall comply with IEEE Standard 308-1971, Paragraph 5.4.

7.1.2.1.3.1 Loss of Power Alarm or Indication in the Control Room for Class 1E and Non-Class 1E Buses

An alarm or indication of loss of power is provided in the control room either directly or indirectly, for each 6900-, 4160- and 480-Vac and 125-Vdc bus.

Each 6.9-kV and 4.16-kV bus is provided with a feed breaker trip, control power failure, and bus low voltage alarm, as well as bus energized lights on the main control board mimic bus. Each 480-V substation bus is provided with a feed breaker trip and control power failure alarm, as well as bus energized lights on the main control board mimic bus. Each 480-V motor control center (MCC) bus is provided with a feed breaker trip alarm. Loss of a-c power to a 480-V substation or MCC bus will be indicated (monitored) by the operation of the associated 6900-V or 4160-V bus low voltage alarm or feed breaker trip alarm. The identification number (name) of each motor control center is keyed to the substation from which it is supplied. Each 120-Vac instrument bus is provided with an inverter trouble (including loss of power) alarm. Each 125-Vdc bus is provided with a low voltage alarm.

In addition, each of the following cabinets is provided with a power failure or power supply trouble alarm: auxiliary relay cabinets, safeguards test cabinets, ESF sequencing and actuation cabinets, process I&C cabinets, ESF sequencing and actuation cabinets, process I&C cabinets, reactor protection

(solid-state) cabinets, transmitter power supply cabinets, MCB panels, sequence-of-events recorder (main and reserve supply), and annunciator input cabinets (main and reserve supply).

All the above alarms appear both as lights on annunciator windows and as print-out on the sequence-of-events recorder.

Since loss of power alarms and/or indications are provided for all buses, the operator will be alerted to the loss of power for each bus that supplies power to all safety-related and non-safety-related instrumentation and control systems.

7.1.2.1.4 Emergency Power System

Design bases and system description for the emergency power system are provided in Chapter 8.0.

7.1.2.1.5 Interlocks

Interlocks are discussed in Sections 7.2, 7.3, 7.6, and 7.7. The protection (P) interlocks are given in Tables 7.2-2 and 7.3-3. The safety analyses demonstrate 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 have been designed to meet IEEE Standard 279-1971 and are entirely redundant and separate, including all permissives and blocks. All blocks of a protective function are automatically cleared whenever the protective function would be required to function in accordance with General Design Criteria 20, 21, and 22 and Paragraphs 4.11, 4.12, and 4.13 of IEEE Standard 279-1971. Control interlocks (C) are identified on Table 7.7-1. Because control interlocks are not safety-related, they have not been specifically designed to meet the requirements of IEEE Protection System Standards.

7.1.2.1.6 Bypasses

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

The capability of bypass testing is provided for the 7300 Process Protection System Reactor Trip and Engineered Safety Features Actuation functions and the Nuclear Instrumentation System Reactor Trip functions.

The Bypass Test Instrumentation which allows testing in a bypassed condition instead of a tripped condition conforms to applicable regulatory criteria including IEEE 279-1971 and Regulatory Guide 1.47. Additional information concerning test in bypass can be found in WCAP-17349-P.

This page has been intentionally deleted.

7.1.2.1.7 Equipment Protection

The criteria for equipment protection are given in Chapter 3.0. Equipment related to safe operation of the plant is designed, constructed, and installed to protect it from damage. This is accomplished by working to accepted standards and criteria aimed at providing reliable instrumentation which is available under varying conditions. As an example: certain equipment is seismically qualified in accordance with IEEE Standard 344-1975. During construction, independence and separation are achieved, as required by IEEE Standard 279-1971, IEEE Standard 384-1974, either by barriers, physical separation, or demonstration test. This serves to protect against complete destruction of a system by fires, missiles, or other natural hazards.

7.1.2.1.8 Diversity

Functional diversity has been designed into the ESFAS and the reactor trip system. Functional diversity is discussed in Reference 1. The extent of diverse system variables has been evaluated for a wide variety of postulated accidents as discussed in Reference 2. 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, reactor coolant pump under-frequency and undervoltage measurements, and steam generator pressure and steam line pressure measurements as well as manually and by initiation of 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:

a. low pressurizer pressure and

b. high containment pressure (Hi-1).

For a steam break accident, safety injection signal actuation is provided by the following diverse parameter measurements:

a. low steamline pressure,

b. low pressurizer pressure, and

c. for a steam break inside containment, high containment pressure (Hi-1) 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 Standard 279-1971.

7.1.2.1.9 Bistable Trip Setpoints

Westinghouse specifies three values applicable to reactor trip and engineered safety features actuation:

a. safety limit,

b. limiting value, and

c. 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 allowable value and is obtained by subtracting a safety margin from the safety limit. The safety margin accounts for instrument error and 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 allowable values will not be exceeded under normal operation.

The setpoints that provide trip action are given in TRM 2.0.a. A further discussion on setpoints is found in Subsection 7.2.2.2.1.

The safety limit is determined by the accident analysis presented in Chapter 15.0. As described above, allowance is 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 at its 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% 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 on accuracy, linearity, and reproducibility. 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 operates normally within 5% 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 were finalized based on the results and evaluation of safety studies carried out using data pertinent to the plant. Emphasis was placed on establishing adequate performance requirements under both normal and faulted conditions. This included consideration of process transmitter 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, $\Delta T$ 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.

7.1.2.1.10 Engineered Safety Features Motor Specifications

The residual heat removal pump motors and engineered safety features auxiliary system pump motors will accelerate the driven equipment from standstill to operating speed within the required sequencing interval and with the motor terminal voltage provided by either offsite or onsite power sources.

Verification of the engineered safety features pump motor capability to operate within design temperature ratings, including the NEMA Test Specification MG1-20.43 (number of starts), is based on the design tests of the prototype motor that are performed at the manufacturer's test facilities, rather than by means of initial or periodic tests in the field.

The protective relays associated with the circuit breakers supplying the engineered safety features pump motors provide overload, stall and fail to start protection for the respective motors.

Six stator resistance type temperature detectors are embedded in the stators of engineered safety features pump motors rated above 1000 horsepower and at 4000 volts. Stator temperature for these motors is monitored.

7.1.2.1.11 Other Safety-Related Systems

Other safety-related systems described in this chapter include the following:

a. Heating, ventilating, and air conditioning (HVAC) systems which act as support systems by maintaining the environment of the rooms and/or buildings which contain portions of safety-related systems (including auxiliary building HVAC, main control room HVAC, auxiliary electric equipment room HVAC, diesel generator room ventilation, miscellaneous electric equipment room ventilation, switchgear

heat removal, and portions of chilled water relating to main control room HVAC).

See Section 7.3 for system description and design bases.

b. Other safety-related systems not already covered elsewhere (including diesel oil, post-LOCA hydrogen recombiner, neutron monitoring, and portions of chemical and volume control which supplies reactor coolant pumps with seal water).

See Section 7.6 for description and design bases.

7.1.2.2 Independence of Redundant Safety-Related Systems

The safety-related systems in Subsection 7.1.1.1 are designed to meet the independence and separation requirements of Criterion 22 of the 1971 General Design Criteria and Paragraph 4.6 of IEEE Standard 279-1971. For detailed information, see Subsection 8.3.1.4.

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 shall include, but not be limited to, the effects of short circuits, pipe breaks, missiles, fire, etc., and are considered in the basic plant design. Control board details are given in Section 7.5. In the control board, separation of redundant circuits is maintained as described in Subsection 7.1.2.2.2.

7.1.2.2.1 General

The physical separation criteria for redundant safety-related system sensors, sensing lines, wireways, cables, and components on racks within the NSSS scope meet recommendations contained in the physical independence of electric system with the following comments:

a. The Westinghouse design of the protection system relies on the provisions of IEEE 384-1974 relative to meeting Regulatory Guide 1.75 with overcurrent devices to prevent malfunctions in one circuit from causing unacceptable influences on the functioning of the protection system. 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.

b. Because of different functional requirements, main control boards contain redundant circuits which are required to be physically separated from each other. However, since there are no redundant circuits which share a single compartment of an NSSS protection instrumentation rack and since these redundant protection instrumentation racks are physically separated from each other, the physical separation requirements specified for the main control board do not apply.

   However, redundant, isolated control signal cables leaving the protection racks are brought into close proximity elsewhere in the plant, such as the control board. It could be postulated that electrical faults or interference at these locations might be propagated into all redundant racks and degrade protection circuits because of the close proximity of protection and control wiring within each rack. IEEE 384-1974 Paragraph 4.5(3) provides the option to demonstrate that the absence of physical separation could not significantly reduce the availability of Class 1E circuits.

   The nuclear instrumentation and solid-state protection systems were included in the "Westinghouse Protection System Noise Tests" report submitted and accepted by the NRC in support of the Diablo Canyon application (Docket Numbers 50-275 and 50-323). The tests on the Process Control System - 7300 Series are reported in Reference 4, the conclusions having been accepted by the NRC.

   Provisions are made to provide assurance that maximum credible fault voltages and conditions which could be postulated in the Byron and Braidwood Stations, as a result of BOP cable routing design, will not exceed those used in the tests.

   These Westinghouse tests demonstrated that protection system performance would not be degraded even if subjected to abnormal electrical conditions which far exceed those which can be reasonably postulated.

c. The physical separation criteria for instrument cabinets supplied by Westinghouse meet the recommendations contained in Paragraph 5.7 of IEEE 384-1974.

7.1.2.2.2 Specific Systems

Independence is maintained 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 protection channel set. Redundant analog equipment is separated by locating modules in different protection rack sets. Each redundant channel set is energized from a separate a-c power feed.

There are four separate process analog sets. Separation of redundant analog channels begins at the process sensors and is maintained in the field wiring, containment penetrations, and analog protection cabinets to the redundant trains in the logic racks. Redundant analog channels are separated by locating modules in different cabinets. Since all equipment within any cabinet is associated with a single protection set, there is no requirement for separation of wiring and components within the cabinet.

In the nuclear instrumentation system, process systems, and the solid-state protection system input cabinets where redundant channel instrumentation are physically adjacent, there are no wireways 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. Redundant analog channels are separated by locating modules in different cabinets. Since all equipment within any cabinet is associated with a single protection set, there is no requirement for separation of wiring and components within the cabinet.

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.

Reactor Trip System

a. 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.

b. Separate routing of the redundant reactor trip signals from the redundant logic system cabinets is maintained, and in addition, they are separated (by

spatial separation, by provision of barriers, or by separate cable trays or wireways) from the four analog channel sets.

Engineered Safety Features Actuation System

a. Separate routing is maintained for the four basic sets of engineered safety features actuation system analog sensing signals, bistable output signals, and power supplies for such systems. The separation of these four channel sets shall be maintained from sensors to instrument cabinets to logic system input cabinets.

b. Separate routing of the engineered safety features actuation signals from the redundant logic system cabinets is maintained. In addition, they are separated by spatial separation or by provisions of barriers or by separate cable trays or wireways from the four analog channel sets.

c. Separate routing of control and power circuits associated with the operation of engineered safety features equipment is required to retain redundancies provided in the system design and power supplies.

Instrumentation and Control Power Supply System

a. The separation criteria presented also apply to the power supplies for the load centers and buses distributing power to redundant components and to the control of these power supplies.

Reactor trip system and engineered safety features actuation system analog circuits may be routed in the same wireways provided circuits have the same power supply and channel set identified (I, II, III, or IV).

7.1.2.2.3 Fire Protection

Details of the plant's fire protection system are provided in the Byron/Braidwood Fire Protection Report (Reference 5).

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. The solid-state protection system input cabinets are divided into four isolated compartments, each serving one of the four redundant input channels. Horizontal 1/8-inch thick solid steel barriers, coated with fire-retardant paint, separate the compartments. Four 1/8-inch thick solid steel wireways coated with fire-retardant paint enter the input cabinets vertically, even in its own quadrant. The wireway for a particular compartment is open only into the compartment so that flame could not propagate to affect other channels. A diagram of the input cabinet is given in Figure 7.1-2. At the logic racks, the protection set color coding for redundant channels is clearly maintained until the channel looses its identity in the redundant logic trains.

This subject is discussed in Subsection 8.3.1.3.

7.1.2.4 Conformance to Criteria

A listing of applicable criteria and the UFSAR sections where conformance is discussed is given in Table 7.1-1.

7.1.2.5 Instrument Lines Penetrating Primary Reactor Containment

Guidelines for instrument lines which penetrate primary reactor containment and which are part of the reactor coolant pressure boundary do not apply since there are no lines which fall directly in this category. Two instrument lines penetrating reactor containment are used for the integrated leak rate test (ILRT) system. These instrument lines are each equipped with two manual valves (one internal and one external), which are located as close as possible to the containment wall. These valves are administratively controlled in a locked closed position, except during periods of ILRT surveillance testing. Containment pressure is monitored by six redundant pressure transmitters (four narrow range, two wide range) located outside containment. Each transmitter monitors containment atmosphere pressure through a sealed capillary line filled with silicone oil to a bellows sensor located inside containment exposed to atmosphere. The lines both inside and outside containment are kept as short as minimum bending radii permit. Similarly, four redundant pressure transmitters located outside containment monitor reactor coolant system (RCS) pressure through two shared capillary lines filled with deaerated distilled water each to a bellows sensor located inside containment exposed to RCS fluid. Another instrument line penetrating reactor containment is filled with distilled water and is used in conjunction with a deadweight

tester to provide a calibration check of pressurizer pressure transmitters. This instrument line is equipped with a manual valve external, but as close as possible, to the containment wall. The valve is administratively controlled in a locked closed condition, except during periods of testing installed pressurizer pressure instruments. No other instrument lines penetrate reactor containment.

7.1.2.6 Periodic Testing of Protection System Actuation Functions (Regulatory Guide 1.22)

Periodic testing of the reactor trip and engineered safety features actuation systems is described in Subsections 7.2.2 and 7.3.2.

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 light for the train under 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.

Administrative and procedural controls are used to prevent testing of more than one redundant protection set of the analog circuitry simultaneously.

The actuation logic for the reactor trip and engineered safety features actuation system is tested as described in Sections 7.2 and 7.3. Where actuated equipment is not tested during reactor operation, it has been determined that;

a. there is no practicable system design that would permit operation of the equipment without adversely affecting the safety or operability of the plant or the equipment is not available for testing due to conflicting Technical Specification LCO requirements that place the equipment in its safeguards actuated condition with power removed;

b. 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

c. the equipment can routinely be tested when the reactor is shut down.

The list of equipment that cannot be tested at full power so as not to damage equipment or upset plant operations is:

a. manual actuation switches,

b. reactor coolant pump breakers,

c. turbine (trips),

d. main steamline isolation valves (close),

e. main feedwater isolation valves (close),

f. feedwater control valves (close),

g. main feedwater pump trip solenoids,

h. reactor coolant pump component cooling return isolation valves (close), and

i. reactor coolant pump seal water return valves (close).

The justifications for not testing items a through i above at full power are discussed below.

Manual Actuation Switches - These 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:

a. The analog signals, from which the automatic safety injection signal is derived, are tested at power in the same manner as the other analog signals and as described in Subsection 7.2.2.2.3 (item j). 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 semiautomatic test provisions of the SSPS.

Tripping of Reactor Coolant Pump Breakers

No credit is taken in the accident analyses for a reactor coolant pump breaker opening causing a direct reactor trip. Since testing the reactor coolant pump breakers at power would cause plant upset, they do not need to be tested at power.

Turbine

The reactor protection system receives anticipatory trip signals from the turbine via pressure switch contacts actuated by loss of emergency trip fluid pressure or limit switch contacts actuated by closure of the turbine stop valves. Testing which would result in the generation of either of these two trip signals with the reactor at power would produce a reactor trip and plant upset. Turbine anticipatory trips to the reactor protection system provide additional protection and conservatism beyond that required for the health and safety of the public and are provided as good engineering practice and design.

Conversely, turbine trips can be generated as a result of reactor trips. Therefore, testability of the turbine trip system is provided to meet the guidelines for bypass conditions for protection system trip signals. On-line testability is provided as follows:

a. Steam Inlet Valve Testing

A functional test of the turbine steam inlet valves can be made while the unit is carrying loads. The purpose of this test is to ensure proper operation of the throttle valves, governor valves, reheat stop valves, and interceptor valves. A complete check of the valve stem freedom of the throttle valves can be made up to 100% of maximum load. The load at which the test of the governor valves is to be performed can be set at any point between the minimum load point and the maximum load point (usually around 90% of rated load). The maximum load is the load that can be carried when one

governor valve is completely closed. The reheat inlet valves (reheat stop and interceptor valves) can be tested at any load up to maximum load with no more than 2% load reduction during the test. In addition to the above test, the following design features also improve valve reliability.

1. The digital electrohydraulic (DEH) control system utilizes improved filtration systems which should minimize the possibility of relevant failures due to impurities in the oil. This is an improvement over older designs with valve servo actuators using lubricating oil.

2. Improved valve position monitoring systems for DEH control systems.

3. Decreased valve closure time with DEH systems as compared to systems having servos using lubricating oil.

4. Increased closing force on the governor valves as compared to governor valves on earlier units.

5. Steam sealed throttle valve stems, back-seated in the full open position to minimize the potential of deposits.

6. Steam sealed governor valve stems back-seated in the full open position to minimize the potential of deposits.

7. Spiral grooves in each valve stem to help break up deposits on the bushing or stem when the valve is stroked.

In addition, the all volatile treatment (AVT) water chemistry should greatly decrease the possibility of phosphates producing valve stem deposits.

b. Turbine Trip System Testing

The trip manifold is designed to allow for on-line testing of individual solenoid valves. On-line testing does not require additional solenoids or valves, which would change the configuration of the trip system such that the testing state is different from the normal operation of the system. When performing on-line testing, the turbine trip system is still fully functional such that an actual turbine trip can be processed while the test is in progress. The test is initiated by the operator via the emergency trip system (ETS) human machine interface display. No other valve or manifold tests are allowed by the control system while the manifold test is in progress. The Ovation controller monitors ETS and operator auto trip manifold pressures for normal conditions. The solenoid selected for test is de-energized and pressure is monitored for the correct condition after a timer has expired. If the pressure has reacted in the correct manner, the solenoid is energized and pressure is monitored again for correct response after a timer has expired. If a solenoid is determined to have failed the test sequence, testing capability for all remaining solenoids on that trip manifold will be disabled and a test failure message will appear on the testing display.

c. Turbine Overspeed Protection Control

There are three independent overspeed protection systems. The Braun system uses three turbine speed channels, each with its own magnetic speed pickup, arranged in a two out of three logic configuration. The turbine overspeed hard and soft logic is also provided in the Ovation emergency trip system and operator auto controllers. The Ovation speed detector modules sense turbine speed. There are three modules per controller. These controllers use two out of three logic from the turbine speed channels for overspeed sensing and tripping. As a result, a malfunction in any one of these channels will not cause an invalid trip or prevent a valid trip. Logic is also provided in the controllers to detect and identify a malfunction in the speed pickups.

The overspeed control, using two out of three logic, will slow the turbine by energizing the OPC solenoids, which will in turn close the governor valves and intercept valves when turbine speed exceeds 103%. The normal overspeed protection control is designed to regulate the turbine speed back to within normal range and avoid a turbine overspeed trip. A diagram of the turbine protection system is shown in Figure 7.1-4.

Closing the Main Steamline Isolation Valves

Main steam isolation valves are periodically tested. Testing of main steam isolation valve closure at power would cause a plant upset and reactor trip.

Capability is provided to perform a partial operational test of the main steam isolation valves. Manual controls are provided to separately test the two redundant control circuit channels which actuate each valve. Test actuation of the valve will cause it to move from the full open position to the 90% open position and automatically return to the full open position.

The test will prove control circuit, valve, and valve actuator operability to the extent as stated above.

Closing the Feedwater Isolation Valve

The feedwater isolation valves are periodically tested. Fully closing of these feedwater isolation valves at power would cause a plant upset and trip the reactor.

Capability is provided to perform a partial operational test of the feedwater isolation valves. Manual controls are provided to separately test the two redundant control circuit channels which actuate each valve. Test actuation of the valve will cause it to move from the full open position to the 90% open position and automatically return to the full open position. The test will prove the control circuit, valve, and valve actuator operability to the extent as stated above.

The acceptability of performing the partial operational test may be limited by certain plant load conditions to preclude the possibility of feedwater perturbations which might result in reactor upset.

Closing the Feedwater Control Valves

These valves are periodically tested. To close these valves at power would cause a plant upset and trip the reactor. The verification of operability of feedwater control valves at power is assured by confirmation of proper operation of the steam generator water level system. The actuation of the slave relays, which provide closing function, is periodically tested as discussed in Subsection 7.3.2.2.5. Although the actual closing of these control valves is blocked when the slave relay is tested, all functions are tested to ensure that no electrical malfunctions have occurred which could defeat the protective function. It is noted that the solenoids work on the deenergize-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.

Main Feedwater Pump Trip Solenoids

Tripping of the feedwater pumps on safety injection signal is provided in addition to the closing of the feedwater isolation valves, feedwater control valves, and feedwater pump discharge valves. This trip is provided to protect the feedwater pumps from undesirable damage. Since actuation of the trip solenoids at power for test purposes would cause plant upset, they do not need to be tested at power.

RCP Component Cooling Water Isolation Valves

Component cooling water supply and return containment isolation valves are periodically tested. 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 immediately 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 10 minutes after component cooling water is isolated, pump damage could be incurred.

Based on the above described potential reactor coolant pump damage, these valves will be routinely tested only when the reactor coolant pumps are not operating.

Seal Water Return Valves

Seal return line isolation valves are periodically tested. Closure of these valves during operation would cause the CV 8121 relief valve to lift, with the possibility of valve chatter and damage to the relief valve.

### 7.1.2.7 Seismic Design Classification

Seismic Category I classification has been assigned to all instruments which perform a safety-related function.

Instrumentation and controls for the items listed in Chapter 3.0, Table 3.2-1 as Seismic Category I have likewise been specified to withstand the effects of the SSE and remain functional.

### 7.1.2.8 Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment

A Quality Assurance Program in conformance with the requirements of 10 CFR 50 Appendix B is imposed on the suppliers of all safety-related control and instrumentation equipment and systems. These requirements are also imposed on the installation and testing of these systems and equipment. Specifications impose requirements to conform to IEEE Standard 336-1985 (NQA-1-1994, Subpart 2.4). Test results are required submittals.

### 7.1.2.9 Qualification Tests of Continuous Duty Motors Installed Inside the Containment of Water-Cooled Nuclear Power Plant

Refer to Subsection 8.1.7 for discussion of conformance to these guidelines.

7.1.2.10 Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems (Regulatory Guide 1.47)

Regulatory Guide 1.47 requires a means of displaying indication of bypassed or inoperable equipment important to safety at the system level. Since this regulatory guide was issued in May of 1973 and the since accident at Three Mile Island, great progress has been made in the area of human factors consideration for the design of plant systems and the layout of the control room. The NRC has issued several rules and regulations, such as Regulatory Guide 1.97, NUREG-0700 "Guidelines for Control Room Design Reviews," and NUREG-0737, "Clarification of TMI Action Plan Requirements," which resulted in significant changes in the design and operation of nuclear power plants. These design changes have been implemented and have resulted in improvements in the amount and utility of the information being made available to the operators. Braidwood and Byron Stations meet the requirements of Regulatory Guide 1.47 with the following main control room indications, alarms, and features:

a. six monitor light panels, described in Subsection 7.5.1, display pertinent information to the operator to verify functions being performed and provide the operator with the information necessary to quickly assess the status of key remotely operated engineered safety features (ESF) valves, motors, or other essential components,

b. bypass permissive and trip status lights arranged by function provide information to the operator on the status of the bypass permissive and bistable of the protection systems and serve to alert the operators of abnormal conditions,

c. main control board panels designed with system and functional grouping to facilitate their operation; lines of demarcation to highlight panel and system separation,as well as critical instrumentation; labels to present information in a hierarchical fashion;and background shading to enhance functional relationships between controls and displays within and across panels,

d. main control boards designed with the green board concept (individual component controls are green when they are in their normal lineup above 30% power) to allow for immediate operator recognition of any abnormal condition which would be indicated by red lights,

e. a control room annunciator system designed so all annunciator windows are dark when no abnormal condition exists at power (illuminated windows allow operators to quickly identify abnormal plant conditions), and

f. a sequence of events recorder which allows the operators to quickly review any abnormal indications throughout the stored information and take any appropriate action quickly.

In addition to the above plant design changes, many administrative programs and procedures are in place to aid operator knowledge of the plant status. These include the following:

a. a locked valve program controls the position of critical manual valves to ensure safety functions will be fulfilled,

b. an abnormal position log manually tracks any equipment that is maintained in a position that differs from the normal at-power lineup,

c. a Technical Specification Limiting Conditions for Operation (LCO) tracking system tracks the status of all LCOs,

d. a degraded equipment log provides readily available information on important equipment that has experienced some form of degradation, and

e. a computerized out-of-service program tracks equipment out of service.

7.1.2.11 Application of the Single Failure Criterion to Nuclear Power Plant Protection System (Regulatory Guide 1.53)

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 for application of the single failure criterion to nuclear power plant protection systems (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.

7.1.2.12 Manual Initiation of Protective Actions

Conformance to these guidelines is discussed in Subsection 7.2.1 Item h (for reactor trip) and in Subsection 7.3.2 (for ESF actuation).

7.1.2.12.1 Manual Initiation of Protective Actions Required by Regulatory Guide 1.62

The manual reactor trip consists of two switches, switch A and switch B. 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.

There are four individual main steam isolation valve momentary control switches (one per loop) mounted on the control board. Each switch, when actuated, isolates one of the main steamlines. In addition, there are two system level switches. Each switch will actuate all four main steamline isolation valves.

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. Portions of the safety injection initiation circuitry are shared between the manual and automatic initiation functions. There is no sharing of circuitry between trains, therefore, a single failure in a shared function of train A does not defeat the protective action of train B. It is further noted that the sharing of the logic by manual and automatic initiation is consistent with the system level action

requirements of IEEE 279-1971, Paragraph 4.17, and consistent with the minimization of complexity.

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

Backup manual actuation switches link the separate trains by mechanical means to provide greater reliability of operator action for the manual reactor trip function and manual engineered safety features actuations. The linked switches are redundant so that operation of either set of linked switches will actuate safety trains A and B simultaneously. This is shown in Figure 7.1-5. The design of the manual reactor trip function and manual ESF actuations complies with Regulatory Guide 1.62. Regulatory Guide 1.62 references IEEE 279-1971 for the manual initiations required for protective actions.

7.1.2.13 Electric Penetration Assemblies in Containment Structures for Light-Water-Cooled Nuclear Power Plants

Refer to Subsection 8.1.12 for discussion of conformance to these guidelines.

7.1.2.14 Initial Test Programs for Water-Cooled Reactor Power Plants

Refer to Chapter 14.0 for discussion of conformance to guidelines for preoperational testing.

7.1.2.15 Qualification Tests of Electric Valve Operators Installed Inside the Containment of Nuclear Power Plants

Refer to Subsection 8.1.13 for discussion of conformance to this requirement.

7.1.2.16 Physical Independence of Electric Systems

Physical separation of safety-related control and instrumentation circuits are discussed in Subsection 8.3.1.4. Identification of safety-related control and instrument circuits and equipment is discussed in Subsection 8.3.1.3.

7.1.2.17 Preoperational Testing of Instrument Air Systems

Refer to Chapter 14.0 for discussion of this subject.

7.1.2.18 Qualification Program

Conformance to requirements for preoperational testing of instrument air systems and to IEEE Standards 323-1974 is discussed in Section 3.11. See Table 7.1-1 for references to discussions of NSSS equipment. Manufacturers of safety-related control and instrumentation equipment provided programs to show qualification to IEEE Standard 323-1974. In some instances where similar components were furnished by a number of separate contractors, the Licensee provided the qualification program.

7.1.2.19 Conformance to IEEE Standard 338-1987

The periodic testing of the reactor trip system and engineered safety features actuation system conforms to the requirements of IEEE Standard 338-1987 and RG 1.118 with the following comments.

a. The surveillance requirements of the technical specifications for protective systems 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, excluding sensors, signal processing and actuation logic.

   Overall protection systems response times are demonstrated by test. Response time may be verified by actual response time tests in any series of sequential, overlapping or total channel measurements, or by the summation of allocated sensor, signal processing, and actuation logic response times with actual response time tests on the remainder of the channel. Allocations for sensor response times may be obtained from: (1) historical records based on acceptable response time tests (hydraulic, noise, or power interrupt tests), (2) inplace, onsite, or offsite (e.g. vendor) test measurements, or (3) utilizing vendor engineering specifications. Allocations for signal processing and actuation logic response times may be obtained from (1) inplace, onsite, or offsite test measurements, or (2) utilizing vendor engineering specifications. The Nuclear Instrumentation System detectors are excluded since they exhibit response time characteristics such that delays attributable to them are negligible in the overall channel response time required for safety.

   Each test shall include at least one logic train such that both logic trains are tested at least once per 36 months and one channel per function such that each channel is tested at least once during N surveillance frequency interals, where N is the total number of redundant channels in a specific protective function.

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

b. Where practical, test devices or procedures incorporate the test methods necessary to perform periodic testing. After completion of testing, the operability or safety function is restored.

c. Technical Specifications definitions may take precedence over those in the standard.

7.1.3 References

1. W. C. Gangloff and W. D. Loftus, "An Evaluation of Solid State Logic Reactor Protection in Anticipated Transients," WCAP-7706-L, February 1973 (Proprietary), and WCAP-7706, February 1973 (Non-Proprietary).

2. D. N. Katz, "Solid State Logic Protection System Description," WCAP-7488-L, March 1971 (Proprietary), and WCAP-7672, May 1971 (Non-Proprietary).

3. The Institute of Electrical and Electronic Engineers, Inc., "Criteria for Protection Systems for Nuclear Power Generating Station," IEEE Standard 279-1971.

4. R. M. Siroky and F. W. Marasco, "7300 Series Process Control System Noise Test," WCAP-8892A (Non-Proprietary), June 1977.

5. Commonwealth Edison Company, "Byron/Braidwood Stations Fire Protection Report in Response to Appendix A of BTP APCSB 9.5-1" (current amendment).

TABLE 7.1-1

LISTING OF APPLICABLE CRITERIA

| CRITERIA | TITLE | CONFORMANCE DISCUSSED IN |
|---|---|---|
| 1. General Design Criteria (GDC), Appendix A to 10 CFR 50 (In general discussed in Section 3.1) | | |
| GDC 1 | Quality Standards and Records | 3.1.2, 17 |
| GDC 2 | Design Bases for Protection Against Natural Phenomena | 3.1.2, 3.10, 7.2.1.1.11 |
| GDC 3 | Fire Protection | 3.1.2, 7.1.2.2.3 |
| GDC 4 | Environmental and Missile Design Bases | 3.1.2, 7.2.2.2 |
| GDC 5 | Sharing of Structures, Systems and Components | 3.1.2 |
| GDC 10 | Reactor Design | 3.1.2, 7.2.2.2 |
| GDC 12 | Suppression of Reactor Power Oscillations | 3.1.2 |
| GDC 13 | Instrumentation and Control | 3.1.2, 7.3.1, 7.3.2 |
| GDC 15 | Reactor Coolant System Design | 3.1.2, 7.2.2.2 |
| GDC 17 | Electric Power Systems | 3.1.2, 7.2.2.2 |
| GDC 19 | Control Room | 3.1.2 |
| GDC 20 | Protection System Functions | 3.1.2, 7.2.2.2, 7.3.1, 7.3.2 |

TABLE 7.1-1, (Cont'd)

| CRITERIA | TITLE | CONFORMANCE DISCUSSED IN |
|---|---|---|
| GDC 21 | Protection System Reliability and Testability | 3.1.2, 7.2.2.2, 7.3.1, 7.3.2 |
| GDC 22 | Protection System Independence | 3.1.2, 7.1.2.2, 7.2.2.2, 7.3.1, 7.3.2 |
| GDC 23 | Protection System Failure Modes | 3.1.2, 7.2.2.2, 7.3.1, 7.3.2 |
| GDC 24 | Separation of Protection and Control Systems | 3.1.2, 7.2.2.2, 7.3.1, 7.3.2 |
| GDC 25 | Protection System Requirements for Reactivity Control Malfunctions | 3.1.2, 7.3.2 |
| GDC 26 | Reactivity Control System Redundancy and Capability | 3.1.2 |
| GDC 27 | Combined Reactivity Control Systems Capability | 3.1.2, 7.3.1, 7.3.2 |
| GDC 28 | Reactivity Limits | 3.1.2, 7.3.1, 7.3.2 |
| GDC 29 | Protection Against Anticipated Operational Occurrences | 3.1.2, 7.2.2.2 |
| GDC 30 | Quality of Reactor Coolant Pressure Boundary | 3.1.2 |
| GDC 31 | Fracture Prevention, Reactor Coolant Pressure Boundary | 3.1.2 |
| GDC 32 | Inspection of Reactor Coolant Pressure Boundary | 3.1.2 |

TABLE 7.1-1 (Cont'd)

| CRITERIA | TITLE | CONFORMANCE DISCUSSED IN |
|---|---|---|
| GDC 33 | Reactor Coolant Makeup | 3.1.2 |
| GDC 34 | Residual Heat Removal | 3.1.2 |
| GDC 35 | Emergency Core Cooling | 3.1.2, 7.3.1, 7.3.2 |
| GDC 37 | Testing of Emergency Core Cooling System | 3.1.2, 7.3.2 |
| GDC 38 | Containment Heat Removal | 3.1.2, 7.3.1, 7.3.2 |
| GDC 40 | Testing of Containment Heat Removal System | 3.1.2, 7.3.2 |
| GDC 41 | Containment Atmosphere Cleanup | 3.1.2, 7.3.2 |
| GDC 43 | Testing of Containment Atmosphere Cleanup Systems | 3.1.2, 7.3.2 |
| GDC 44 | Cooling Water | 3.1.2 |
| GDC 46 | Testing of Cooling Water System | 3.1.2, 7.3.2 |
| GDC 50 | Containment Design Basis | 3.1.2 |
| GDC 54 | Piping Systems Penetrating Containment | 3.1.2 |
| GDC 55 | Reactor Coolant Pressure Boundary Penetrating Containment | 3.1.2 |
| GDC 56 | Primary Containment Isolation | 3.1.2 |
| GDC 57 | Closed Systems Isolation | 3.1.2 |

TABLE 7.1-1 (Cont'd)

| CRITERIA | TITLE | CONFORMANCE DISCUSSED IN |
|---|---|---|
| 2. Institute of Electrical and Electronics Engineers (IEEE) Standards: | | |
| IEEE Std 279-1971 (ANSI N42.7-1972) | Criteria for Protection Systems for Nuclear Power Generating Stations | 7.1, 7.2, 7.3, 7.6 |
| IEEE Std 308-1971 | Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations | 7.6 |
| IEEE Std 317-1972 | Electric Penetration Assemblies in Containment Structures for Nuclear Power Generating Stations | 8.1.12 |
| IEEE Std 323-1974 | IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations | 3.11 |
| IEEE Std 334-1971 | Type Tests of Continuous-Duty Class I Motors Installed Inside the Containment of Nuclear Power Generating Stations | Appendix A |
| IEEE Std 336-1985 (NQA-1-1994, Subpart 2.4) | Installation, Inspection and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations | 7.1.2.15, 7.1.2.8 |

TABLE 7.1-1 (Cont'd)

| CRITERIA | TITLE | CONFORMANCE DISCUSSED IN |
|---|---|---|
| IEEE Std 338-1975 | Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems | 8.1.18 |
| IEEE Std 338-1987 | Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems | 7.1.2.19 |
| IEEE Std 344-1975 (ANSI N41.7) | Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations | 3.10, 8.1.19 |
| IEEE Std 379-1972 (ANSI N41.2) | Guide for the Application of the Single Failure Criterion to Nuclear Power Generating Station Protection Systems | 7.1.2.11 |
| IEEE Std 382-1972 | Type Test of Class I Electric Valve Operators | Appendix A |
| IEEE Std 384-1974 (ANSI N41.4) | Criteria for Separation of Class IE Equipment and Circuits | 7.1.2.2.1 |
| 3. Regulatory Guides (RG) (In general discussed in Appendix A) | | |

4. Branch Technical Positions*
(BTP) EICSB

| | | |
|---|---|---|
| BTP EICSB 1 | Backfitting of the Protection and Emergency Power Systems of Nuclear Reactors | 7, 8 |
| BTP EICSB 3 | Isolation of Low Pressure Systems from the High Pressure Reactor Coolant System | 7.6.2 |

TABLE 7.1-1 (Cont'd)

| CRITERIA | TITLE | CONFORMANCE DISCUSSED IN |
|---|---|---|
| BTP EICSB 4 | Requirements on Motor-Operated Valves in the ECCS Accumulator Lines | 7.6.4 |
| BTP EICSB 5 | Scram Breaker Test Requirements - Technical Specifications | 7.2.2, Tech. Spec. |
| BTP EICSB 9 | Definition and Use of "Channel-Calibration" - Technical Specifications | Tech. Spec. |
| BTP EICSB 10 | Electrical and Mechanical Equipment Seismic Qualification Program | 3.10 |
| BTP EICSB 12 | Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service | 7.2.2, Tech. Spec. |
| BTP EICSB 13 | Design Criteria for Auxiliary Feedwater Systems | 7.3.2 |
| BTP EICSB 14 | Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors | 7.7.2, 15.2.1, 15.2.2, 15.3.6 |
| BTP EICSB 15 | Reactor Coolant Pump Breaker Qualification | 7.1.2, 7.2.1 |
| BTP EICSB 18 | Application of the Single Failure Criteria to Manually-Controlled Electrically-Operated Valves | Tech. Spec. |

TABLE 7.1-1 (Cont'd)

| CRITERIA | TITLE | CONFORMANCE DISCUSSED IN |
|---|---|---|
| BTP EICSB 20 | Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode | 7.6.5, 6.3.2, Table 6.3-7 |
| BTP EICSB 21 | Guidance for Application of Regulatory Guide 1.47 | 7.1.2 |
| BTP EISCB 22 | Guidance for Application of Regulatory Guide 1.22 | 7.1.2 |
| BTP EISCB 23 | Qualification of Safety-Related Display Instrumentation for Post-Accident Condition Monitoring and Safe Shutdown | 7.5 |
| BTP EISCB 24 | Testing of Reactor Trip System and Engineered Safety Feature Actuation System Sensor Response Times | 7.1.2 |
| BTP EISCB 25 | Guidance for the Interpretation of General Design Criterion 37 for Testing the Operability of the Emergency Core Cooling System as a Whole | 3.1.2 |

TABLE 7.1-1 (Cont'd)

| CRITERIA | TITLE | CONFORMANCE DISCUSSED IN |
|---|---|---|
| BTP EISCB 26 | Requirements for Reactor Protection System Anticipatory Trips | 7.2.1.1 |
| BTP EISCB 27 | Design Criteria for Thermal Overload Protection for Motors of Motor-Operated Valves | 8.3.1 |

* Branch Technical Positions discussed are those in effect on date of docketing the FSAR.

TABLE 7.1-2

IDENTIFICATION OF SAFETY-RELATED FEATURES*

| SYSTEM | NOTES |
|---|---|
| Reactor Trip System | 1 |
| Engineered Safety Features Actuation System | 1 |
| Instrumentation and Control Power Supply System | 1 |
| Emergency Power System | |
| Diesel Fuel Oil | |
| Component Cooling | 1 |
| Containment Spray | 2 |
| Post-LOCA Hydrogen Recombiner System | |
| Ex-core Neutron Monitoring | 1 (3 at Byron) |
| Residual Heat Removal | 1 |
| Auxiliary Feedwater | 2 |
| Safety Injection | 1 |
| Essential Service Water | |
| Auxiliary Building HVAC | |
| Chemical and Volume Control | 3 |
| Control Room, Auxiliary Electric Equipment Room HVAC | |
| Diesel-Generator Room Ventilation | |
| Misc. Electric Equipment Room Ventilation | |
| Primary Containment Ventilation (only the portion containing the Reactor Containment Fan Coolers) | |
| Switchgear Heat Removal | |
| Chilled Water (only the portion relating to the Main Control Room) | |

The following systems have some safety-related instrumentation associated with them which is supplied by Westinghouse:

SYSTEM

Boric Acid Processing
Main Feedwater
Main Steam
Reactor Coolant
Reactor Coolant Pressurizer

*See Table 3.2-1 for safety category and quality group classifications

Note 1 - System is designed and built by Westinghouse.

Note 2 - System is designed and built by the AE but contains some Westinghouse supplied instrumentation.

Note 3 - System is designed and built by Westinghouse but contains some instrumentation supplied by others.

## 7.2 REACTOR TRIP SYSTEM

### 7.2.1 Description

#### 7.2.1.1 System Description

The reactor trip system automatically keeps the reactor operating 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. In any event, 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 makeup the reactor trip system (see References 1, 2, and 3 for additional background information):

a. process instrumentation and control system,

b. nuclear instrumentation system,

c. solid state logic protection system,

d. reactor trip switchgear, and

e. manual actuation circuit.

The reactor trip system consists of sensors which, when connected with analog circuitry consisting of two to four redundant channels monitor 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 trains, A and B, is capable of opening a separate and independent reactor trip breaker, RTA and RTB, respectively. The two trip breakers in series connect three-phase a-c power from the rod drive motor generator sets to the rod drive power cabinets, as shown in Drawings 108D685. During plant power operation, a d-c 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 a reactor trip, a loss of d-c voltage to the undervoltage coil, as well as energization of the shunt trip coil, trips open the breaker; a manual trip also energizes the shunt trip coil. 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.

7.2.1.1.1 Functional Performance Requirements

The reactor trip system automatically initiates reactor trip:

a. whenever necessary to prevent fuel damage for an anticipated operational transient (Condition II);

b. to limit core damage for infrequent faults (Condition III); and

c. 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 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 7.2-1 provides a list of reactor trips which are described below.

a. Nuclear overpower trips

The specific trip functions generated are as follows:

1. 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 per channel, each with its own trip setting used for a high and a 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% power (P-10). Three out of the four channels below 10% automatically reinstates the trip function. Refer to Table 7.2-2 for a listing of all protection system interlocks.

2. Intermediate range high neutron flux trip

The intermediate range high neutron flux trip circuit trips the reactor when one 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% 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 (including detectors) are separate from the power range channels. The intermediate range channels can be individually bypassed at the nuclear instrumentation racks to permit channel testing during plant shutdown or prior to startup. This bypass action is annunciated on the control board.

3. Source range high neutron flux trip

The source range high neutron flux trip circuit trips the reactor when one of the two source range channels exceeds the trip setpoint. This trip, which provides protection during reactor startup and plant shutdown, can be manually 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 above the P-6 setpoint (source range cutoff power level) but below 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.

4. 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 provides DNB protection against rod ejection accidents of low worth from mid-power and is always active. Circuit calibration is always active. Circuit calibration is performed periodically, see Technical Specification 3.3.1. To confirm proper setting, see Technical Requirements Manual, (TRM) 2.0.a.

5. Power range high negative neutron flux rate trip

   Automatic trip protection against one or more dropped rods is not required to prevent occurrence of DNBR per Westinghouse WCAP 11394-P-A, subject to plant/cycle specific analysis.

   The Power Range high negative neutron flux rate trip was removed from the Technical Specification and the automatic trip feature eliminated concurrent with NRC approval.

b. Core thermal overpower trips

The specific trip functions generated are as follows:

1. Overtemperature $\Delta T$ trip

This trip protects the core against low DNBR and trips the reactor on coincidence as listed in Table 7.2-1 with one set of temperature measurements per loop. The setpoint for this trip is continuously calculated by analog circuitry for each loop. The equation for calculation of this setpoint is given in Technical Specification 3.3.1. Lead/lag compensation setpoints are calibrated periodically in accordance with Technical Specification 3.3.1.

A separate long ion chamber unit supplies the flux signal for each overtemperature $\Delta T$ trip channel.

Increases in neutron flux difference between the upper and lower ion chambers beyond a predefined deadband result in a decrease in trip setpoint.

The required pressurizer pressure parameters are 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 Subsection 7.2.2.3.3 for an analysis of this arrangement.

Drawings 108D685 show the logic for overtemperature $\Delta T$ trip function.

2. Overpower $\Delta T$ trip

This trip protects against excessive power (fuel rod rating protection) and trips the reactor on coincidence as listed in Table 7.2-1, with one set of temperature measurements per loop. The setpoint for each channel is continuously calculated. The equation for calculation of this setpoint is given in the Technical Specification 3.3.1. Lead/lag compensation setpoints are calibrated periodically in accordance with Technical Specification 3.3.1.

The source of temperature and flux information is identical to that of the overtemperature $\Delta T$ trip and the resultant $\Delta T$ setpoint is compared to the same $\Delta T$. Drawings 108D685 show the logic for this trip function.

c. Reactor coolant system pressurizer pressure and water level trips

The specific trip functions generated are as follows:

1. 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 the 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 7.2-1.

The trip logic is shown on Drawing 108D685, Sheet 6.

In the event that any power-operated relief valve (PORV) opens due to a failure in any pressure channel associated with normal PORV operation, the 2185 psig PORV interlock is provided to close the PORV as pressure decreases below the interlock pressure setpoint. The pressure signal associated with the interlock originates in the pressurizer pressure instrumentation. This signal and interlock operate completely independent of the cold overpressure pressure control signal, which originates in the wide range pressure instrumentation in the RCS loops. This independence of operation is illustrated in Drawing 108D685, Sheet 11, which shows the signals to be "OR"ed for operating the PORV. No interlock disabling system is required.

2. Pressurizer high-pressure trip

The purpose of this trip is to protect the reactor coolant system against system overpressure.

The same sensors and transmitters which are 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 uncompensated pressurizer pressure signals exceed preset limits on coincidence as listed in Table 7.2-1. There are no interlocks or permissives associated with this trip function.

The logic for this trip is shown on Drawing 108D685, Sheet 6.

3. 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 pressurizer high water level signals are given in Table 7.2-1.

The trip logic for this function is shown in Drawing 108D685, Sheet 6.

d. Reactor coolant system low flow trips

These trips protect the core from DNB in the event of a loss of coolant flow situation. Drawing 108D685, Sheet 5 shows the logic for these trips. The means of sensing the loss of coolant flow are as follows:

1. Low reactor coolant flow

The parameter sensed is reactor coolant flow. Three low-pressure elbow taps and one high-pressure tap in each coolant loop are used to drive three flow devices that indicate the status of reactor coolant flow. The basic function 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. Below P-7, the low reactor coolant flow trip function is blocked. Above P-7 but below P-8, the trip occurs on low flow in two out of four loops. Above P-8, the trip occurs on low flow in any loop.

The coincidence logic and interlocks are given in Table 7.2-1.

2. 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 bus (e.g., from plant loss of nonemergency a-c power).

   There are two undervoltage sensing relays (one for Train A and one for Train B) in each 6900-V switchgear bus with each bus feeding a reactor coolant pump motor. These relays provide a time delayed output signal when the pump voltage stays below approximately 70% of rated voltage. The undervoltage relay contacts are employed as inputs to the reactor protection system cabinets, where the signals are processed, conditioned, and connected so as to provide two (two out of four) redundant logic trains. The two redundant logic trains will then initiate the required actions as shown on the Westinghouse functional logic diagram, Drawing 108D685, Sheet 5. The coincidence logic and interlocks are given in Table 7.2-1.

   The undervoltage relays are periodically tested (to verify relay operation) during station shutdowns in accordance with the manufacturer's (Westinghouse) recommendations. The circuitry associated with the Westinghouse Reactor Protection logic has complete on-line testability to verify its integrity.

3. 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 coolant pump breakers for an underfrequency condition greater than that specified in TRM 2.0.a. The setpoint of the underfrequency relays is adjustable.

   There are two underfrequency sensing relays (one for Train A and one for Train B) in each 6900-V switchgear bus with each bus feeding a reactor coolant pump motor. The underfrequency relay contacts are employed as inputs to the reactor protection system cabinets, where the signals are processed, conditioned, and connected so as to provide two (two out of four) redundant logic trains.

The two redundant logic trains will then initiate the required actions as shown on the Westinghouse functional

logic diagram, Drawing 108D685, Sheet 5. The trip of any two relays of the same train (time delayed up to approximately 0.1 second to prevent spurious trips caused by short-term frequency perturbations) will trip the reactor if the power level is above P-7.

The underfrequency relays are periodically tested (to verify relay operation) during station shutdowns in accordance with the manufacturer's (Westinghouse) recommendations. The circuitry associated with the Westinghouse Reactor Protection logic has complete on-line testability to verify its integrity.

4. Reactor coolant pump breaker trip

Opening of two of four reactor coolant pump breakers will also cause a reactor trip if the power level is above P-7.

e. Low-low steam generator water level trip

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

The logic is shown on Drawing 108D685, Sheet 7.

f. Reactor trip on a turbine trip (anticipatory)

The reactor trip on a turbine trip is actuated by two-out-of-three logic from emergency trip fluid pressure signals or by all closed signals from the turbine steam stop valves. A turbine trip causes a direct reactor trip above P-8. The reactor trip on turbine trip provides additional protection and conservatism. No credit is taken in any of the safety analyses (Chapter 15.0) for this trip.

The turbine provides trips to the reactor protection system from contacts which change position when the turbine stop valves close or when the turbine emergency trip fluid pressure goes below its setpoint.

One of the design bases considered in the protection system is the possibility of an earthquake. With respect to these contacts, their functioning is unrelated to a seismic event in that they are

anticipatory to other diverse parameters which cause reactor trip. The contacts are shut during plant operation and open to cause reactor trip when the turbine is tripped. No power is provided to the protection system from the contacts; they merely serve to interrupt power from the protection system to cause reactor trip. This design functions in a deenergize-to-trip fashion to cause a plant trip if power is interrupted in the trip circuitry. This ensures that the protection system will in no way be degraded by this anticipatory trip because seismic design consideration do not form part of the design bases for anticipatory trip sensors. The reactor protection system cabinets which receive the inputs from the anticipatory trip sensors are seismically qualified as discussed in Section 3.10. Therefore, the anticipatory trips meet IEEE 279-1971, including redundancy, separation, single failure, etc.

The logic for this trip is shown on Drawing 108D685, Sheet 16.

g. 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.

Drawing 108D685, Sheet 8 shows the logic for this trip.

h. Manual trip

The manual trip consists of two switches with two outputs on each switch. One output is used to actuate the Train A trip breaker, the other output actuates the Train B trip breaker. Normally closed contacts of redundant manual trip switches are connected to the undervoltage circuits in the solid state protection system (SSPS) and normally open contacts to the shunt coil in the reactor trip switchgear. Switch operation opens (deenergizes) the undervoltage coil in the breaker through the SSPS and simultaneously closes (energizes) the shunt coil directly. Either or both of these circuits will trip open both Train A and Train B breakers holding rod power. No single failure in the switches, SSPS, switchgear, or associated wiring can prevent manual tripping of the reactor. The circuits are implemented in the most direct way and are functionally diverse.

There are no interlocks which can block this trip. Drawing 108D685, Sheet 3 shows the manual trip logic. The design conforms to requirements for manual initiation of protective actions as shown in Drawings 108D685.

In order to maintain separation between wiring associated with different trains, mutually redundant safety train wiring is not terminated on a single device. Backup manual actuation switches link the separate trains by mechanical means to provide greater reliability of operator action for the manual reactor trip function and manual Engineered Safety Features actuations. The linked switches are themselves redundant so that operation of either set of linked switches will actuate safety trains A and B simultaneously. This is shown in Figure 7.2-2. The design of the manual reactor trip function and manual ESF actuations comply with Regulatory Guide 1.62.

7.2.1.1.3 Reactor Trip System Interlocks

a. Power escalation permissives

The overpower protection is provided by the out of core nuclear instrumentation. It 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.

At Braidwood, one of two intermediate range permissive signal (P-6) is required prior to source range trip blocking and detector high voltage cutoff. Source range trips are automatically reactivated and high voltage restored 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 and detector high voltage when between the permissive P-6 and P-10 setpoints, if required. Source range level trip block and high voltage cutoff are always maintained when above the permissive P-10 setpoint.

At Byron, a one 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 Drawing 108D685, Sheet 4. All of the permissive signals are digital; they are derived in bistables from analog signals in the nuclear power range and intermediate range channels.

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

b. Blocks of reactor trips at low power

Interlock P-7 blocks a reactor trip at low power (below approximately 10% of full power) on a low reactor coolant flow in more than one loop, reactor coolant pump breakers open in more than one loop, reactor coolant pump bus undervoltage, underfrequency, pressurizer low pressure, or pressurizer high water level. See Drawing 108D685, Sheets 5, 6, and 16 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 Drawing 108D685, Sheets 4 and 16 for the derivation of P-7.

The P-8 interlock blocks a reactor trip when the plant is below approximately 30% of full power, on a low reactor coolant flow in any one loop or turbine trip. 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 will be allowed to operate with one inactive loop and trip will not occur until two loops are indicating low flow. See Drawing 108D685, Sheet 4 for derivation of P-8, and Sheet 5 for applicable logic.

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

7.2.1.1.4 Coolant Temperature Sensor Arrangement

The hot and cold leg narrow-range, fast-response resistance temperature detectors (RTDs) are mounted in thermowells. A major benefit in using thermowell-mounted RTDs is that a faulty RTD may be replaced without breaching the reactor coolant system pressure boundary.

The temperature of the coolant from the reactor core is not uniform across the pipe cross section (coolant temperature streaming). Therefore, three scoops are installed in a cross-sectional plane of each hot leg at approximately 120° intervals. The scoops are located upstream of the steam generators and extend several inches into the hot leg coolant stream. Each scoop contains five inlet orifices distributed along its length and one discharge opening, located in the bottom of the scoop. In this way, a total of fifteen locations in the hot leg stream are sampled, providing a representative coolant temperature. The hot leg thermowell-mounted RTDs are positioned in the scoops to provide an average temperature reading for each scoop (the thermowell positioned so that the tip of the RTD is adjacent to the third orifice). The discharge opening at the end of each hot leg scoop serves to facilitate flow past the thermowell.

The cold leg reactor coolant flow is well mixed by the reactor coolant pump, thereby eliminating any cold leg coolant temperature streaming. Therefore, for each coolant loop, the cold leg temperature is measured by a single thermowell-mounted RTD located downstream of the pump discharge. Each cold leg thermowell extends approximately 3.3 inches into the flow stream.

#### 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 physicochemical 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 higher 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% of full power. At Byron, source and intermediate range use fission chamber neutron detectors. The power range channels are capable of recording overpower excursions up to 200% 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 six decades of leakage neutron flux. The lowest observed count rate depends on the strength of the neutron sources in the core and the core multiplication associated with the shutdown reactivity. This is generally greater than two counts per second. The next range ("intermediate" range) covers eight 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. Startup-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 takes binary inputs (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 undervoltage trip attachment and shunt trip auxiliary relay coils of the reactor trip circuit breakers when the necessary combination of signals occur. The system also provides annunciator, status light and computer 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.

7.2.1.1.8 Isolation Amplifiers

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

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

7.2.1.1.9 Energy Supply and Environmental Variations

The energy supply for the reactor trip system, including the voltage and frequency variations, is described in Section 7.6 and Chapter 8.0. The environmental variations, throughout which the system will perform, are given in Section 3.11 and Chapter 8.0.

7.2.1.1.10 Setpoints

The setpoints that require trip action are given in TRM 2.0.a. A detailed discussion on setpoints is found in Subsection 7.1.2.1.9.

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 Basis Information

The information given below presents the design basis information requested by Section 3 of IEEE Standard 279-1971. Functional logic diagrams are presented in Drawings 108D685.

7.2.1.2.1 Unit Conditions

The following are the unit conditions requiring reactor trip.

a. DNBR approaching limit.

b. Power density (kilowatts per foot) approaching rated value for Condition II faults (see Chapter 4.0 for fuel design limits).

c. Reactor coolant system overpressure creating stresses approaching the limits specified in Chapter 5.0.

7.2.1.2.2 Unit Variables

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

a. Neutron flux;

b. Reactor coolant temperature;

c. Pressurizer pressure;

d. Pressurizer water level;

e. Reactor coolant flow;

f. Reactor coolant pump operational status (voltage, frequency, and breaker position);

g. Steam generator water level; and

h. Turbine-generator operational status (trip fluid pressure and stop valve position).

7.2.1.2.3 Spatially Dependent Variables

The following variables are spatially dependent:

a. Reactor coolant temperature, and

b. Neutron flux.

7.2.1.2.4 Limits, Margins, and Setpoints

The parameter values that will require reactor trip are given in the Technical Specification and the TRM, and in Chapter 15.0, Accident Analyses. Chapter 15.0 shows that the setpoints used in the Technical Specifications 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 cladding damage and loss of integrity of the reactor coolant system as a result of any ANS Condition II incident (anticipated malfunction). As such, during any ANS Condition II incident, the reactor trip system limits the following parameters:

a. minimum DNBR,

b. maximum system pressure, and

c. fuel rod maximum lineal power for determination of protection setpoints.

The accident analyses as listed in Chapter 15.0 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 15.0-5). A discussion of the safety limits associated with the reactor core and reactor coolant system, plus the allowable values (limiting values), 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:

a. Earthquakes (see Chapters 2.0 and 3.0),

b. Fire (see Section 9.5),

c. Explosion (hydrogen buildup inside containment) (see Section 6.2.),

d. Missiles (see Section 3.5),

e. Flood (see Chapters 2.0 and 3.0), and

f. Wind and Tornadoes (see Section 3.3).

The reactor trip system fulfills the requirements of IEEE Standard 279-1971 to provide automatic protection and to provide initiating signals to mitigate the consequences of faulted conditions. The reactor trip system has been protected against destruction from fires, explosions, floods, wind, and tornadoes (see each item above).

7.2.1.2.6 Minimum Performance Requirements

a. Reactor trip system response times

Reactor trip system response time is defined in Section 7.1. Typical time delays in generating the reactor trip signal are tabulated in Table 7.2-3. See Subsection 7.1.2.19 for a discussion of periodic response time verification capabilities. Maximum allowable reactor trip system response times shall be as shown in Table 7.2-19. No credit was taken in the safety analyses for those channels with response times indicated as "N.A.", not applicable.

b. Reactor trip accuracies

Accuracy is defined in Section 7.1. Reactor trip accuracies are tabulated in Table 7.2-3. An additional discussion on accuracy is found in Subsection 7.1.2.1.9.

c. Protection system ranges

Typical protection system ranges are tabulated in Table 7.2-3. 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 System Drawings

Functional block diagrams, electrical elementaries, and other drawings required to assure electrical separation and perform a safety review were provided in the safety-related drawing package (see Section 1.7 of the FSAR).

## 7.2.2 Analysis

### 7.2.2.1 Failure Mode and Effects Analyses

An analysis of the reactor trip system has been performed. Results of this study and a fault tree analysis are presented in Reference 4. Reference 4 is not specifically presented in the format of a failure mode and effects analysis (FMEA) for

the reactor trip. However, credit is taken for Reference 4 as fulfilling the purpose of an FMEA for the reactor trip. The conditions of a reactor trip FMEA, which considers single random failures, can be shown to be bounded by the Reference 4 conditions, which cover not only single random failures but also systematic failures.

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 $\Delta T$ and overpower $\Delta T$ setpoints. All setpoints in the reactor trip system have been selected on the basis of engineering design of 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 Chapter 15.0. These accident analyses are carried out using those setpoints determined from results of the engineering design studies.

Setpoint limits are presented in the TRM 2.0.a. 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 selection trip setpoints all provide for margin before protection action is actually required to allow for uncertain-ties 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 a DNBR of 1.30 there is likely to be significant local fuel cladding failure. The DNBR existing at any point in the core is a function of inlet temperature, power output, operating pressure and flow. Consequently, core safety limits in terms of a DNBR equal to 1.30 for the hot channel can be developed as a function of core $\Delta T$, $T_{avg}$ and pressure for a specified flow as illustrated by the solid lines in Figure 15.0-1. Also shown as solid lines in Figure 15.0-1 are the loci of conditions equivalent to 118% of power as a function of $\Delta T$ and $T_{avg}$ representing the overpower (kW/ft) limit on the fuel. The dashed lines indicate the maximum permissible setpoint ($\Delta T$) as a function of $T_{avg}$ and pressure for the overtemperature and overpower reactor trip. Actual setpoint constants in the equation representing the dashed lines are as given in Technical Specification 3.3.1. 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 overtemperature 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 $\Delta T$ 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 $\Delta T$ 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 7.2-4 which lists the various trips of the reactor trip system, the corresponding Technical Specification on safety limits, 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 nonstandard 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 the DNB ratios less than 1.30 will not be realized during any Condition II transients occurring during 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 $\Delta T$ function to more restrictive values as listed in the Technical Specifications, the P-8 setpoint can be increased to the maximum value consistent with maintaining DNBR above 1.30 for Condition II transients in the one-loop shutdown mode. The resetting of the $\Delta T$ 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 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 Chapter 15.0. 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 elbow taps used on 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 elbow tap signal is given by the following Equation:

$$(\Delta P/\Delta P_{\circ}) = (w/w_{\circ})^{2}, \qquad (7.2\text{-}1)$$

where $\Delta P_{\circ}$ is the pressure differential at the reference flow $w_{\circ}$, and $\Delta P$ is the pressure differential at the corresponding flow, w. The full flow reference point is established by extrapolating along the correlation curve. The expected absolute accuracy of the channel is within ±10% of full flow and field results have shown the repeatability of the trip point to be within ± 1%.

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 Standard 279-1971, as indicated below.

a. General functional requirement

   The protection system automatically initiates appropriate protective action whenever a condition monitored by the system reaches a preset value. Functional performance requirements are given in Subsection 7.2.1.1.1. Subsection 7.2.1.2.4 presents a discussion of limits, margins and setpoints; Subsection 7.2.1.2.5 discusses unusual

(abnormal) events; and Subsection 7.2.1.2.6 presents minimum performance requirements.

b. 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.

c. 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 17.0. The quality assurance applied conforms to Criterion 1 of the 1971 GDC.

d. 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.

e. Channel integrity

Protection system channels are required to operate in accident conditions, maintain necessary functional capability under extremes of conditions relating to environment, power supply, malfunctions, and accidents. The power supply for the reactor trip system is described in Section 7.6 and Chapter 8.0. The environmental variations, in which the system will perform are given in Section 3.11.

f. 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 a-c 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 7.1-1.)

The design philosophy is to make 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.

g. Control and protection system interaction

The protection system is designed to be independent of the control system. In certain applications the control signals and other nonprotective functions are derived from individual protective channels through isolation 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 nonprotective 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 Standard 279-1971.

The results of applying various malfunction conditions on the output portion of the isolation amplifiers show that no significant disturbance to the isolation amplifier input signal occurred.

h. Derivation of system inputs

To the extent feasible and practical, protection system inputs are derived from signals which are direct measures of the desired variable. Variables monitored for the various reactor trips are listed in Subsection 7.2.1.2.2.

i. 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 the Technical Specifications.

j. 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 ensure complete system operation. The testing capabilities are in conformance with requirements for periodic testing of protection system actuation functions as discussed in Subsection 7.1.2.6.

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 ability to test the analog system in bypass and 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.

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 test by a test switch which, when thrown, deenergizes 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 removed 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 analog system also has test in bypass capability which through an additional test switch maintains the associated logic input and prevents the actuation of the logic (partial trip). The bypass capability is designed so that credible failures (e.g. relays) will not result in a function being automatically placed in a bypassed condition. A local status light, main control room annunciator, and Sequence of Events Recorder message are provided to indicate a bypassed condition.

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

1. $T_{avg}$ and $\Delta T$ protection channel testing;

2. pressurizer pressure protection channel testing;

3. pressurizer water level protection channel testing;

4. steam generator water level protection channel testing;

5. reactor coolant low flow, underfrequency, and undervoltage protection channels;

6. impulse chamber pressure channel testing;

7. steam pressure protection channels; and

8. containment pressure.

Nuclear Instrumentation Channel Tests

The power range channels of the nuclear instrumentation system can be 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 bistables are not placed into a tripped condition prior to testing in this condition since that action would preclude testing. Allowing the bistables to remain in their normal state is acceptable because superposition of the test signal onto the existing signal cannot result in a nonconservative effect on the trip setpoints; therefore, channel logic remains in a two-out-of-four coincidence. 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 without placing the channel into a condition in which it must be declared inoperable.

Testing and calibrating a power range channel may be accomplished by placing the channel in an inoperable status. This is done to allow more precise determination of the actual bistable setpoints than is possible with an existing variable signal from the detector. With a channel in bypassed status, the channel logic becomes two-out-of-three, since the bypassed channel will no longer respond to actual reactor flux. If the channel must be maintained as bypassed for an unacceptable time period, its output bistables must be placed in a tripped condition to reduce the channel logic to one-out-of-three.

This page has been intentionally deleted.

For the purpose of testing or calibrating protection channels, a power range channel may be bypassed temporarily. The channel's output bistables may remain in an untripped state, within an acceptable time period, to calibrate or test the channel.

These channels are provided with a bypass function to prevent initiation of an undesired action from the system function during the period that one channel is in test. When the bypass test capability is used, the logic circultry will not be actuated and bistable operation will be indicated locally.

One channel may be bypassed to support surveillance testing and setpoint adjustments as allowed by Technical Specifications.

To permit testing in the bypass condition, a test panel is provided on each of the four NIS protection sets. Use of administrative controls will ensure that not more than one channel will be bypassed at a time. The bypass capability is designed so that credible failures (e.g. relays) will not result in a function being automatically placed in a bypassed condition. Annunciators and Sequence of Events Recorder message in the main control room and bypass status lights on the bypass test panels are provided to indicate the bypassed condition.

A "TEST OPERATE" switch is provided such that deliberate operator action is required to test a power range channel. Operation of this switch initiates the "CHANNEL TEST" annunciator in the control room. If the bypass test capability is not used, bistable operation is tested in all channel operability conditions by increasing the provided test signal until the channel output reaches its trip setpoint and by verifying bistable relay operation by control board annunciator and trip status lights.

A nuclear instrumentation system channel which can cause a reactor trip through one of two protection logic (source or intermediate range) is provided with a bypass function which prevents the initiation of a reactor trip from that particular channel during the short period that it is undergoing a test.

The following periodic tests of the nuclear instrumentation system are performed:

1. testing at plant shutdown

   a) source range testing,

   b) intermediate range testing, and

   c) power range testing.

2. Testing between P-6 and P-10 permissive power levels

   a) source range testing and

   b) power range testing.

3. Testing above P-10 permissive power level

   a) power range testing.

Any deviations noted during the performance of these tests are investigated and corrected in accordance with established procedures.

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 panels. 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 nontrip logic. Trip logic is not maintained sufficiently long enough to permit opening of the reactor trip breakers. The reactor trip undervoltage trip attachment and shunt trip auxiliary relay 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 on the reactor coolant pump buses is provided as discussed in Subsection 7.2.1 and shown on Drawings 108D685. The logic for these trips is capable of being tested during power operation. When parts of the trip are being tested, the sequence is such that an overlap is provided between parts so that a complete logic test is provided.

This design complies with the testing requirements of IEEE Standard 279-1971 and 338-1987 discussed in Subsection 7.1.2.19.

The permissive and block interlocks associated with the reactor trip system and engineered safety features actuation system are given on Tables 7.2-2 and 7.3-3 and designated protection or "P" interlocks. As a part of the protection system, these interlocks are designed to meet the testing requirements of IEEE Standard 279-1971 and 338-1987.

The reactor trip switchgear, where certain safety interlocks originate, and protection instrumentation systems are periodically tested was found to have the P-4 interlock for safety injection block/reset to be nontested on a system basis and was reported to the NRC by Westinghouse under 10

CFR 50.55(e) and Part 21. The recommended corrective action includes specific testing requirements for all Westinghouse plants for this interlock.

Assessment of the adequacy of protection system interlock testing has been completed. The need for new, revised, or additional procedures were established as required.

Testing of the protection system interlocks is provided by the logic testing and semiautomatic testing capabilities of the solid-state protection system. In the solid-state protection system the undervoltage trip attachment and shunt trip auxiliary relay 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 (two-out-of-four loops showing two-out-of-three low flow) is tested to verify operability of the trip above P-7 and non-trip below P-7. (See Drawing 108D685, Sheet 5.) 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:

1. 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 deenergize. 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 that input relays in both

trains have been deenergized. A flashing lamp means that the input relays in the two trains did not both deenergize. 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 testing of those systems supplying the inputs to the logic protection system. Test indications are status lamps and annunciators on the control board. Inputs to the logic protection system are checked one channel at a time, leaving the other channels in service. For example, when testing with the channel bistable in a trip mode, 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. When testing in the bypass mode, a function that trips the reactor when two out of four channels trip becomes a two-out–of–three trip when one channel is bypassed. The input relay operation may still be verified by momentarily placing the channel in a trip condition during routine surveillance testing. If the channel is not placed in a trip condition during on-line surveillance, then the input relay operation will be verified in accordance with the Surveillance Frequency Control Program. Both trains of logic protection system remain in service during this portion of the test.

2. Check of logic matrices

Logic matrices are checked one train at a time. Input relays are not operated during this portion of the test. Reactor trips from the train being tested are inhibited with the use of the input error inhibit switch on the semiautomatic test panel in the train. At the completion of the logic matrix tests, one bistable in each channel of process instrumentation or nuclear instrumentation is 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 nontrip 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 trip attachment and shunt trip auxiliary relay coils to the tester. The pulses are of such short duration that the reactor trip breaker undervoltage coil armature cannot respond mechanically.

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

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 of the conditions exist in both trains at the same time, the general warning alarm circuits will automatically trip the reactor.

a. Loss of either of two 48-Vdc or either of two 15-Vdc 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. Train bypass breaker 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:

1. rack in and close 52/BYA-manually trip 52/RTA through a protection system logic matrix by operation of the automatic shunt trip "trip" pushbutton on the automatic shunt trip panel. This verifies operation of the shunt trip auxiliary relay when the breaker trips. After reclosing RTA, it trips again through a protection system logic matrix while at the same time operating the automatic shunt trip "block" pushbutton on the automatic shunt trip panel. This verifies operation of the undervoltage trip attachment (UVTA) when the breaker trips;

2. reset 52/RTA;

3. trip and rack out 52/BYA; and

4. repeat above steps to test trip breaker 52/RTB using bypass breaker 52/BYB.

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. Therefore, the minimum number of operable channels has been formulated in Technical Specification 3.3.1 to permit on-line testing of the various protection channels or to permit continued operation in the event of a subsystem instrumentation channel failure. This Technical Specification also defines the required restriction to operation in the event that the channel operability requirements cannot be met.

k. 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 ability to test the analog system in bypass and the coincidence logic required for reactor trip. Additional information is given in Subsection 7.2.2.2.3j.

l. 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.

m. Indication of bypasses

Bypass indication is discussed in Subsection 7.1.2.10.

n. Access to means for bypassing

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

o. Multiple setpoints

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

p. 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.

q. 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 using a diverse method; i.e., energizing a shunt trip coil.

r. Access

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

s. Identification of protective actions

Protective channel identification is discussed in Subsection 7.1.2.3. Indication is discussed in Item t below.

t. Information readout

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 sum 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.

u. 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 j 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 auctioneered high signal is derived by auctioneering of the four channels 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 Coolant Temperature

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

bypass loop resistance temperature detector signals were compared with the core exit thermocouple signals. The bypass loop piping has since been removed. The bypass loop piping used direct immersion single-element RTDs, which were mounted in manifolds. The bypass loop has been replaced by thermowell-mounted, dual element, fast response RTDs, which extend into the reactor coolant loop. The hot leg scoops have been modified to accept new thermowells. The RTDs were placed in each of the three existing hot leg scoops and in the cold leg penetration of each loop. The three hot leg temperature signals are electronically averaged in the reactor protection system (RPS) to produce a representative hot leg temperature. The spare RTD element is wired to the 7300 process protection cabinets to facilitate switching to the spare element at the racks in the event of a failure of the active element.

To assess whether the new method of obtaining hot leg temperature yields results consistent with the RTD bypass manifold system, the $\Delta T$ readings of each loop are compared (normalized to full power) before and after installation of the modification. Any unexpected differences or anomalies are evaluated and addressed. The impact of this new method of obtaining a representative $T_{avg}$ signal is not expected to affect control systems that rely on $T_{avg}$ as an input signal because these control systems receive their inputs after the RCS temperature signal has been processed.

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 average temperature of the loop with the highest temperature, the control rods are always moved based upon the most pessimistic temperature measurement with respect to margins to DNB. A spurious low average temperature measurement from any loop temperature control channel will cause no control action. A spurious high average temperature measurement will cause rod insertion (safe direction).

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

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 $\Delta T$ trip protection function. Isolated output signals from these channels are used for pressure control. These are used to control pressurizer spray and heaters and power-operated relief valves. Pressurizer pressure is sensed by fast response pressure transmitters.

A spurious high-pressure signal from one channel can cause decreasing pressure by actuation of either spray or relief valves. Protection from inadvertent spray valve or relief valve operation is provided by the low pressurizer pressure reactor trip and by 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%. 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 shared tap is plugged, the affected channels will remain static. If the impulse line bursts, the indicated pressure will drop to zero. In either case the fault is easily detectable, and the protective function remains operable.

7.2.2.3.4 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. A failure in the level control system could fill or empty the pressurizer at a slow rate (on the order of 1/2 hour or more).

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.

7.2.2.3.5 Steam Generator Water Level

Steam generator narrow range water level instrumentation is a safety grade system designed to actuate a reactor trip due to a

loss of heat sink. A reactor trip is generated on two-out-of-four low-low level signals in any steam generator. The logic diagram is shown in Drawing 108D685, Sheet 7.

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.

A spurious low signal from the feedwater flow channel being used for control would cause an increase in feedwater flow. The mismatch between steam flow and feedwater flow produced by the spurious signal would actuate alarms to alert the operator of the situation in time for manual correction. If the condition continues, a two-out-of-four high-high steam generator water level signal in any loop, independent of the indicated feedwater flow, will cause feedwater isolation and trip the turbine. The turbine trip will result in a subsequent reactor trip if power is above the P-8 setpoint. 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 effect at all. A spurious low or high steam flow signal would have the same effect as high or low feedwater signal, discussed above.

A spurious high steam generator water level signal from the protection channel used for control will tend to close the feedwater valve. However, before a reactor trip would occur, two-out-of-four channels for a steam generator would have to indicate a high water level. A spurious low steam generator

water level signal will tend to open the feedwater valve. Again, 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.

7.2.2.3.6 Main Steamline Pressure Instrumentation

The main steamline pressure instrumentation senses pressure for actuated engineered safety features in the event of a secondary high energy line break. This function is discussed in Subsection 7.3.2.4.2. Drawing 108D685, Sheet 7, includes the functional logic diagram showing initiation of safety injection and steamline isolation from steamline pressure instruments.

7.2.2.3.7 Effect of an Adverse Environment on Four Reactor Protection Control Systems

Westinghouse identified four systems which, if subjected to an adverse environment, could potentially lead to control system faulty operation which may impact protective functions. These four systems have been investigated and it has been concluded that the proposed accident sequences are either not applicable to Byron/Braidwood or would not result in a more limiting event than those presented in the plant Safety Analysis Report. Each potential problem is discussed in the following.

Automatic Rod Control System

The potential problem is a failure in the excore neutron detectors or associated cabling resulting in inaccurate detector output in the low direction causing an automatic rod withdrawal accident coincident with a steamline break.

The excore detectors are not required once the reactor has tripped. Prior to reactor trip, several factors tend to decrease the possibility of a significant consequential malfunction of the automatic rod control system due to a steamline break inside containment. The physical location of the excore detectors relative to the postulated break location does not provide direct access for steam to travel to the excore detectors. The detectors are located in an annulus around the reactor vessel separated by a concrete barrier from the other primary components and piping.

As stated in Subsection 7.2.2.3.1, an isolated auctioneered high signal is derived by auctioneering of the four channels for automatic rod control. That is, rod withdrawal is based on the highest of the four excore detectors. Therefore, rod withdrawal will occur only if all four excore detectors fail low. For these reasons it is unlikely that rod withdrawal will result from environmental failure of the excore detectors prior to reactor trip.

Based on the low probability of the occurrence of a consequential malfunction of the rod control system, we do not believe this scenario represents a significant safety question.

Main Feedwater Control System

The postulated problem is a malfunction of the main feedwater control system due to an adverse environment following a break of a small feedwater line. If an assumption is made that this malfunction causes the feedwater control valves to close in both the damaged loop and the intact loops, liquid level in the intact steam generators could be affected.

The feedwater flow control devices under question are the feedwater flow elements and associated transmitters which are located outside containment in the steam tunnel as it opens to the turbine building, some 100 feet from the nearest break location. The steam generator level and steam flow transmitters are located inside containment, but outside the missile barrier and physically separated for each loop. Because of the small size of the postulated break, and the physical separation of each device from the proximity of the break, it is unlikely that the environment around the devices could cause failure, particularly simultaneous failure, in all four loops. For this reason, it is not believed that this scenario represents a significant safety question that requires further action.

Pressurizer PORV Control System

The potential problem is that the adverse environment resulting from a feedwater line break may affect the pressurizer PORV control system. If this system malfunctions such that the PORV fails in the open position, an additional breach of the reactor coolant system boundary will have occurred.

As part of the following efforts of the TMI-2 accident, Westinghouse has analyzed this class of accidents (for the Westinghouse TMI Owners' Group) and reported the results in WCAP-9600. In the analysis of Section 4.2 of the WCAP-9600, the complete loss of feedwater (main and auxiliary) was assumed to determine the time when operator action would be required to prevent uncovering of the core.

The results of the analyses presented in WCAP-9600, Section 4.2, which illustrates that the operator is not required to take corrective action to open the pressurizer PORVs for at least 2,500 seconds following the loss of feedwater to achieve adequate core inventory also applies to this scenario. Conservatively assuming that all liquid inventory in the steam generator associated with the feedline break is lost via the break without removing any heat, the loss of heat sink due to the liquid inventory blowdown of the faulted steam generator is more than counterbalanced by the auxiliary feedwater being injected into the intact steam generators following reactor trip. Hence, the conclusions reported in WCAP-9600 are conservative with respect to the possibility of one or both pressurizer PORVs stuck open due to a consequential malfunction of the PORV control system.

The auxiliary feedwater system is provided with sufficient flow restriction in each line to each steam generator such that one pump (single failure) can deliver the minimum required flow to each of the three unfaulted steam generators within 1 minute following an accident in order to mitigate the feedwater line break transient (subsection 15.2.8). Operator action is assumed not to be required for at least 30 minutes following the accident.

The feedwater system pipe break analysis concludes that the auxiliary feedwater system capacity is adequate to remove decay heat, prevent overpressurization of the reactor coolant system, and prevent uncovering of the core.

Also, the PORVs and their control components are located far away from postulated feedline break and the PORVs (fail close valves) are shielded from feedwater lines by a carrier barrier. The PORVs are qualified for the environment in which they are required to operate.

The consequences of feedline break with the consequential failure of the PORV control system are bounded by the analyses in Section 4.2 of WCAP-9600 and the feedline break analysis.

Steam Generator PORV Control System

The potential problem is that the adverse environment following a feedwater line break may result in a failure of the PORV control system. This failure would lead to depressurization of the steam generators which supply steam to turbine-driven auxiliary feedwater pumps reducing the capability of the turbine-driven pumps to supply feedwater to the steam generators in the intact loops.

Motor-driven and diesel-driven pumps are used for the auxiliary feedwater system rather than turbine-driven pumps. Hence, loss of steam supply is inconsequential to auxiliary feedwater system operation, and this concern is not applicable .

Westinghouse has analyzed, on a generic basis, a multiple steam generator blowdown for a full double-ended steam line break. The results of this generic analysis showed that there was little change in the minimum calculated DNBR from that of the UFSAR case. (The minimum DNBR was slightly higher for the case where two steam generators blew down for the duration of the transient.) In a multiple steam generator blowdown, cooler RCS temperatures in the presence of a negative moderator coefficient will result in a higher return to power than the UFSAR case. This is a penalty in DNBR. However, because two steam generators are blowing down, a more uniform cooling effect is seen across the core. This means a less adverse power shape (benefit in radial peaking factor in the region of the stuck rod). The conclusion reached from the generic analysis is that there is an even trade-off between the penalty for higher return to power and the benefit in power peaking factor in the region of the stuck rod for a multiple steam generator blowdown transient.

The generic analysis is applicable for two steam generator blowdown through break sizes up to a full-double ended break. For the multiple steam generator blowdown in question, the loop with the break will blow down through an effective area of 1.4 $ft^2$ (integral flow restrictor) and the second steam generator will blowdown through a break area of much less than 1.1 $ft^2$ for Unit 1 and 1.4 $ft^2$ for Unit 2 (orifice size of PORV). This case is, therefore, covered by the generic analysis, i.e., the main steamline break is more limiting than the multiple steam generator blowdown case postulated.

7.2.2.4 Additional Postulated Accidents

Loss of plant instrument air or loss of component cooling water is discussed in Subsection 7.3.2. Load rejection and turbine trip are discussed in further detail in Section 7.7.

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 Subsection 7.7.1.4.1 and listed in Table 7.7-1. Excessively high power operation (which is prevented by blocking of automatic rod withdrawal), if allowed to continue, might lead to a safety limit (as given in Technical Specification 2.1) being reached. Before such a limit is reached, protection will be available from the reactor trip system. At the power level 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 systems, and are considered as control systems.

Failures which affect the major components of the NSSS control system have been analyzed. In this analysis, it was demonstrated that the resulting event for each failure was within the bounds for accident analyses presented in Chapter 15.0. The individual postulations of failures and accident analyses are presented in the following subsections.

The events considered are:

a. Loss of any single instrument,

b. Break of any single instrument line, and

c. Loss of power to all systems powered by a single power supply system (i.e., single inverter).

The analysis is conducted for all five major NSSS control systems:

1. Reactor control system,

2. Steam dump system,

3. Pressurizer pressure control system,

4. Pressurizer level control system, and

5. Feedwater control system.

The initial conditions for the analysis are assumed to be anywhere within full operating power range of the plant (i.e., 0% to 100%) where applicable.

The results of the analysis indicate that, for any of the postulated events considered in items a through c above, the Condition II accident analyses given in Chapter 15.0 are bounding.

7.2.2.4.1 Loss of Any Single Instrument

Table 7.2-5 is a sensor-by-sensor evaluation of the effect on the control systems itemized above caused by a sensor failing either high or low. The particular sensor considered is given, along with the number of channels which exist, the failed channel, the control systems impacted by the sensor, the effects on the control systems for failures in both directions, and the bounding UFSAR accident. Where no control action occurs or where control action is in a safe direction, no bounding accident is given.

The table clearly shows that for any single instrument failure, either high or low, the Condition II events itemized in Chapter 15.0 are bounding.

7.2.2.4.2 Loss of Power to an Inverter, Control Group, or Protection Set

Tables 7.2-6 through 7.2-9 present analyses of the effects on the control systems caused by the loss of power to an instrument distribution panel. The Byron/Braidwood Units 1 and 2 NSSS instrument power supply consists of four instrument distribution panels (1A, 2A, 3A, and 4A) receiving power through four inverters (for convenience called inverters I through IV). Each instrument distribution panel powers a single control group and a single protection set (panel 1A, powered by inverter I, distributes power to control group 1 and protection set I; panel 2A, powered by inverter II, distributes power to control group 2 and protection set II, etc.). Therefore, loss of power to one inverter causes a loss of power to both a protection set and a control group. In the tables, the control systems affected, the sensors affected, the failure direction, the effect on the control systems, and the bounding UFSAR accident are given. Where no control action occurs or where control action is in a safe direction, no bounding accident is given.

Besides the loss of the inverter feeding both a protection set and a control group, there is also a chance of losing power to just a control group or a protection set (for example, through the failure of a fuse or circuit breaker). The consequences of a loss of power to a control group or a protection set are tabulated in Tables 7.2-10 through 7.2-13 for losing protection set I, II, III, or IV, respectively, and on Table 7.2-14 through 7.2-17 for losing control group 1, 2, 3, or 4, respectively. The data is presented in a similar manner to that for the loss of an inverter described in the previous paragraph.

All of the above described inverters, control groups, and protection sets are unique to the NSSS. In addition, two other control related signals are powered by non-safety motor control centers in the BOP power system. The condenser available signals in the steam dump control system are powered by 120-Vdc distribution panel tapped off of one of the motor control centers. The steamline pressure signals used to activate the steam generator atmospheric relief valves are also powered by a distribution panel from a separate motor control center. The steamline pressure signals used to activate the steam generator atmospheric relief valves primary power supply is from a distribution panel fed from an inverter. In the event of a loss of the motor control center for the atmospheric relief valve, automatic switch-over provides backup power from a redundant motor control center. A loss of power to the condenser available signal results in blockage of the steam dump; a loss of power to the steamline pressure signals cause the steam generator relief valves to fail closed. Thus, even in the event of a total loss of power to these control signals, no control actions or bounding events results.

Besides the loss of power to a complete control group or protection set, there is the chance of having an electrical fault on one of the control system circuit cards. The control systems are designed so that each card is used in only one control system. A circuit card failure cannot directly impact more than one control system. A failure on a control card would cause the controller to generate either an "off" or a "full on" output, depending on the type of failure. This result would be similar to having a fault in a sensor feeding the control system. Therefore, the failure of or loss of power in any control system circuit card would be bounded by the loss of any single instrument analysis described in Table 7.2-5.

The tables show that for a loss of power to any inverter, control group, or protection set, the Condition II events analyzed in Chapter 15.0 are bounding.

7.2.2.4.3 Loss of Common Instrument Lines

Table 7.2-18 presents the scenario whereby an instrument line which supplies more than one signal breaks, causing faulty sensor readings.

Two sets of sensors are located in common lines:

a. Loop steam flow (protection sets I and II for any steam generator) and narrow range steam generator level (protection sets I or II, any steam generator) and

b. Pressurizer level (protection sets I, II, or III) and pressurizer pressure (protection sets I, II, III, or IV).

The loop flow transmitters are not shown on the tables since they are not part of the plant control system and are used for

protection only. There are three flow transmitters in each loop with each transmitter having a common high pressure tap but separate and unique low pressure taps. Therefore, a break at the high pressure flow transmitter tap would disable all three flow transmitters in one loop, resulting in a low flow reading for all three transmitters. This break causes a reactor trip if the plant is above the P-8 setpoint, or an annunciation if it is below P-8.

The only malfunction mode explicitly analyzed was a break in the common instrument line at the tap. Another possibility is to have a complete blockage in the sensor tap, causing the sensor to read a constant (before blockage) value. However, this last failure mode is not analyzed since it is really not a credible event. There is no anticipated agent available that would cause a tap blockage. The reactor coolant system piping and fittings and the instrument impulse line tubing are all stainless steel, so no products of corrosion are expected. Also the water chemistry is of high quality, which along with high temperature operation, precludes the presence of solids in the water and assures the maintenance of the solubility of chemicals in the water. In addition, prior to startup and during any shutdown as well, it is routine maintenance and servicing practice for instrument lines to be blown down to a canister. Since the buildup of sludge is a slow process, any buildup would be detected during response time testing done during shutdown. Therefore, the hypothesis of the presence of a complete blockage of the sensor tap is not sufficiently credible to warrant its consideration as a design basis.

In the extremely unlikely event that a complete instrument line blockage were to occur, the condition is detectable because the reading would become static (no variations over time). In an unblocked channel, a reading would always vary somewhat due to noise (i.e., flow induced noise in flow channels) or slight controller action (i.e., cycling operation of spray and heaters in pressurizer). By a comparison of a static channel to the redundant unblocked channels, the operator would be informed that a blockage in one channel has occurred.

### 7.2.3 Tests and Inspections

The reactor trip system meets the testing requirements of IEEE Standard 338-1987, as discussed in Subsection 7.1.2.19. The testability of the system is discussed in Subsection 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 Standard 338-1987, are available for audit by responsible personnel. Periodic testing complies with requirements for periodic testing of protection system actuation functions as discussed in Subsections 7.1.2.13 and 7.2.2.2.3.

7.2.4 References

1. J.B. Reid, "Process Instrumentation for Westinghouse Nuclear Steam Supply Systems," WCAP-7913, January 1973. (Additional background information only.)

2. J.G. Lipchak, "Nuclear Instrumentation System," WCAP-8255, January 1974. (Additional background information only.)

3. D.N. Katz, "Solid State Logic Protection System Description," WCAP-7488-L, March 1971 (Proprietary), and WCAP-7672, May 1971 (Non-Proprietary). (Additional background information only.)

4. W.C. Gangloff, and W.D. Loftus, "An Evaluation of Solid State Logic Reactor Protection In Anticipated Transients," WCAP-7706-L, February 1971 (Proprietary), and WCAP-7706, February 1971 (Non-Proprietary).

TABLE 7.2-1

LIST OF REACTOR TRIPS

| | REACTOR TRIP | COINCIDENCE LOGIC | INTERLOCKS | COMMENTS |
|---|---|---|---|---|
| 1. | a. High neutron flux (power range - low setting) | 2/4 | Manual block of low setting permitted by P-10 | Manual block and automatic reset of low setting by P-10. |
| | b. High neutron flux (power range - high setting) | 2/4 | No interlocks | |
| 2. | Intermediate range neutron flux | 1/2 | Manual block permitted by P-10 | Manual block and automatic reset. |
| 3. | Source range neutron flux | 1/2 | Manual block permitted by P-6, interlocked with P-10 | Manual block and automatic reset. Automatic block above P-10. |
| 4. | Power range high positive neutron flux rate | 2/4 | No interlocks | |
| 5. | | | Intentionally left blank | |
| 6. | Overtemperature $\Delta T$ | 2/4 | No interlocks | |
| 7. | Overpower $\Delta T$ | 2/4 | No interlocks | |
| 8. | Pressurizer low-pressure | 2/4 | Interlocked with P-7 | Blocked below P-7. |

TABLE 7.2-1 (Cont'd)

| | REACTOR TRIP | COINCIDENCE LOGIC | INTERLOCKS | COMMENTS |
|---|---|---|---|---|
| 9. | Pressurizer high-pressure | 2/4 | No interlocks | |
| 10. | Pressurizer high water level | 2/3 | Interlocked with P-7 | Blocked below P-7. |
| 11. | Low reactor coolant flow | 2/3 in any loop | Interlocked with P-7 and P-8 | Low flow in one loop will cause a reactor trip when above P-8 and a low flow in two loops will cause a reactor trip when above P-7. Blocked below P-7. |
| 12. | RCP breakers | 2/4 | Interlocked with P-7 | Two-out-of-four RCP Breakers open will cause a reactor trip when above P-7. Blocked below P-7. |
| 13. | Reactor coolant pump bus undervoltage | 2/4 | Interlocked with P-7 | Low voltage on all buses permitted below P-7. |
| 14. | Reactor coolant pump underfrequency | 2/4 | Interlocked with P-7 | Underfrequency on two motors will trip all reactor coolant pump breakers and cause reactor trip; reactor trip blocked below P-7. |
| 15. | Low-low steam generator water level | 2/4 in any loop | Interlocked with RCIV valves closed | |

TABLE 7.2-1 (Cont'd)

| REACTOR TRIP | COINCIDENCE LOGIC | INTERLOCKS | COMMENTS |
|---|---|---|---|
| 16. Safety injection signal | Coincident with actuation of safety injection | No interlocks | (See Section 7.3 for Engineered Safety Features actuation conditions.) |
| 17. Turbine trip (anticipatory) | | | |
| a. Low trip fluid pressure | 2/3 | Interlocked with P-8 | Blocked below P-8. |
| b. Turbine stop | 4/4 | Interlocked with P-8 | Blocked below P-8. |
| 18. Manual | 1/2 | No interlocks | |

TABLE 7.2-2

PROTECTION SYSTEM INTERLOCKS

| DESIGNATION | DERIVATION | FUNCTION |
|---|---|---|
| | I POWER ESCALATION PERMISSIVES | |
| P-6 | Presence of P-6: 1/2 neutron flux (intermediate range) above setpoint | Allows manual block of source range reactor trip |
| | Absence of P-6: 2/2 neutron flux (intermediate range) below setpoint | Defeats the block of source range reactor trip |
| P-10 | Presence of P-10: 2/4 neutron flux (power range) above setpoint | Allows manual block of power range (low setpoint) reactor trip |
| | | Allows manual block of intermediate range reactor trip and intermediate range rod stops (C-1) |
| | | Blocks source range reactor trip (backup for P-6) |
| | Absence of P-10: 3/4 neutron flux (power range) below setpoint | Defeats the block of power range (low setpoint) reactor trip. |
| | | Defeats the block of intermediate range reactor trip and intermediate range rod stops (C-1). Input to P-7. |

TABLE 7.2-2 (Cont'd)

| DESIGNATION | DERIVATION | FUNCTION |
|---|---|---|
| | II BLOCKS OF REACTOR TRIPS | |
| P-7 | Absence of P-7: 3/4 neutron flux (power range) below setpoint (from P-10) and 2/2 turbine impulse chamber pressure below setpoint (from P-13) | Blocks reactor trip on: Low reactor coolant flow in more than one loop, RCP breaker open in more than one loop, reactor coolant pump bus undervoltage, underfrequency, pressurizer low pressure, and pressurizer high level |
| P-8 | Absence of P-8: 3/4 neutron flux (power range) below setpoint | Blocks reactor trip on: reactor coolant flow in a single loop, or turbine trip |
| P-13 | 2/2 turbine impulse chamber pressure below setpoint | Input to P-7 |

TABLE 7.2-3

REACTOR TRIP SYSTEM INSTRUMENTATION

| REACTOR TRIP SIGNAL | TYPICAL RANGE | TYPICAL TRIP ACCURACY | TYPICAL TIME RESPONSE (sec) |
|---|---|---|---|
| 1. Power range high neutron flux | 1 to 120% full power | 1% of full power | 0.5 |
| 2. Intermediate range high neutron flux | 8 decades of neutron flux overlapping source range by 2 decades | ±5% of full scale<br>±1% of full scale from $10^{-4}$ to $10^{-3}$ amperes (10 to $10^{2}$% RTP at Byron) (1) | 0.2 |
| 3. Source range high neutron flux | 6 decades of neutron flux (1 to $10^{6}$ counts/sec) | ±5% of full scale (1) | 0.2 |
| 4. Power range high positive neutron flux rate | +15% of full power | ±5% (1) | 0.2 |
| 5. | Intentionally left blank | | |
| 6. Overtemperature ΔT: | $T_H$ 530 to 650°F<br>$T_C$ 510 to 630°F<br>$T_{AV}$ 530 to 630°F<br>$P_{PRZR}$ 1700 to 2500 psig<br>F (ΔΦ) -50 to +50<br>ΔT Setpoint 0 to 100°F | ±3.2°F | 8.0 (including transport time) |
| 7. Overpower ΔT | $T_H$ 530 to 650°F<br>$T_C$ 510 to 630°F<br>$T_{AV}$ 530 to 630°F<br>ΔT Setpoint 0 to 100°F | ±2.7°F | 8.0 (including transport time) |

TABLE 7.2-3 (Cont'd)

| REACTOR TRIP SIGNAL | TYPICAL RANGE | TYPICAL TRIP ACCURACY | TYPICAL TIME RESPONSE (sec) |
|---|---|---|---|
| 8. Pressurizer low-pressure | 1700 to 2500 psig | ±18 psi (compensated signal) | 2.0 |
| 9. Pressurizer high-pressure | 1700 to 2500 psig | ±18 psi (non-compensated signal) | 2.0 |
| 10. Pressurizer high water level | Entire cylindrical portion of pressurizer (distance between taps) | ±2.3% of full range $\Delta\rho$ between taps at design temperature and pressure. | 1.2 |
| 11. Low reactor coolant flow | 0 to 120% of rated flow | ±2.5% of full flow within range of 70% to 100% of full flow (1) | 1.0 |
| 12. Reactor coolant pump bus undervoltage | 0 to 100% rated voltage | ±1% | 0.7 (Braidwood Unit 1)<br>0.8 (Byron and Braidwood Unit 2) |
| 13. Reactor coolant pump underfrequency | 50 to 65 Hz | ±0.1 Hz | 0.3 |
| 14. Low-low steam generator water level | ±~ 6 ft from nominal full load water level | ±2.3% of $\Delta\rho$ signal over pressure range of 700 to 1200 psig | 2.0 |
| 15. Turbine trip | | | 0.3 |

NOTES:

(1) Reproducibility (see definitions in Section 7.1).

TABLE 7.2-4

REACTOR TRIP CORRELATION

| | TRIP* | ACCIDENT** | TECH SPEC.*** |
|---|---|---|---|
| 1. | Power Range high neutrol flux trip (low setpoint) | Uncontrolled Rod Cluster Control Assembly Bank Withdrawal From a Subcritical or Low Power Startup Condition (15.4.1)<br><br>Feedwater System Malfunctions that Result in a Decrease in Feedwater Temperature (15.1.1)<br><br>Spectrum of Rod Cluster Control Assembly Ejection Accidents (15.4.8) | 3.3.1 Table 3.3.1-1 #2 |
| 2. | Power range high neutron flux trip (high setpoint) | Uncontrolled Rod Cluster Control Assembly Bank Withdrawal From a Subcritical or Low Power Startup Condition (15.4.1)<br><br>Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power (15.4.2)<br><br>Feedwater System Malfunctions that Result in a Decrease in Feedwater Temperature (15.1.1)<br><br>Excessive Increase in Secondary Steam Flow (15.1.3)<br><br>Inadvertent Opening of a Steam Generator Relief or Safety Valve (15.1.4)<br><br>Spectrum or Steam System Piping Failures Inside and Outside of Containment in a PWR (15.1.5)<br><br>Spectrum of Rod Cluster Control Assembly Ejection Accidents (15.4.8) | 3.3.1 Table 3.3.1-1 #2 |

TABLE 7.2-4 (Cont'd)

| | TRIP* | ACCIDENT* | TECH SPEC.*** |
|---|---|---|---|
| 3. | Intermediate range high neutron flux trip | Uncontrolled Rod Cluster Control Assembly Bank Withdrawal From a Subcritical or Low Power Startup Condition (15.4.1) | † 3.3.1 Table 3.3.1-1 #4 |
| 4. | Source range high neutron flux trip | Uncontrolled Rod Cluster Control Assembly Bank Withdrawal From a Subcritical or Low Power Startup Condition (15.4.1) | 3.3.1 Table 3.3.1-1 #5 |
| 5. | Power range high positive neutron flux rate trip | Spectrum of Rod Cluster Control Assembly Ejection Accidents (15.4.8) | 3.3.1 Table 3.3.1-1 #3a |
| 6. | | Intentionally left blank | |
| 7. | Overtemperature $\Delta T$ trip | Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power (15.4.2)<br><br>Chemical and Volume Control System Malfunction that Results in a Decrease in the Boro Concentration in the Reactor Coolant (15.4.6)<br><br>Loss of External Electrical Load (15.2.2)<br><br>Turbine Trip (15.2.3)<br><br>Feedwater System Malfunctions that Result in a Decrease in Feedwater Temperature (15.1.1)<br><br>Excessive Increase in Secondary Steam Flow (15.1.3)<br><br>Inadvertent Opening of a Pressurizer Safety or Relief Valve (15.6.1) | 3.3.1 Table 3.3.1-1 #6 Note 1 |

TABLE 7.2-4 (Cont'd)

| TRIP* | ACCIDENT** | TECH SPEC.*** |
|---|---|---|
| | Inadvertent Opening of a Steam Generator Relief or Safety Valve (15.1.4) | |
| | Steam Generator Tube Rupture (15.6.3) | |
| | Loss-of-Coolant Accidents Resulting from the Spectrum of Postulated Piping Breaks within the Reactor Coolant Pressure Boundary (15.6.5) | |
| 8. Overpower $\Delta T$ trip | Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power (15.4.2) | 3.3.1 Table 3.3.1-1 #7 Note 2 |
| | Feedwater System Malfunctions that Result in a Decrease in Feedwater Temperature (15.1.1) | |
| | Excessive Increase in Secondary Steam Flow (15.1.3) | |
| | Inadvertent Opening of a Steam Generator Relief or Safety Valve (15.1.4) | |
| | Spectrum of Steam System Piping Failures Inside and Outside of Containment in a PWR (15.1.5) | |
| 9. Pressurizer low-pressure trip | Inadvertent Opening of a Pressurizer Safety or Relief Valve (15.6.1) | 3.3.1 Table 3.3.1-1 #8a |
| | Loss-of-Coolant Accidents Resulting from the Spectrum of Postulated Piping Breaks within the Reactor Coolant Pressure Boundary (15.6.5) | |
| 10. Pressurizer high-pressure trip | Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power (15.4.2) | 3.3.1 Table 3.3.1-1 #8b |

TABLE 7.2-4 (Cont'd)

| TRIP* | ACCIDENT** | TECH SPEC.*** |
|---|---|---|
| | Loss of External Electrical Load (15.2.2) | |
| | Turbine Trip (15.2.3) | |
| 11. Pressurizer high water level trip | Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power (15.4.2) | 3.3.1 TABLE 3.3.1-1 #9 |
| | Loss of External Electrical Load Trip (15.2.2) | |
| | Turbine Trip (15.2.3) | |
| 12. Low reactor coolant flow | Partial Loss of Forced Reactor Coolant Flow (15.3.1) | 3.3.1 TABLE 3.3.1-1 #10 |
| | Loss of Nonemergency A-C Power to the Station Auxiliaries (15.2.6) | |
| | Complete Loss of Forced Reactor Coolant Flow (15.3.1) | |
| 13. Reactor coolant pump under-voltage trip | Complete Loss of Forced Reactor Coolant Flow (15.3.1) | 3.3.1 TABLE 3.3.1-1 #12 |
| 14. Reactor coolant pump under-frequency trip | Complete Loss of Forced Reactor Coolant Flow (15.3.1) | 3.3.1 TABLE 3.3.1-1 #13 |
| 15. Low-low steam generator water level trip | Loss of Normal Feedwater Flow (15.2.7) | 3.3.1 TABLE 3.3.1-1 #14 |
| | Feedwater System Pipe Break (15.2.8) | |
| 16. Reactor trip on turbine trip | Loss of External Electrical Load (15.2.2) | † 3.3.1 TABLE 3.3.1-1 #15 |
| | Turbine Trip (15.2.3) | |

TABLE 7.2-4 (Cont'd)

| TRIP* | ACCIDENT** | TECH SPEC.*** |
|---|---|---|
| | Loss of Nonemergency A-C Power to the Station Auxiliaries (15.2.6) | |
| 17. Safety injection signal actuation trip | Inadvertent Opening of a Steam Generator Relief or Safety Valve (15.1.4) | †† |
| 18. Manual trip | Available for all Accidents (Chapter 15.0) | † |

* Trips are listed in order of discussion in Section 7.2.
** References refer to accident analyses presented in Chapter 15.0.
*** References refer to Technical Specifications.
† A Technical Specification is not required because this trip is not assumed to function in the accident analyses.
†† Accident assumes that the reactor is tripped at end of life (EOL) which is the worst initial condition for this case.

TABLE 7.2-5

LOSS OF ANY SINGLE INSTRUMENT

| SENSOR | NUMBER OF CHANNELS | FAILED CHANNEL | SYSTEM | ASSUMED FAILURE DIRECTION | EFFECT | BOUNDING EVENT |
|---|---|---|---|---|---|---|
| feedpump discharge pressure | 1 per plant | | feedwater control | low | FW pump speed increases if in auto mode. (FW control valves close due to increased flow if in auto mode.) | If FW pump in manual - no event. If FW pump and FCV in auto - new steady-state w/higher pump speed and decreased FCV lift. If FW pump in auto and FCV in manual - bounding event is excessive FW flow (Subsection 15.1.2) |
| | | | | high | FW pump speed decreases if in auto mode. (FW control valves open due to decreased flow if in auto mode.) | If FW pump in manual - no event. Other modes - result in a decreased FW flow over time, hence bounding event is loss of normal FW flow (Subsection 15.2.7) |
| steam header pressure | 1 per plant | | feedwater control steam dump ($T_{AVG}$ Mode) | low | FW pump speed decreases if in auto mode. (FW control valves open due to decreased flow if in auto mode.) | If FW pump in manual - no event. Other modes - result in a decreased FW flow over time, hence bounding event is loss of normal FW flow (Subsection 15.2.7) |

TABLE 7.2-5 (Cont'd)

| SENSOR | NUMBER OF CHANNELS | FAILED CHANNEL | SYSTEM | ASSUMED FAILURE DIRECTION | EFFECT | BOUNDING EVENT |
|---|---|---|---|---|---|---|
| | | | | high | FW pump speed increases if in auto mode. (FW control valves close due to increased flow if in auto mode.) | If FW pump in manual - no event. If FW pump and FCV in auto - new steady-state w/higher pump speed and decreased FCV lift. If FW pump in auto and FCV in manual - bounding event is excessive FW flow (Subsection 15.1.2) |
| steam header pressure | 1 per plant | | feedwater control steam dump (pressure mode) | low | FW pump speed decreases if in auto mode. (FW control valves open due to decreased flow if auto mode.) | If FW pump in manual - no event. Other modes - result in a decreased FW flow over time, hence bounding event is loss of normal FW flow (Subsection 15.2.7) |
| | | | | high | FW pump speed increases if in auto mode. (FW control valves close due to increased flow if in auto mode.) Dump valves open (Steam dump blocked on Low-Low $T_{AVG}$ (P-12).) | Steam dump in pressure mode at hot standby or very low power only. Hence, dump valves will open for only a very short time till low-low $T_{AVG}$ (P-12) is reached. If FW pump speed is in manual or FW pump and |

TABLE 7.2-5 (Cont'd)

| SENSOR | NUMBER OF CHANNELS | FAILED CHANNEL | SYSTEM | ASSUMED FAILURE DIRECTION | EFFECT | BOUNDING EVENT |
|---|---|---|---|---|---|---|
| | | | | | | FCV in auto, then this event is bounded by excessive increase in secondary steam flow (Subsection 15.1.3). If FW pump in auto and FCV in manual, get increase in FW flow causing excessive cooling. Bounding event is excessive FW flow (Subsection 15.1.2) |
| loop steam flow | 2 per loop | 1 selected for control | feedwater control | low | FW pump speed decreases if in auto mode. FW valves close if in auto mode. | If FW pump and FCV in manual - no event. Other modes result in decreased FW flow, bounding event is loss of normal FW flow (Subsection 15.2.7) |
| | | | | high | FW pump speed increases if in auto mode. FW valves open if in auto mode. | If FW pump and FCV in manual - no event. Other modes - result in increased FW flow, bounding event is excessive FW flow (Subsection 15.1.2) |

TABLE 7.2-5 (Cont'd)

| SENSOR | NUMBER OF CHANNELS | FAILED CHANNEL | SYSTEM | ASSUMED FAILURE DIRECTION | EFFECT | BOUNDING EVENT |
|---|---|---|---|---|---|---|
| loop FW flow | 2 per loop | 1 selected for control | feedwater control | low | FW valve opens if in auto mode. | If FCV in manual - no event. If FCV in auto, result is excessive FW flow (Subsection 15.1.2) |
| | | | | high | FW valve closes if in auto mode. | If FCV in manual - no event. If FCV is auto, result is decreased FW flow. Bounding event is loss of normal FW flow (Subsection 15.2.7) |
| narrow range level | 4 per steam generator (two available for control | 1 selected for control (I or II) | feedwater control | low | FW valve opens if in auto mode. | If FCV in manual - no event. If FCV in auto, result in excessive FW flow (Subsection 15.1.2) |
| | | | | high | FW valve closes if in auto mode. | If FCV in manual - no event. If FCV is auto, result is decreased FW flow. Bounding event is loss of normal FW flow (Subsection 15.2.7) |

TABLE 7.2-5 (Cont'd)

| SENSOR | NUMBER OF CHANNELS | FAILED CHANNEL | SYSTEM | ASSUMED FAILURE DIRECTION | EFFECT | BOUNDING EVENT |
|---|---|---|---|---|---|---|
| pressurizer level (control) | 3 per plant | I or III | pressurizer level control | low | Charging flow increases. Heaters turn off (except local control). Letdown isolated (VCT empties, charging pumps take suction from RWST.) | Bounding event is increased reactor coolant inventory (Subsection 15.5.2) |
| | | | | high | Charging flow decreases Backup heaters on (Later, letdown isolation from interlock channel, heaters blocked from interlock channel.) | While heaters are on, no net depressurization of RCS. After heaters are blocked, decreased charging flow acts to depressurize RCS. Depressurization event is therefore bounded by inadvertent opening of a pressurizer safety or relief valve (Subsection 15.6.1) |
| pressurizer level (interlock) | 3 per plant | II or III | pressurizer level control | low | Letdown isolated. Pressurizer heaters blocked (except for local control). (Charging flow reduced to maintain level.) | Steady-state reached at slightly high level. No event. |
| | | | | high | No control action, get high level annunciation. | Not applicable |

TABLE 7.2-5 (Cont'd)

| SENSOR | NUMBER OF CHANNELS | FAILED CHANNEL | SYSTEM | ASSUMED FAILURE DIRECTION | EFFECT | BOUNDING EVENT |
|---|---|---|---|---|---|---|
| pressurizer pressure | 4 per plant | I | pressurizer pressure control (Pos. 1 or 2)* | low | Turn on pressurizer variable and backup heaters. PORV 455A blocked from opening. PORV 456 opens if required, closes when pressure falls below dead band. Spray remains off. | Heaters being on cause increase in pressurizer pressure to PORV 456 actuation. No event. |
| | | | | high | PORV 455A opens, closes on low pressure due to interlock. Spray turned on. | Result is bounded by inadvertent opening of a pressurizer safety or relief valve (Subsection 15.6.1) |
| | | | (Pos. 3)* | | Channels not connected. | |
| pressurizer pressure | 4 per plant | II | pressurizer pressure control (Pos. 2 or 3)* | low | No control action. PORV 456 blocked from opening. PORV 455A opens if required, closes when pressure falls below deadband. | Not applicable |
| | | | | high | PORV 456 opens, closes when pressure falls below interlock setpoint. | Result is bounded by inadvertent opening of a pressurizer safety or relief valve (Subsection 15.6.1) |

TABLE 7.2-5 (Cont'd)

| SENSOR | NUMBER OF CHANNELS | FAILED CHANNEL | SYSTEM | ASSUMED FAILURE DIRECTION | EFFECT | BOUNDING EVENT |
|---|---|---|---|---|---|---|
| | | | (Pos. 1)* | | Channels not connected | Not applicable |
| pressurizer pressure | 4 per plant | III | pressurizer pressure control (Pos. 3)* | low | Turn on pressurizer variable and backup heaters. PORV 455A and 456 blocked from opening. Spray remains off. | Heaters being on cause increase in pressurizer pressure, possibly to safety valve actuation No event. |
| | | | | high | PORV 455A opens, closes on low pressure interlock. Spray turned on. PORV 456 unblocked. | Result is bounded by inadvertent opening of a pressurizer safety or relief valve (Subsection 15.6.1) |
| | | | (Pos. 1 or 2)* | low | Block PORV 456 from opening; no control action | Not applicable |
| | | | | high | Unblock PORV 456; no control action | Not applicable |
| pressurizer pressure | 4 per plant | IV | pressurizer pressure control (Pos. 1)* | low | Block PORV 456 and 455A from opening; no control action | Not applicable |
| | | | | high | PORV 455A unblocked. PORV 456 opens, closes when pressure falls below interlock setpoint. | Result is bounded by inadvertent opening of a pressurizer safety or relief valve (Subsection 15.6.1) |

TABLE 7.2-5 (Cont'd)

| SENSOR | NUMBER OF CHANNELS | FAILED CHANNEL | SYSTEM | ASSUMED FAILURE DIRECTION | EFFECT | BOUNDING EVENT |
|---|---|---|---|---|---|---|
| | | | (Pos. 2 or 3)* | low | Block PORV 455A from opening; no control action | Not applicable |
| | | | | high | Unblock PORV 455A; no control action | Not applicable |
| $T_{AVG}$ | one per loop | any<br>auctioneered high | steam dump ($T_{AVG}$ Mode) reactor control pressurizer level control | low | Stop turbine loadings defeat remote dispatching (C-16 annunciation occurs) | Not applicable |
| | | auctioneered low | turbine loading/ dispatching | high | Rods in (safe direction). Charging flow increases until full power pressurizer level is reached (if at reduced power). If reactor trips, steam dump enabled and dump valves open until steam dump stops when Low-Low $T_{AVG}$ is reached. | No event unless reactor trips, then dump valves open and bounding event is excessive increase in secondary steam flow (Subsection 15.1.3) |
| $T_{AVG}$ | one per loop | any<br>auctioneered high | steam dump (pressure mode) reactor control pressurizer level control | low | Stop turbine loading, defeat remote dispatching (C-16 annunciation occurs) | Not applicable |

TABLE 7.2-5 (Cont'd)

| SENSOR | NUMBER OF CHANNELS | FAILED CHANNEL | SYSTEM | ASSUMED FAILURE DIRECTION | EFFECT | BOUNDING EVENT |
|---|---|---|---|---|---|---|
| | | auctioneered low | turbine loading/ dispatching | high | Rods in (safe direction). Charging flow increases until full power pressurizer level is reached (if at reduced power). | Steady-state reached at full power pressurizer level. No event |
| steamline pressure | 3 per loop for protection, 1 per loop for control (different from those used for protection) | control channel | steam dump | low | No control action | Not applicable |
| | | | | high | Steam generator relief valve opens | Result is bounded by inadvertent opening of a steam generator relief or safety valve (Subsection 15.1.4) |
| intermediate range flux | 2 per plant | I or II | reactor control | low | No control action | Not applicable |
| | | | | high | Reactor trips (during startup only) | Not applicable |
| turbine impulse chamber pressure (control) | 2 per turbine | 1 (Pos. 1)* | steam dump $T_{AVG}$ mode) reactor control FW control | low | Rods in (safe direction), auto rod withdrawal blocked and remote dispatching defeated (C-5). Steam dump signaled to open but is blocked by interlock. (If reactor trip occurs, steam dump unblocked and dump valves | Not applicable |

TABLE 7.2-5 (Cont'd)

| SENSOR | NUMBER OF CHANNELS | FAILED CHANNEL | SYSTEM | ASSUMED FAILURE DIRECTION | EFFECT | BOUNDING EVENT |
|---|---|---|---|---|---|---|
| | | | | | modulate until no load $T_{AVG}$ is reached.) No effect on FW control since have constant SG level program. | |
| | | | | high | Stop turbine loading; defeat remote dispatching (C-16). Rods out until blocked by high flux, overpower, or overtemperature, rod stop, or until programmed $T_{REF}$ limit is reached. (If reactor trip occurs, steam dump unblocked and dump valves open until no load $T_{AVG}$ is reached.) No effect on FW control since have constant SG level program. | Result is bounded by uncontrolled rod cluster control assembly bank withdrawal at power (Subsection 15.4.2) |
| | | I (Pos. 2)* | steam dump ($T_{AVG}$ mode) | low or high | No control action | Not applicable |

TABLE 7.2-5 (Cont'd)

| SENSOR | NUMBER OF CHANNELS | FAILED CHANNEL | SYSTEM | ASSUMED FAILURE DIRECTION | EFFECT | BOUNDING EVENT |
|---|---|---|---|---|---|---|
| turbine impulse chamber pressure (control) | 2 per turbine | I (Pos. 1)*<br>II (Pos. 2)* | steam dump (pressure mode) reactor control FW control | low | Rods in, (safe direction), auto rod withdrawal blocked (C-5), and remote dispatching defeated No effect on FW control since have constant SG level program. | Not applicable |
| | | | | high | Stop turbine loading; defeat remote dispatching (C-16). Rods out until blocked by high flux, overpower, or overtemperature rod stop. (Steam dump valves open if required to keep steam header pressure at or below setpoint.) No effect on FW control since have constant SG level program. | Result is bounded by uncontrolled rod cluster control assembly bank withdrawal at power (Subsection 15.4.2) |
| turbine impulse chamber pressure (interlock) | 2 per turbine | II (Pos. 1)* | steam dump ($T_{AVG}$ mode) | low | Unblock steam dump | Not applicable |

TABLE 7.2-5 (Cont'd)

| SENSOR | NUMBER OF CHANNELS | FAILED CHANNEL | SYSTEM | ASSUMED FAILURE DIRECTION | EFFECT | BOUNDING EVENT |
|---|---|---|---|---|---|---|
| | | | | high | Steam dump on turbine trip only, steam dump blocked on load rejection. | Not applicable |
| turbine impulse chamber pressure (interlock) | 2 per turbine | II (Pos. 1)* | steam dump (pressure mode) | low or high | No control action | Not applicable |
| | | II (Pos. 2)* | steam dump ($T_{AVG}$ Mode) reactor control FW control | low | Steam dump unblocked. Rods in (safe direction), auto rod withdrawal blocked and remote dispatching defeated (C-5). (If reactor trip occurs steam dump comes on and dump valves modulate until no load $T_{AVG}$ is reached.) No effect on FW control since have constant SG level program. | Not applicable |
| | | | | high | Stop turbine loading; defeat remote dispatching (C-16). Rods out until blocked by high flux, overpower, or overtemperature, rod | Result is bounded by uncontrolled rod cluster control assembly bank withdrawal at power (Subsection 15.4.2) |

TABLE 7.2-5 (Cont'd)

| SENSOR | NUMBER OF CHANNELS | FAILED CHANNEL | SYSTEM | ASSUMED FAILURE DIRECTION | EFFECT | BOUNDING EVENT |
|---|---|---|---|---|---|---|
| | | | | | stop, or until programmed $T_{REF}$ limit is reached. (If reactor trip occurs, steam dump unblocked and dump valves open until no load $T_{AVG}$ is reached.) No effect on FW control since have constant SG level program. | |
| power range flux | 4 per plant | any | reactor control FW control | low | No control action. (auctioneered high) | Not applicable |
| | | | | high | Auto and manual rod withdrawal blocked (C-2), rods in (safe direction). FW bypass valve opens if in auto. (If reactor trip occurs, dump valves open until no-load $T_{AVG}$ is reached.) Rising SG level causes valve to close until steam and feed flows match. | Steady-state reached with higher SG level. No event. |
| condenser available | 1 per plant | _____ | steam dump | low | No control action-steam dump blocked, condenser unavailable. | Not applicable |

TABLE 7.2-5 (Cont'd)

| SENSOR | NUMBER OF CHANNELS | FAILED CHANNEL | SYSTEM | ASSUMED FAILURE DIRECTION | EFFECT | BOUNDING EVENT |
|---|---|---|---|---|---|---|
| | | | | high | No control action-steam dump unblocked, condenser available. | Not applicable |
| $T_{AVG}$ high auctioneer backup | 1 per plant<br>cluster control | _____ | steam dump reactor control pressurizer level control | low | Steam dump blocked ($T_{AVG}$ mode). Charging flow decreased until no-load level reached. Backup heaters on. Rods out, power increases until blocked by high flux, overpower, or overtemperature rod stop. | Result is bounded by uncontrolled rod cluster control assembly bank withdrawal at power (Subsection 15.4.2) |
| | | | | high | Identical to $T_{AVG}$ channel failing high, see analysis above. | See above |
| steam flow pressure compensator | 2 per loop | control channel | steam flow | low | Identical to loop steam flow channel failing low. See analysis above. | See above |
| | | | | high | Identical to loop steam flow channel failing high. See analysis above. | See above |

_____
* Signals for pressurizer level or pressure and turbine impulse chamber pressure can be obtained from different channels. Selection of desired channels is done by manual switches in the control room. Resulting accident due to failed instrument is dependent on switch positions.

TABLE 7.2-6

LOSS OF POWER TO INVERTER I

(Loss of Power to Protection Set I and Control Group 1)

| CONTROL SYSTEMS AFFECTED | SIGNALS AFFECTED | FAILURE DIRECTION | ITEMIZED EFFECTS | BOUNDING EVENT |
|---|---|---|---|---|
| steam dump | all (system deenergized) | off/closed | No initiating event, steam dump system unavailable. | |
| reactor control | power range flux (Ch. 1) | low | For turbine impulse pressure switch in normal position. | |
| | turbine pressure (control) | low | Rods in, power decreases. Auto rod withdrawal blocked, stop turbine loading, defeat | |
| | $T_{AVG}$ (Loop 1) | low | remote dispatching (C-5, C-16). No control action if turbine impulse pressure switch is in alternate position. | |
| FW control (SG 1) and pump speed control | all (system deenergized) | FW valve closes in SG 1. Pump speed decreases (auto mode only) | Loss of main FW in SG 1. (Plant trips on low SG 1 level) Other loops have decrease in FW flow due to decreased pump speed. | Loss of FW flow (Subsection 15.2.7) event is bounding since increased charging flow/isolated letdown has little effect relative to the decreased feed flow in SG 1. (Reactor trip would occur on SG low-low level) |
| FW control (SG 2, 3) and/or 4) | narrow range level | low | Depending on the relative switch positions in each loop for steam | |
| | steam flow | low | flow, feedwater flow, and narrow-range level, feedwater valve could | |
| | feedwater flow | low | open, close, or remain fixed; thus, a feedwater flow transient may occur in these loops. | |

TABLE 7.2-6 (Cont'd)

| CONTROL SYSTEMS AFFECTED | SIGNALS AFFECTED | FAILURE DIRECTION | ITEMIZED EFFECTS | BOUNDING EVENT |
|---|---|---|---|---|
| pressurizer level | pressurizer level (control) | low | Sw. pos. 2 or 3 - Charging flow increases, heaters blocked, letdown isolated<br><br>Sw. pos. 1 or 2 - channel not connected, no control action. | |
| pressurizer pressure | pressurizer pressure (PORV 455A control) | low | Sw. pos. 1 or 2 - spray off. PORV 455A blocked from opening. PORV 456 available if needed. Sw. pos. 3 - Channel not connected, no control action. | |

TABLE 7.2-7

LOSS OF POWER TO INVERTER II

(Loss of Power to Protection Set II and Control Group 2)

| CONTROL SYSTEMS AFFECTED | SIGNALS AFFECTED | FAILURE DIRECTION | ITEMIZED EFFECTS | BOUNDING EVENT |
|---|---|---|---|---|
| steam dump | turbine pressure (interlock) | low | No control action, steam dump unblocked. | |
| reactor control | power range flux (Ch. 2) | low | For turbine impulse pressure switch in alternate position, rods in, power decreases. Auto rod withdrawal blocked, stop turbine loading, defeat remote dispatching (C-5, C-16). No control action if turbine impulse pressure switch is in normal position. | Loss of FW flow (Subsection 15.2.7) event is bounding for similar reasons as for loss of inverter I. (Reactor trip would occur on SG 2 low-low level) |
| | turbine pressure (interlock and control) | low | | |
| | $T_{AVG}$ (Loop 2) | low | | |
| FW control (SG 2) | all in SG 2 (system deenergized) | FW valve closes | Loss of main FW in SG 2. (Plant trips on low SG 2 level.) | |
| FW control (SG 1, 3) and/or 4) | narrow range level | low | Depending on the relative switch positions in each loop for steam flow, feedwater flow, and narrow-range level, feedwater valves could open, close, or remain fixed; thus, a feedwater transient may occur in these loops. | |
| | steam flow | low | | |
| | feedwater flow | low | | |

TABLE 7.2-7 (Cont'd)

| CONTROL SYSTEMS AFFECTED | SIGNALS AFFECTED | FAILURE DIRECTION | ITEMIZED EFFECTS | BOUNDING EVENT |
|---|---|---|---|---|
| pressurizer level | all (system deenergized) | low | Charging flow off, letdown isolated, heaters blocked. | |
| pressurizer pressure | pressurizer pressure (PORV 456 control) | closed | Selection switch loses power (control group 2) and is locked normal position, pos. 2 - No control action, PORV 456 stays closed, PORV 455A available if needed. | |

TABLE 7.2-8

LOSS OF POWER TO INVERTER III

(Loss of Power to Protection Set III and Control Group 3)

| CONTROL SYSTEMS AFFECTED | SIGNALS AFFECTED | FAILURE DIRECTION | ITEMIZED EFFECTS | BOUNDING EVENT |
|---|---|---|---|---|
| steam dump | none | - - | No signals affected, no control action. | |
| rod control | power range flux (Ch. 3)<br>$T_{AVG}$ Loop 3 | low<br>low | Stop turbine loading/defeat remote dispatching. | Loss of FW flow (Subsection 15.2.7) event is bounding for similar reasons as for loss of Inverter I. Reactor trip will occur on SG 3 low-low water level) |
| FW control (SG 3) | all (system deenergized) | FW valve closes | Loss of main FW in SG 3. (Plant trips on low SG 3 level.) | |
| pressurizer level | pressurizer level (control or interlock) | low | Sw. pos. 1 - charging flow increases, heaters blocked, letdown isolated.<br><br>Sw. pos. 2 - no control action, channel not connected.<br><br>Sw. pos. 3 - Heaters blocked, letdown isolated. (Charging flow reduces to maintain level.) | |
| pressurizer pressure | pressurizer pressure (PORV 456 interlock; PORV 455A control) | low | Sw. pos. 1 or 2 - No control action, PORV 456 blocked closed Sw. pos. 3 - PORV 455A and 456 blocked closed, pressurizer heaters on (if allowed by level interlock), spray off. | |

TABLE 7.2-9

LOSS OF POWER TO INVERTER IV

(Loss of Power to Protection Set IV and Control Group 4)

| CONTROL SYSTEMS AFFECTED | SIGNALS AFFECTED | FAILURE DIRECTION | ITEMIZED EFFECTS | BOUNDING EVENT |
|---|---|---|---|---|
| steam dump | auctioneered $T_{AVG}$ | low | No initiating accident, low $T_{AVG}$ prevents activation of steam dump. | |
| rod control | all (system deenergized) | low | No control action, no rod motion. | Loss of FW flow (Subsection 15.2.7) event is bounding since turning on of pressurizer heaters is temporary and transient effects are slow-reacting in comparison with loss of FW. (SG 4 tripped on low-low water level.) |
| FW control (SG 4) | all (system deenergized) | FW Valve Closes | Loss of main FW in SG 4 (Plant trips on low SG 4 level.) | |
| pressurizer level | auctioneered $T_{AVG}$ | low | Any Sw. pos. - turn on all backup heaters. Charging flow reduced till no-load level reached. (Spray turned on when pressure rises to lower setpoint due to heaters. | |
| pressurizer pressure | pressurizer pressure (PORV 455A interlock; PORV 456 control) | low | Sw. pos. 1 - No control action; both PORVs blocked closed. Sw. pos. 2 or 3 - No control action, PORV 455A blocked closed. | |

TABLE 7.2-10

LOSS OF POWER TO PROTECTION SET I

| CONTROL SYSTEMS AFFECTED | SIGNALS AFFECTED | FAILURE DIRECTION | ITEMIZED EFFECTS | BOUNDING EVENT |
|---|---|---|---|---|
| steam dump | turbine pressure (control) | low | Steam dump demanded but blocked from interlock. If reactor trips, steam dump performs as designed.) | |
| reactor control | power range flux (Ch. 1)<br><br>turbine pressure (control)<br><br>$T_{AVG}$ (Loop 1) | low | For turbine impulse pressure switch in normal position, rods in (safe direction), power decreases. Auto rod withdrawal blocked, (C-5). Stop turbine loading/defeat remote dispatching (C-16). No control action if turbine impulse pressure switch is in alternate position. | Bounding event is either excessive FW flow (Subsection 15.1.2), or loss of normal feedwater flow (Subsection 15.2.7), depending on channels used. Increased charging flow and pressurizer transients have little effect in comparison. |
| FW control | narrow range level (any loop)<br><br>steam flow pressure (any loop)<br><br>feedwater flow (any loop) | low<br><br>low<br><br>low | Depending on the relative switch position in each loop for steam flow, FW flow, and narrow-range level, FW valve could open, close, or remain fixed; thus, a FW transient may occur in these loops. | |

TABLE 7.2-10 (Cont'd)

| CONTROL SYSTEMS AFFECTED | SIGNALS AFFECTED | FAILURE DIRECTION | ITEMIZED EFFECTS | ROUNDING EVENT |
|---|---|---|---|---|
| pressurizer level | pressurizer level (control) | low | If affected level signal used for control, charging flow increases, letdown isolated, heaters blocked. Otherwise, channel not connected, no control action. | |
| pressurizer pressure | pressurizer pressure (PORV 455A) | low | If affected pressure signal used for control, PORV 455A stays closed, back-up heaters on (but could be blocked on level signal, see above). Spray off. (PORV 456 available if required.) Otherwise, channel not connected, no control action. | |

TABLE 7.2-11

LOSS OF POWER TO PROTECTION SET II

| CONTROL SYSTEMS AFFECTED | SIGNALS AFFECTED | FAILURE DIRECTION | ITEMIZED EFFECTS | BOUNDING EVENT |
|---|---|---|---|---|
| steam dump | turbine pressure (interlock) | low | Steam dump unblocked. (If reactor trips, steam dump performs as designed.) | |
| reactor control | power range flux (control) | low | For turbine impulse pressure switch in alternate position, rods in (safe direction), power decreases. Auto rod withdrawal blocked, (C-5). Stop turbine loading/defeat remote dispatching (C-16). No control action if turbine impulse pressure switch is in normal position. | Bounding event is either excessive FW flow (Subsection 15.1.2), or loss of normal FW flow (Subsection 15.2.7), depending on channels used. |
| | turbine pressure (control) | low | | |
| | $T_{AVG}$ (Loop 2) | low | | |
| FW control | narrow range level (any loop) | low | Depending on the relative switch positions in each loop for steam flow, FW flow, and narrow-range level, FW valves could open, close, or remain fixed; thus, a FW transient may occur in these loops. | |
| | steam flow (any loop) | low | | |
| | feedwater flow (any loop) | low | | |

TABLE 7.2-11 (Cont'd)

| CONTROL SYSTEMS AFFECTED | SIGNALS AFFECTED | FAILURE DIRECTION | ITEMIZED EFFECTS | BOUNDING EVENT |
|---|---|---|---|---|
| pressurizer level | pressurizer level (interlock) | low | If affected level signal used for interlock, block heaters and isolate letdown Otherwise, channel not connected, no control action. | |
| pressurizer pressure | pressurizer pressure (PORV 456) | low | If affected pressure signal used for control, PORV 456 stays closed. (PORV 455A available if required). Otherwise, channel not connected, no control action. | |

TABLE 7.2-12

LOSS OF POWER TO PROTECTION SET III

| CONTROL SYSTEMS AFFECTED | SIGNALS AFFECTED | FAILURE DIRECTION | ITEMIZED EFFECTS | BOUNDING EVENT |
|---|---|---|---|---|
| steam dump | none | - - | No signals affected, no control action. | |
| reactor control | power range flux (control) | low | No control action due to auctioneers. | |
| | $T_{AVG}$ (Loop 3) | low | | |
| FW control | none | -- | No signals affected, no control action. | |
| pressurizer level | pressurizer level (control or interlock) | low | If affected level signal used for control, charging flow increases, letdown isolated, heaters blocked. If used for interlock, heaters blocked and letdown isolated. Otherwise, channel not connected, no control action. | Combining effects of pressurizer level and pressure control systems, could have either increasing charging flow with heater off causing a depressurization, or else heaters cause pressure to increase unit PORV 455A is actuated, or until safety valve opens. Either way, event is bounded by inadvertent opening of a pressurizer safety or relief valve (Subsection 15.6.1) |

TABLE 7.2-12 (Cont'd)

| CONTROL SYSTEMS AFFECTED | SIGNALS AFFECTED | FAILURE DIRECTION | ITEMIZED EFFECTS | BOUNDING EVENT |
|---|---|---|---|---|
| pressurizer pressure | pressurizer pressure (PORV 456 interlock and PORV 455A control) | low | PORV 456 closed. If affected pressure signal used for control, PORV 455A stays closed, pressurizer heaters on (if allowed by level signal, see above) and spray off. Otherwise, PORV 455A available if required. | |

TABLE 7.2-13

LOSS OF POWER TO PROTECTION SET IV

| CONTROL SYSTEMS AFFECTED | SIGNALS AFFECTED | FAILURE DIRECTION | ITEMIZED EFFECTS | BOUNDING EVENT |
|---|---|---|---|---|
| steam dump | none | - - | No signals affected, no control action. | |
| reactor control | power range flux (control) | low | No control action due to auctioneers. | |
| | $T_{AVG}$ (Loop 4) | low | | |
| FW control | none | - - | No signals affected, no control action. | No event is initiated due to loss of power, therefore bounding event is not applicable |
| pressurizer level | none | - - | No signals affected, no control action. | |
| pressurizer pressure | pressurizer pressure (control and interlock) (PORV 456 control and PORV 455A interlock) | low | PORV 455A stays closed. If affected pressure signal used for control, PORV 456 also stays closed. Otherwise, PORV 456 available if needed. | |

TABLE 7.2-14

LOSS OF POWER TO CONTROL GROUP 1

| CONTROL SYSTEMS AFFECTED | SIGNALS AFFECTED | FAILURE DIRECTION | ITEMIZED EFFECTS | BOUNDING EVENT |
|---|---|---|---|---|
| steam dump | all (system deenergized) | off/closed | No initiating event, steam dump system unavailable. (If reactor trip occurs, SG atmos. relief valves available.) | |
| reactor control | none | - - | No signals affected, no control action | Bounding event is loss of normal FW flow (Subsection 15.2.7). Plant trips on low level in SG 1). |
| FW control (SG 1) and FW pump speed control | all (system deenergized) | FW Valve Closes pump speed Decreases (Auto mode only) | Loss of main FW in SG 1. If FW pump in auto mode, pump speed decreases causing FCV to open in SG 2, 3, and 4. (Plant trips on low level in SG 1) | |
| pressurizer level | none | - - | No signals affected, no control action. | |
| pressurizer pressure | pressurizer pressure (PORV 455A control) | closed | No initiating event, PORV 455A remains closed, heaters and spray remain off. (PORV 456 available if needed.) | |
| | spray and heater actuation | off | | |

TABLE 7.2-15

LOSS OF POWER TO CONTROL GROUP 2

| CONTROL SYSTEMS AFFECTED | SIGNALS AFFECTED | FAILURE DIRECTION | ITEMIZED EFFECTS | BOUNDING EVENT |
|---|---|---|---|---|
| steam dump | none | - - | No signals affected, no control action. | |
| reactor control | none | - - | No signals affected, no control action. | |
| FW control (SG 2) | all (system deenergized) | FW valve closes | Loss of main FW in SG 2 (Plant trips on low level in SG 2) | Bounding event is loss of normal FW flow (Subsection 15.2.7). (Plant trips on low level in SG 2). |
| pressurizer level | all (system deenergized) | off | Charging flow increases letdown isolated, heaters blocked | |
| pressurizer pressure | pressurizer pressure (PORV 456 control) | closed | PORV 456 blocked closed. (PORV 455A available if needed.) | |

TABLE 7.2-16

LOSS OF POWER TO CONTROL GROUP 3

| CONTROL SYSTEMS AFFECTED | SIGNALS AFFECTED | FAILURE DIRECTION | ITEMIZED EFFECTS | BOUNDING EVENT |
|---|---|---|---|---|
| steam dump | none | - - | No signals affected, no control action. | |
| reactor control | none | - - | No signals affected, no control action. | |
| FW control (SG 3) | all (system deenergized) | FW valve closes | Loss of main FW in SG 3 (Plant trips on low level in SG 3) | Bounding event is loss of normal FW flow (Subsection 15.2.7). (Plant trips on low level in SG 3). |
| pressurizer level | none | - - | No signals affected, no control action. | |
| pressurizer pressure | pressurizer pressure (PORV 456 interlock) | closed | No initiating event, PORV 456 blocked closed. (PORV 455A available if needed.) | |

TABLE 7.2-17

LOSS OF POWER TO CONTROL GROUP 4

| CONTROL SYSTEMS AFFECTED | SIGNALS AFFECTED | FAILURE DIRECTION | ITEMIZED EFFECTS | BOUNDING EVENT |
|---|---|---|---|---|
| steam dump | auctioneered $T_{AVG}$ | low | No initiating event, steam dump dump system unavailable. (If reactor trip occurs, SG atmos. relief valves available.) | |
| reactor control | all (system deenergized) | off | Rods stay stationary | |
| FW control | all (system deenergized) | FW valve closes | Loss of main FW in SG 4 (Plant trips on low level in SG 4) | Bounding event is loss of normal FW flow (Subsection 15.2.7) since decreased charging flow has little effect in comparison. (Plant trips on low SG 4 level.) |
| pressurizer level | auctioneered $T_{AVG}$ | low | Charging flow decreases till nonload pressurizer level reached. | |
| pressurizer pressure | pressurizer pressure (PORV 455A interlock) | closed | No initiating event, PORV 455A blocked closed. (PORV 456 available if needed.) | |

TABLE 7.2-18

LOSS OF COMMON INSTRUMENT LINES

(ASSUMED BREAK IN LINE)

| SENSORS | FAILED CHANNELS | SYSTEM | FAILURE DIRECTION | EFFECT | BOUNDING ACCIDENT |
|---|---|---|---|---|---|
| loop steam flow and narrow range level | I or II | feedwater control | low high | If steam flow and/or narrow-range level selectors switched to failed channel, FW valve closes in affected SG, pump speed decreases. | Bounding event is loss of normal FW (Subsection 15.1.2) |
| pressurizer level (control) and pressurizer pressure (PORV 455A, control) | I (level and pressure) | pressurizer level control (Sw. Pos. 1 or 2) | high | PORV 455A stays closed. Spray unavailable. Charging flow decreases (control). Backup heaters on (control). (On low level, letdown isolated from interlock channel and heaters blocked.) | These effects at worst result in a depressurization which is bounded by inadvertent opening of a pressurizer safety or relief valve (Subsection 15.6.1). |
| | | pressurizer pressure control (Sw. Pos. 1 or 3) | low | | |
| pressurizer level (interlock) and pressurizer pressure (PORV 456, control) | II (level and pressure) | pressurizer level control (Sw. Pos. Pos. 1 or 2) | III | No level control action. PORV 456 stays closed. | Not applicable |
| | | pressurizer pressure control (Sw. Pos. 1 or 2) | low | | |

TABLE 7.2-18 (Cont'd)

| SENSORS | FAILED CHANNELS | SYSTEM | FAILURE DIRECTION | EFFECT | BOUNDING ACCIDENT |
|---|---|---|---|---|---|
| pressurizer level (control or interlock) and pressurizer pressure (either PORV, interlock) | III (level)<br><br>III and IV (pressure) | pressurizer pressure control (Sw. Pos. 1, interlock); Sw. Pos. 2, control pressurizer pressure control (any switch position) | high<br>low | PORV 455A and 456 blocked closed. Spray unavailable if on Channel III (Sw. pos. 3). Charging flow decreases and backup heaters on if on control channel. No control action from level interlock. (On low level, letdown isolation and heaters blocked from nonfailed interlock channel.) | Depending on switch positions, these effects at worst result in a depressurization which is bounded by inadvertent opening of a pressurizer safety or relief valve (Subsection 15.6.1). |

TABLE 7.2-19

REACTOR TRIP SYSTEM INSTRUMENTATION MAXIMUM ALLOWABLE RESPONSE TIMES

| FUNCTIONAL UNIT | MAXIMUM ALLOWABLE RESPONSE TIME |
|---|---|
| 1. Manual Reactor Trip | N.A. |
| 2. Power Range, Neutron Flux | ≤ 0.5 second* |
| 3. Power Range, Neutron Flux, High Positive Rate | N.A. |
| 4. Intentionally left blank | |
| 5. Intermediate Range, Neutron Flux | N.A. |
| 6. Source Range, Neutron Flux | ≤ 0.5 second* |
| 7. Overtemperature $\Delta T$ | ≤ 8.0 seconds** |
| 8. Overpower $\Delta T$ | ≤ 8.0 seconds** |
| 9. Pressurizer Pressure-Low (Above P-7) | ≤ 2.0 seconds |
| 10. Pressurizer Pressure-High | ≤ 2.0 seconds |
| 11. Pressurizer Water Level-High (Above P-7) | N.A. |
| 12. Low Reactor Coolant Flow - Low | |
| a. Single Loop (Above P-8) | ≤ 1.0 second |
| b. Two Loops (Above P-7 and below P-8) | ≤ 1.0 second |
| 13. Steam Generator Water Level-Low-Low | ≤ 2.0 seconds |

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

** Total time delay (including RTD response time and trip circuit channel electronic delays) from the time the temperature difference in the coolant loop exceeds the trip setpoint until the rods are free to fall, including time for trip breakers to open and CRDM gripper release.

TABLE 7.2-19 (Cont'd)

| FUNCTIONAL UNIT | MAXIMUM ALLOWABLE RESPONSE TIME |
|---|---|
| 14. Undervoltage-Reactor Coolant Pumps (Above P-7) | ≤ 1.5 seconds |
| 15. Underfrequency-Reactor Coolant Pumps (Above P-7) | ≤ 0.6 second |
| 16. Turbine Trip (Above P-8) | |
| a. Emergency Trip Header Pressure | N.A. |
| b. Turbine Throttle Valve Closure | N.A. |
| 17. Safety Injection Input from ESF | N.A. |
| 18. Reactor Coolant Pump Breaker Position Trip (Above P-7) | N.A. |
| 19. Reactor Trip System Interlocks | N.A. |
| 20. Reactor Trip Breakers | N.A. |
| 21. Automatic Trip and Interlock Logic | N.A. |

## 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 a loss-of-a-coolant accident or a steamline 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 ensure 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 uses 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 breaks (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 instrumentation readouts provided to the operator to enable him to perform required manual safety actions and to determine the effect of manual actions taken following reactor trip due to a Condition II, III, or IV event are listed in Table 7.5-1. Instrumentation is considered to include indicators, recorders, and manual and manual/auto control stations. All instrumentation in the main control room powered from non-ESF busses would be presumed lost following a loss of offsite power. This would include instrumentation for circulating water, primary water, nonessential service water, instrument air, service air, condensate and condensate booster, environmental monitoring, off gas, fire protection, HVAC, switchyard, turbine, generator, auxiliary steam, extraction steam, heater drains, and feedwater. The annunciator system and plant computer are not lost following a loss of offsite power because they are provided with battery backup. The engineered safety features actuation system meets the requirements of Criteria 13, 20, 27, 28, and 38 of the 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 Subsection 7.3.1.1.1 is listed below and discussed in this section. (For

additional background information refer to References 1, 2, and 3.)

a. process instrumentation and control system (Reference 1),

b. solid-state logic protection system (Reference 2),

c. engineered safety features test cabinet (Reference 3), and

d. manual actuation circuits.

The engineered safety features actuation system consists of two discrete portions of circuitry: (1) an analog portion consisting of three or four redundant channels per parameter to monitor the reactor coolant system pressure, temperatures and flows, steamline pressure, and containment pressure; 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 redundant 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 in Drawing 108D685, Sheets 5, 6, 7, and 8. Tables 7.3-1 and 7.3-2 give additional information pertaining to logic and function.

The interlocks associated with the engineered safety features actuation system are outlined in Table 7.3-3. These interlocks satisfy the functional requirements discussed in Subsection 7.1.2.1.5.

Manual actuation is provided from the control board by operation of either redundant control for containment isolation Phase A and safety injection. Each control consists of two backup linked actuation switches. Manual controls are provided for activation of containment isolation Phase B by either of the two sets of controls.

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

7.3.1.1.1 Function Initiation

The specific functions which rely on the engineered safety features actuation system for initiation are:

a. A reactor trip, provided one has not already been generated by the reactor trip system.

b. Charging pumps, safety injection pumps, and residual heat removal pumps which provide borated emergency makeup water to the cold legs of the reactor coolant system following a loss-of-coolant accident.

c. Reactor containment fan coolers serve to cool the containment air and limit the potential for release of fission products from the containment by reducing the pressure following an accident.

d. Those pumps which serve as part of the ultimate heat sink and as part of the heat sink for containment cooling (e.g., essential service water, component cooling water pumps, and motor and diesel-driven auxiliary feedwater pumps serve as part of the ultimate heat sink).

e. Phase A containment isolation, whose function is to prevent fission product release by isolation of process lines which are not essential to reactor protection.

f. Steamline isolation to prevent the continuous, uncontrolled blowdown of more than one steam generator and thereby uncontrolled reactor coolant system cooldown.

g. Main feedwater line isolation as required to prevent or mitigate the effect of excessive cooldown.

h. Starting the emergency diesels to assure backup supply of power to emergency and supporting systems components.

i. Isolation of the appropriate control room intake ducts to meet control room occupancy requirements following a loss-of-coolant, HELB, or other design basis accidents.

j. Containment spray actuation which performs the following functions:

   1. Initiates containment spray to reduce containment pressure, temperature, and airborne iodine inventory following a loss-of-coolant or steamline break accident inside of containment.

2. Initiates Phase B containment isolation which isolates the containment on high containment pressure 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.

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 sensors monitoring the primary system are located as shown on the piping flow diagrams in Section 5.1. The secondary system sensor locations are shown on the steam system flow diagrams given in Section 10.3.

Containment pressure is sensed by four physically separated differential pressure transmitters mounted outside of the containment (which are connected to containment atmosphere by a filled and sealed hydraulic transmission system). The distance from penetration to transmitter is kept to a minimum, and separation is maintained. This arrangement, together with the pressure sensors external to the containment, forms a double barrier and conforms to GDC 56.

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 in Drawing 108D685, Sheet 2.

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 Subsection 7.3.2.2.5.

7.3.1.1.4 Final Actuation Circuit

The outputs of the solid-state logic protection system (the slave relays) are energized to actuate. These devices actuated by the slave relays are listed as follows:

a. Safety injection system pump and valve actuators (see Subsection 6.3.2).

b. Containment isolation (Phase A signal isolates all nonessential process lines on receipt of safety injection signal; Phase B signal isolates remaining process lines (which do not include safety injection lines) on receipt of 2/4 Hi 3 containment pressure signal. For further information, see Subsection 6.2.4.

c. Reactor containment fan coolers (see Subsection 6.2.2).

d. Essential service water pump and valve actuators (see Subsection 9.2.1).

e. Auxiliary feed pumps (see Subsection 10.4.9).

f. Emergency diesel-generators (see Subsection 8.3.1).

g. Feedwater isolation (see Subsection 10.4.7).

h. Ventilation isolation valve and damper actuators (see Subsection 6.4.2).

i. Steamline isolation valve actuators (see Subsection 10.3.3).

j. Containment spray pump and valve actuators (see Subsection 6.5.2).

If an accident is assumed to occur coincident with a loss of offsite power, the engineered safety features loads must be sequenced onto the diesel generators to prevent overloading them. This sequence is discussed in Subsection 8.3.1. The design meets the requirements of Criterion 35 of the GDC.

Engineered safety features equipment actuated by the reactor protection or engineered safety features actuation systems have output relays that are of the latch-type. Removal of the various isolating or actuating (input) signals due to use of a manual reset feature will not cause any of the associated safety-related equipment to change from its emergency mode. The design assures that, upon reset of the individual ESF actuation signal, all associated safety-related equipment remains in its emergency mode.

7.3.1.1.5 Support Systems

The following systems are required for support of the engineered safety features:

a. Essential service water - heat removal (see Subsection 9.2.1),

b. Component cooling water system - heat removal (see Subsection 9.2.2),

c. Electrical power distribution systems (see Section 8.3), and

d. Safety-related heating, ventilating, and air conditioning (HVAC) support system (see Section 6.4).

7.3.1.1.6 Auxiliary Feedwater System Operation

a. Auxiliary Feedwater Pumps

A control switch is provided for each pump on the main control board. A transfer switch (REMOTE, LOCAL) and a control switch are provided for each pump at the remote shutdown panel.

With the transfer switch in the REMOTE position, a pump will be started automatically by operation of the safeguard actuation relays or by the ATWS mitigation system relays (see Subsection 7.7.1.21). Manual starting of the pump from the main control board or the remote shutdown panel requires a contact closure from a pressure switch which monitors lube oil pressure. Automatic starting without this interlock can be accomplished without bearing damage (due to retention of an oil film on the bearings) provided that the pumps, or their auxiliary lube oil pumps, are started at least monthly.

A pump will be automatically stopped by any of the following:

1. operation of protective relaying or

2. low pump suction pressure.

Alarms are provided on the main control board to show pump automatic start, pump lube oil pressure low, and pump automatic stop. Turning its selector switch to the LOCAL position energizes a PUMP ON LOCAL CONTROL alarm on the main control board.

For manual starting of an auxiliary feedwater pump, operation of its control switch will start the auxiliary lube oil pump. A pressure switch will

serve as a permissive to operate the same control switch which will start the prime mover. Under automatic safeguards start conditions, the permissive is inoperative, and the prime mover is started at the same time that the auxiliary lube oil pump is energized.

Three chromel-constantan thermocouples are provided for each pump to measure bearing temperatures which are monitored by the computer.

An ammeter is provided on the main control board for the motor-operated pump to measure motor current.

A pressure gauge and transmitter indicate pump discharge pressure locally and remotely. A pressure switch is provided on each pump suction line to trip the pump and energize a low suction pressure alarm. At Byron, a second pressure switch is located upstream of the pump suction check valve and will inhibit the associated pump from starting if suction pressure from the condensate storage tank is inadequate and will energize an inhibit alarm.

A recirculation line is provided for each pump to assure minimum flow through the pump.

b. Diesel-Driven Auxiliary Feedwater Pump

The controls for the diesel-driven pump are similar to the controls for the motor-driven pump, except as noted in Subsection 10.4.9.5.1. A local annunciator for diesel trouble is provided with repeater alarms on the main control board. Refer to Subsection 10.4.9 for a description of the diesel drive.

c. Auxiliary Feedwater Pumps Suction Valves

Normal suction to the auxiliary feedwater pumps is from the condensate storage system through normally open manual valves. A backup source is available from the essential service water system through two normally closed motor-operated valves in series for each pump. These valves are controlled from the main control board.

The essential service water supply valves can be opened by the actuation of at least one-out-of-three safeguard initiation relays coincident with low pump suction pressure or by operator action. The valve can be closed provided that the low pump suction pressure relay is reset.

Limit switches on each valve are used to operate lights at the main control board indicating position.

d. Steam Generator Auxiliary Feedwater Stop Valves

A control switch is provided for each of the valves on the main control board. A transfer switch (REMOTE, LOCAL) and control switch are provided locally on the remote shutdown panel for each valve.

Turning the transfer switch to the LOCAL position energizes a VALVE ON LOCAL CONTROL alarm on the main control board.

Limit switches on each valve are used to operate lights at the main control board indicating valve position.

A failure analysis is provided in Table 10.4-3.

e. Auxiliary Feedwater Flow Control

A flow element, indicators, and transmitter are provided in each of the eight auxiliary feedwater supply lines. Each transmitter sends a flow signal to an indicator on the main control board (nominal accuracy is ± 5%) and on the remote shutdown panel, and to a flow switch which energizes a high flow alarm on the main control board.

Transfer switches (REMOTE, LOCAL) are provided on the remote shutdown panel. The auxiliary feedwater flow to the four steam generators is normally controlled from eight manual control stations mounted on the main control board if the transfer switch is in remote. Each manual control station electrically transmits a flow signal to an electric-to-pneumatic (E/P) converter. The pneumatic output flow signal is transmitted through a permissive three-way solenoid valve (which is deenergized for normal control) to the flow control valves.

An alarm on the main control board will be actuated if the manual control station for any of the eight flow control valves is set below 167.5 gpm while the associated auxiliary feedwater pump drive is not operating.

Going to local control transfers the pneumatic control at the flow control valves from the manual station on the main control board to a local controller mounted on the remote shutdown panel, and energizes a "Valve on Local Control" alarm at the manual control board.

The pneumatic control of the flow control valves from the remote shutdown panel is accomplished by direct valve position control with local flow indication for manually setting the flow.

A failure in the control system for the control valve will cause the valve to fail open. The failure analysis is provided in Table 10.4-4. If there is a loss of air to the air-operated valves in the auxiliary feedwater system, the valves will fail open and flow will be limited by the flow-limiting orifices in each supply line. The air-operated valves feature hand wheels for local isolation or throttling on loss of air. Flow control can also be accomplished by throttling the motor-operated valves.

Flow restricting devices are provided upstream of each flow control valve (Drawing M-37), in order to limit flow in the unlikely event of a pipe break.

f. Diverse Sources of Energy

Diverse sources of energy are provided for the auxiliary feedwater pumps, valve operators, instrumentation, and controls as discussed below.

Electrical equipment and cabling for both auxiliary feedwater pumps is physically separated into separate ESF trains.

One auxiliary feedwater pump per unit is motor driven. Its source of energy is 4-kV ESF bus 141 (241). The other auxiliary feedwater pump for each unit is direct diesel driven. Fuel oil is supplied from its own Category I day tank; all necessary electrical auxiliaries for the diesel-driven auxiliary feedwater pump are powered from its own battery system. The auxiliary feedwater pump diesel, its auxiliaries and appurtenances were evaluated to the same criteria under which the emergency diesel generators are evaluated.

The diesel-engine drives for the auxiliary feedwater pumps are equipped with electric starters, utilizing two sets of batteries for each engine. The system is complete with battery charging equipment. The auxiliary feedwater pump diesel is Seismic Category I and designed to Diesel Engine Manufacturers' Association Standards. This diesel is of such a size that it does not require external air starting or lubricating systems.

The electrical supply for the motor-operated valves and their controlling instrumentation is from the redundant ESF buses. A particular valve's bus assignment is the one associated with its

respective pump. Therefore, the pair of valves associated with each steam generator are powered from redundant ESF buses.

The air-operated valves are supplied from the instrument air system. The instrument air system is described in Subsection 9.3.1. The control instrumentation is supplied from the essential instrument power buses as described in Subsection 8.3.1.1. A particular valve's instrument bus assignment will have the same train designated as the ESF bus associated with the corresponding motor-operated valve and pump. Therefore, the pair of valves associated with each steam generator are powered from redundant instrument power buses.

7.3.1.1.7 Essential Service Water System Operation

There are two 100% capacity essential service water pumps associated with each unit. At Byron Unit 1 or Unit 2, one of the two water pumps takes suction from the essential service cooling tower OA while the other one takes suction from the essential service cooling tower OB. At Braidwood Unit 1 or Unit 2, both of the two water pumps take suction from the essential service water cooling pond. See Subsection 9.2.5 for detailed description. The two pumps in each unit are powered from separate independent ESF buses.

a. Essential Service Water Pump Control

A control switch is provided for each pump on the main control board.

A transfer switch (Remote, Local) and a control switch are provided on the remote shutdown panel for each pump.

1. The pump can be started manually provided that the pump suction valve and the RCFC inlet and outlet valves of the corresponding safety train are open.

The pump can be started automatically by a safety injection signal provided that the suction valve is open.

The pump can be stopped manually provided safeguards actuation relays are reset.

Protective relays will trip the motor breaker open on overcurrent conditions.

Low suction pressure at the pump will trip the pump off the line automatically and will sound a low suction pressure alarm on the main control board.

2. A pressure gauge and transmitter are provided in each pump discharge line for pressure indication locally and on the main control board.

3. An ammeter is provided on the main control board to display motor current.

4. Bearing temperatures for each pump and motor are sensed by thermocouples and monitored by the computer. Motor stator winding temperature is sensed by an RTD and monitored by the computer.

5. A main control board alarm is annunciated whenever the transfer switch on the remote shutdown panel is in the Local position. Placing the main control board control switch in PULL-TO-LOCK provides a signal to the ESF display system.

b. Essential Service Water Pump Suction Valves

One motor-operated suction valve is associated with each essential service water pump. The power source for the valve motor is a 480-Vac motor control center of the same ESF train associated with the corresponding pump.

A control switch is provided on the main board for each valve.

Limit switches on each valve provides valve position indication on the main control board.

c. Component Cooling Water Heat Exchanger Service Inlet Valve

Three heat exchangers are provided - one for each unit and one for common service (Unit 0). The Unit 1 and Unit 2 heat exchangers are each provided with a motor-operated inlet isolation valve. The Unit 0 heat exchanger has two parallel motor-operated inlet valves which allow taking suction from either Unit 1 or Unit 2 essential service water pump discharge header. A control switch is provided on the main control board for each valve.

Unit 1 and Unit 2 heat exchanger valves are powered from ESF Divisions 11 and 21 respectively (Train A). Unit 0 heat exchanger valves are powered from ESF Division 12 and 22 (Train B) to allow separation and independence of power sources.

Limit switches on each valve provide position indication at the main control room.

d. Component Cooling Water Heat Exchanger Service Water Outlet Valve

Each exchanger is provided with a motor-operated outlet isolation valve. Unit 1 and Unit 2 exchanger isolation valves are powered from ESF Divisions 11 and 21 respectively (Train A). The Unit 0 exchanger isolation valve is powered from ESF Division 12 (Train B).

These valves are normally maintained open. A local pushbutton control is provided to operate each valve.

e. Essential Service Water Return Header Cross-tie Valves (SX010, SX011, SX136)

These valves are provided for each unit and are used to direct service water return to the appropriate essential service water cooling tower at Byron and to the essential cooling pond at Braidwood.

Valves 1SX010 and 2SX010 which allow water to return to cooling tower OA (Byron) or the cooling pond (Braidwood) from Unit 1 and Unit 2 heat exchangers are powered from ESF Divisions 12 and 22, respectively.

Valves 1SX011 and 1SX136 (which allow water to return to cooling tower OB or from Units 1 and 2 heat exchangers) are powered from ESF Divisions 12 and 22, respectively. Valves 0SX146 and 0SX147 which return water from the common component cooling heat exchanger, are powered from Divisions 12 and 22, respectively. Therefore, with the 1A and 2A pumps normally aligned with the Unit 1 and Unit 2 component cooling heat exchangers, respectively, and with the cross tie valves normally open between the 1A and 1B, and 2A and 2B pump discharges, water can be diverted to the OB cooling tower in case a single failure occurs in Divisions 11 and 21.

A control switch is provided on the main control board for each valve.

Limit switches on each valve provide position indication at the main control board.

f. Essential Service Water Strainers

One strainer is provided in the discharge line of each essential service water pump. The differential pressure across each strainer is indicated locally. High differential pressure is alarmed on the main

control board annunciator and is used to initiate back flush of the strainers. At Byron, backflush of the strainers is initiated manually.

g. Essential Service Water Temperature Measurement

The water temperature of each pump discharge is displayed on the main control board and on the remote shutdown panel with high and low temperature alarms annunciated on the main control board.

h. Essential Service Water Cooling Tower Fans (Byron only)

Each tower is provided with four two speed fans. Two fans are driven from ESF bus 11 (or 12) and two fans are driven from ESF bus 21 (or 22) respectively for towers OA and OB. The following applies to each fan:

1. Two switches are provided on the main control board for the fan. One switch controls the high speed winding and one switch controls the low speed winding.

2. A control switch and a transfer switch are provided for the low speed winding on the remote shutdown panel. A local-control alarm is annunciated at the main control board whenever the transfer switch is placed in the Local position.

3. "b" contacts on each circuit breaker are used to prevent both high and low speed breakers from being closed at the same time.

4. The service water riser valve in the corresponding cooling tower section must be fully open in order to start the fan.

### 7.3.1.1.8 Auxiliary Building HVAC System Instrumentation and Controls

#### 7.3.1.1.8.1 System Identification

The instrumentation and controls for the auxiliary building HVAC system function to ensure heating, ventilating and air conditioning of the auxiliary building under all station operating conditions is as described in Subsection 9.4.5. The design bases for the instrumentation and controls are described in Subsection 7.3.1.1.8.4.

7.3.1.1.8.2 Identification of Safety Criteria

7.3.1.1.8.2.1 Safety Design Bases

a. The auxiliary building charcoal booster fans are manually started by a control switch upon detection of high radiation. The fans are started automatically on a safety injection signal. The fuel handling building charcoal booster fan starts automatically on detection of high radiation signal or a safety injection signal.

b. The instrumentation detects products of combustion present in the auxiliary building supply air ducts and exhaust air ducts, and annunciates on the local control panel.

c. No single failure, maintenance, calibration, or test operation of the control system on a channel, module or system level prevents the functioning of the auxiliary building HVAC system.

d. Loss of offsite electric power does not affect the normal functioning of the controls and instrumentation, since they are supplied from ESF buses.

e. The physical events accompanying a loss-of-coolant or fuel handling accident do not prevent correct functioning of the controls and instrumentation.

f. Seismic motions resulting from earthquake ground motion, missile, wind, and flood do not prevent correct functioning of the controls and instrumentation.

g. The requirements of IEEE Standards 279-1971, 308-1971, 323-1974, 336-1985, 344-1972, and 420-1973 are met by the HVAC instrumentation and controls. Additionally, General Design Criteria 13, 20, 21, 22, 23, 24, and 29 of 10 CFR 50 Appendix A, have been implemented in the design of the control system.

7.3.1.1.8.2.2 Power Generation Design Basis

Provide capability in the main control room to control and operate various components of the auxiliary building HVAC system.

7.3.1.1.8.2.3 Indication and Annunciation

7.3.1.1.8.2.3.1 Indication

a. outside air temperature,

b. supply air temperature,

c. exhaust air temperature,

d. auxiliary building to atmosphere differential pressure,

e. isolation damper position.

7.3.1.1.8.2.3.2 Alarms

Auxiliary building operating conditions which are annunciated on the main control board and which require operator attention are:

a. low building temperature,

b. high building temperature,

c. high or low differential pressure across supply fans,

d. high or low differential pressure across exhaust fans,

e. high or low air flow in charcoal booster fans,

f. low differential building pressure,

g. high differential building pressure,

h. fan motor trip,

i. filter plenum high differential pressure,

j. high relative humidity in fuel handling building exhaust plenum, and

k. high temperature in safety-related pump cubicles.

7.3.1.1.8.3 System Description

7.3.1.1.8.3.1 Power Supply

The auxiliary building cubicle coolers and associated instrumentation and control for ESF equipment rooms such as RHR pumps, SI pumps, etc., are powered from the same division of power as the equipment they are serving. On loss of cooling as a result of any postulated I&C failure serving the equipment of one power division, the redundant string of equipment associated with the redundant power division is started. Control power for the main auxiliary building HVAC control system is supplied from the bus that powers the corresponding equipment.

7.3.1.1.8.3.2 Initiating Circuits, Logic, and Sequencing

Components of the auxiliary building HVAC system are controlled as follows:

a. The supply and exhaust fans are controlled by switches provided on local control panels and in the control room.

b. The auxiliary building charcoal booster fans are controlled by control switches provided on local control panels and in the control room, and started manually upon detection of high radiation. The fans start automatically on a safety injection signal. The fuel handling building charcoal booster fans are started automatically upon detection of high radiation or a safety injection signal.

c. The hot water heating coils and booster pumps are controlled automatically and are not required to perform a safety function.

d. The auxiliary building non-accessible areas exhaust filter plenum isolation dampers are opened and closed manually by control switches provided in the control room. Two-out-of-three filter plenums will be used during both normal and abnormal plant operating conditions. Plenum selection is an operator function. For further information, see Subsection 6.5.1.

e. The fuel handling building exhaust isolation dampers are operated by control switches provided on the main HVAC control panel. One-of-two filter banks are required for filtering all the fuel handling building exhaust air. Selection is an operator function.

f. The pump cubicle coolers are manually initiated by local control switches and automatically on startup of the associated pumps and high temperature signal from the cubicle temperature switches.

7.3.1.1.8.3.3 Bypasses and Interlocks

a. The plenum bypass and dampers are interlocked to bypass air around the charcoal absorbers and downstream HEPA filters when charcoal filtration is not required.

b. The auxiliary building charcoal booster fans are started automatically on a safety injection signal. The fuel handling building charcoal booster fans are started automatically upon detection of high radiation or a safety injection signal.

c. Each charcoal booster fan is interlocked with its respective charcoal filter fire protection deluge valve to trip when valve is opened.

7.3.1.1.8.3.4 Redundancy/Diversity

The auxiliary building HVAC system consists of redundant equipment having independent controls and instrumentation.

7.3.1.1.8.3.5 Separation

The channels and logic circuits are physically and electrically separated to preclude the possibility that a single event will prevent operation of the auxiliary building HVAC system.

7.3.1.1.8.3.6 Testability

Means have been provided for checking the operational availability of the auxiliary building HVAC system separately at sensor module and control channel levels and jointly as a complete system during operation or shutdown periods.

7.3.1.1.8.3.7 System Drawings

The drawings provided for the auxiliary building HVAC system are as follows:

a. Piping and Installation Diagrams M-95, Sheets 1 through 16 and

b. The Control and Instrument Details and Drawing M-2095, Sheets 1 through 22.

7.3.1.1.8.3.8 Environmental Considerations

Temperature, pressure, humidity, and radiation dosage are considered in the selection of various instruments, controls and devices for the auxiliary building HVAC system. These are described in Section 9.4.

7.3.1.1.8.3.9 Operational Considerations

The system is designed to operate during both normal and abnormal station operating conditions. The automatic circuitry is designed to start the emergency equipment if the signal for its initiation is received as described in Section 9.4.

7.3.1.1.8.4 Design-Bases Information

IEEE Standard 279-1971 defines the requirements for design bases. See Subsection 7.3.2.2.8 for a discussion of this standard.

The generating station condition which requires protective action for startup of the nonaccessible area exhaust filter plenum charcoal booster fans is a high level of radiation.

7.3.1.1.9 Main Control Room Heating, Ventilation, and Air Conditioning Instrumentation Controls

7.3.1.1.9.1 System Identification

The main control room heating, ventilating and air conditioning instrumentation and control system senses abnormal radiation and ionization levels in the control room outside air intake, and initiates rerouting of the circulating air. It also senses abnormal pressure in the control room turbine building intake, and ensures that intake remains closed in the event of a HELB in the turbine building. It also senses abnormal pressure in the control room and initiates the appropriate alarm. There is also a low supply fan suction temperature alarm. The design bases for the instrumentation and controls are described in Subsection 7.3.1.1.9.4.

7.3.1.1.9.2 Identification of Safety Criteria

The main control room heating, ventilating, and air-conditioning system is described in Section 9.4. The instrumentation and controls for this system meet the following design bases.

7.3.1.1.9.2.1 Safety Design-Bases

a. (Braidwood only) The system has the provision for manual isolation upon the notification of an offsite chlorine accident, and is then operated on 100% recirculated air.

b. The system controls are interlocked with the outside air radiation monitoring system and the turbine building HELB pressure monitoring system to automatically transfer the makeup air supply to the turbine building (unless abnormal pressure is detected at the turbine building intake) through one of the emergency filter trains to maintain control room habitability. In the event of a HELB in the turbine building, the turbine building intake is maintained closed to prevent excessive moisture from entering the control room, and makeup air from the outside air bypass line intake is routed through one of the emergency filter trains.

c. The system operates in conjunction with ionization detection of combustion products in the control room air return ducts and outside air intakes.

d. The system is capable of manual purging of the control room with 100% outside air or of manual routing of the outside air-return air mixture from the control room through the normally bypassed recirculation charcoal filters.

e. No single failure, maintenance, calibration, or test

operation prevents the functioning of the control room HVAC system controls and instrumentation.

f. Loss of offsite electric power does not affect the normal functioning of controls and instrumentation, since they are supplied from ESF buses.

g. The physical events accompanying a loss-of-coolant, fuel handling accident, or HELB, do not prevent correct functioning of the controls and instrumentation.

h. Seismic motions resulting from earthquake ground motion, missile, wind, and flood do not impair the operation of the controls and instrumentation.

i. The requirements IEEE 279, 308, 323, 336 and 344 are met by the control room HVAC system instrumentation and controls. Additionally, General Design Criteria 13, 19, 20, through 24, and 29 of 10 CFR 50 Appendix A, have been implemented in the design of this control system.

7.3.1.1.9.2.2 Power Generation Design-Bases

Control the temperature and humidity inside the control room within 75°F ± 2°F and 40% relative humidity ± 5% and maintain the control room at least at a 1/8-inch positive pressure with respect to adjacent areas. Control the temperature inside the upper cable spreading rooms to a maximum of 90°F and HVAC equipment rooms to a maximum of 104°F.

7.3.1.1.9.2.3 Indication and Annunciation

7.3.1.1.9.2.3.1 Indication

Indicate temperatures, humidity, and status of operating equipment, i.e., supply and return air fans, refrigeration unit, etc., on the main control board.

7.3.1.1.9.2.3.2 Annunciation

Annunciate on the main control board any operating transient that requires operator attention. This includes low supply fan suction temperature, high or low differential pressure across supply and return air fans, loss of refrigeration unit, high pressure drop across the supply air filters, low-positive pressure differential between control room envelope and adjacent areas, and high or low airflow from makeup filter unit fans.

7.3.1.1.9.3 System Description - Main Control Room HVAC Control System

The controls and instrumentation for the control room HVAC system function to ensure the habitability of the control room under all station operating conditions, as described in Sections 6.4 and 9.4. The design bases for the control and instrumentation are described in Subsection 7.3.1.1.9.2.

7.3.1.1.9.3.1 Power Supply

Power supply for instrument, control, power, and related systems for each control room HVAC system is fed from separate ESF buses.

7.3.1.1.9.3.2 Initiating Circuits, Logic, and Sequencing

Various components of each redundant control room HVAC system are controlled as follows:

a. The supply and return air fans are controlled by switches provided on local panels and the HVAC control panel.

b. The refrigeration unit is provided with an OFF/ON selector switch on its local panel and a STOP/START switch on the main control board. While in start mode, the refrigeration unit is initiated by the demand signal from the thermostat installed downstream of the cooling coil.

c. On any equipment malfunction alarm on the main control board, the redundant HVAC system is manually started.

d. The process radiation system detects high radiation signal in either of the two outside air intakes and takes the following simultaneous actions:

   1. Alarms the high radiation levels in the affected intake in the main control room.

   2. Closes the normal path of makeup air supply to the control room HVAC system.

   3. Causes makeup air from the turbine building to be routed through the appropriate standby makeup filter train, unless abnormal pressure is detected at the turbine building intake. In the event of a HELB in the turbine building, the turbine building intake is maintained closed to prevent excessive moisture from entering the control room, and makeup air from the outside air bypass line intake is routed through the appropriate standby makeup filter train.

   4. Aligns recirculation filter bypass and isolation dampers to allow airflow through filters.

   5. (Braidwood only) Shuts down the radwaste exhaust filter units, the laboratory HVAC system, and the control room office HVAC system.

e. On detection of combustion products in the control room by the ionization detection system, an alarm is annunciated in the main control room and the system's supply air is routed through the normally bypassed recirculation filters. In addition, if the quality of outside air is proper, the operator can open the maximum outside air intake dampers and the exhaust damper and

close the recirculation air damper for purging the control room air. At Braidwood, the maximum outside air intake and exhaust dampers are blocked in the closed position via a bolted configuration. The blocks can be removed and the dampers can be opened manually should a purge of the main control room air be required.

f. (Braidwood only) Control switches are provided on the local control panels to allow manual isolation of the control room HVAC system and initiate 100% air recirculation upon notification of an offsite chlorine accident. The following simultaneous events occur when manual isolation is initiated:

1. alarm on the main control board,

2. closure of all dampers in the outside air intakes for the control room HVAC system,

3. recirculation of the room air through the recirculation filter,

4. trip of the emergency make-up filter unit fan (if operating),

5. isolation of the computer rooms from the control room offices' HVAC system.

7.3.1.1.9.3.3 Bypass and Interlocks

All of the isolation dampers in each control room HVAC system equipment strings are interlocked with the operation of corresponding supply air and return air fans. Operation of any one of these fans opens the corresponding isolation dampers. The supply and return air fans are started manually.

Zone electric heaters are modulated by temperature controllers with sensors located in the rooms and are interlocked with their respective air flow and thermal cutout switches to guard against overheating.

The operation of the standby makeup air filter trains is interlocked with the process radiation monitor in the outside air intakes.

The electric heating coils for humidity control in the standby makeup air filter trains are interlocked with the corresponding standby makeup air fans.

7.3.1.1.9.3.4 Redundancy/Diversity

Instrumentation and controls for each control room HVAC system are completely independent of each other.

7.3.1.1.9.3.5 Separation

The channels and logic circuits are physically and electrically separated to preclude the possibility that a single event will prevent operation of control room HVAC system.

7.3.1.1.9.3.6 Testability

Instruments used for the control and logic circuitry for the control room HVAC system can be individually checked on sensor, module, channel and system levels by simulating sensing conditions such as temperature, pressure, humidity, and combustion products to test or calibrate the sensors and observing trip or control responses.

7.3.1.1.9.3.7 System Drawings

The drawings provided for the control room HVAC system are as follows:

Piping and Instrumentation Diagrams on Drawing M-96.

7.3.1.1.9.3.8 Environmental Considerations

Temperature, pressure, humidity, and radiation dosage are considered in selection of various equipment, instrumentation, and controls for the control room HVAC system. These are described in detail in Sections 3.11 and 9.4.

7.3.1.1.9.3.9 Operational Considerations

The automatic circuitry is designed to start the emergency equipment, if the signal for its initiation is received, as described in this section. Provisions are made to allow manual control and operation of the various components of the control room HVAC system from the main control room. At Braidwood, purging the main control room air can be initiated after the maximum outside air intake and exhaust dampers are opened manually.

7.3.1.1.9.4 Design-Bases Information

IEEE Standard 279-1971 requirements are discussed in Subsection 7.3.2.2.9.

7.3.1.1.9.4.1 Outdoor Air Intake Radiation Protection Portion of Control Room HVAC System

a. Outdoor air intake is monitored for high radiation levels. Two monitoring channels per intake are used. The radioactivity levels are sensed by monitors upstream of intake isolation dampers, where the air enters the intake louvers. If high radiation level is detected, the makeup air shifts to the turbine building for supply, unless abnormal pressure is detected at the turbine building intake.

b. For operational and protective limits of the radiation monitor, see Table 11.5-1.

c. Normal operating levels are expected to be in the range of <0.5 mR/hr.

d. The power supply is described in Subsection 8.3.1. The range of environmental conditions to which the radiation monitors are subjected is the same as the extreme outdoor conditions. These components are protected from direct rain impingement and are specified and qualified for a range of from -10°F to 120°F dry bulb temperature and relative humidities ranging from 5% to 90%.

e. Design provisions for earthquake, abnormal environmental conditions, and flood protection have been incorporated to retain necessary protective action.

7.3.1.1.9.4.2 Turbine Building Intake HELB Pressure Protection Portion of Control Room HVAC System

a. The turbine building intake is monitored for high pressure. Three (3) monitoring channels per intake are used in a 2 out of 3 logic. If high pressure is detected, the turbine building supply damper is maintained closed and makeup is via a bypass damper from the outside air.

b. The power supply is from an uninterruptible source (120VAC Instrument Buses 1IP01J and 1IP04J) to enable detection of a HELB with a concurrent loss of offsite power.

c. Design provisions for earthquake, abnormal environmental conditions, and flood protection have been incorporated to retain the necessary protective action.

7.3.1.1.9.4.3 Outdoor Air Intake Chlorine Protection Portion of Control Room HVAC System (Braidwood only)

Upon notification of an offsite chlorine accident, the control room HVAC system is manually isolated and is then operated with 100% recirculated air through the recirculation filter.

7.3.1.1.9.4.4 Ionization Detection Portion of Control Room HVAC System

a. Ceiling-mounted detectors are uniformly distributed to provide full detection coverage of each room. Half of the detectors in each room are powered from one ESF bus and the other half from the other ESF bus. The ionization detection system is not safety-related but is seismically supported.

   Duct-mounted ionization detectors are located in each main return air duct connected to the main control boards.

b. The ionization level is expected to be 0 particles per $cm^3$. Ionization levels which are more than 200,000 particles per $cm^3$ are considered hazardous to control room occupancy. The ionization level which will cause protective action is approximately 100,000 particles per $cm^3$.

c. The electrical supply system is described in Section 8.3. The range of environmental conditions to which the ionization detectors are subjected is the same as the main control room as listed in Table 3.11-2.

#### 7.3.1.1.10 Diesel-Generator Room Ventilation System Instrumentation and Controls

##### 7.3.1.1.10.1 System Identification

The instrumentation and controls of the diesel-generator ventilation system are designed to (1) provide ventilation in the diesel-generator rooms and limit the maximum ambient temperature therein to 132°F, (2) provide ventilation in the oil storage room and limit the maximum ambient temperature to 132°F, and (3) provide ventilation in the oil day tank room.

The diesel-generator ventilation system is described in detail in Subsection 9.4.5.2.

##### 7.3.1.1.10.2 Identification of Safety Criteria

The instrumentation and controls for this system meet the following design bases.

###### 7.3.1.1.10.2.1 Safety Design-Bases

a. The system prevents accumulation of diesel oil fumes in various areas of the diesel-generator facility.

b. Loss of offsite electric power does not affect the normal functioning of controls and instrumentation since they are supplied from ESF buses.

c. The physical events accompanying a loss-of-coolant or fuel handling accident do not prevent correct functioning of the controls and instrumentation.

d. Seismic motions resulting from earthquake ground motion, missile, wind, and flood do not impair the operation of the controls and instrumentation.

e. The requirements of IEEE Standards 279-1971, 308-1971, 323-1974, 336-1985, 344-1972, 420-1973 are met by the diesel-generator room ventilation system instrumentation and controls. Additionally, General Design Criteria 13, 19, 21, 22, 23, and 29 of 10 CFR 50 Appendix A, have been implemented in the design of the control system.

###### 7.3.1.1.10.2.2 Power Generation Bases

a. Limit the maximum ambient temperature to 132°F in the diesel-generator rooms and the oil storage rooms.

b. Provide capability in the main control room to control and operate various components of the

diesel-generator room ventilation system manually from the main control room.

7.3.1.1.10.2.3 Indication and Annunciation

7.3.1.1.10.2.3.1 Indication

a. Diesel-generator vent supply fan status-indicated on the HVAC main control panel (MCP).

b. Mixed air temperature-indicated on the local control panel (LCP).

c. Diesel-generator room air temperature-indicated on the LCP.

d. Differential pressure across the diesel-generator vent supply fan-indicated on the LCP.

e. Diesel oil storage room exhaust fan status i.e., on, tripped, or off-indicated on the LCP.

f. Diesel oil storage room high room temperature-indicated on the LCP.

g. Differential pressure across the diesel generator exhaust fan and the diesel-generator oil storage room exhaust fan-indicated on the LCP.

h. Diesel-generator exhaust air fan status-indicated on the LCP.

7.3.1.1.10.2.3.2 Annunciation

a. High diesel-generator room temperature-indicated on the MCP.

b. Low and high differential pressure across the diesel-generator supply fan indicated on the MCP. Diesel generator exhaust and diesel oil storage exhaust fan high and low $\Delta P$-indicated on the LCP.

c. Low diesel-generator room temperature-indicated on the MCP (Byron only).

   Low diesel-generator vent supply fan discharge temperature-indicated on the MCP (Braidwood only).

d. Diesel-generator vent supply fan overload trip-indicated on the MCP.

e. High diesel oil storage room temperature-indicated on the MCP.

f. Diesel oil storage room exhaust fan and diesel generator exhaust fan overload trip-indicated on the LCP.

g. Fan auto restart disabled indicated on the LCP.

7.3.1.1.10.3 System Description

7.3.1.1.10.3.1 Power Supply

The HVAC system and associated instrumentation and controls for ESF equipment rooms, such as diesel generators, are powered from the same division of power as the equipment they are serving.

7.3.1.1.10.3.2 Initiating Circuits, Logic, and Sequencing

The instrument and control systems are described as follows:

a. Diesel-generator supply fans are started (1) manually by independent control switches provided on the HVAC main control panel (MCP) in the main control room, or (2) automatically by the diesel-generator start sequence, (3) one automatic restart after a high differential pressure trip signal, or (4) automatically by a Diesel-Generator Room High Temperature signal.

b. The diesel-generator supply fans are stopped (1) manually by the same control switches on the MCP, or (2) automatically on receipt of (a) trip signal from the diesel generator and temperature below temperature switch setpoint, or (b) signal from ionization detector located downstream of the fans, or (c) high differential pressure across the fans. The fans will trip, then will attempt one automatic restart following a time delay after they tripped.

c. Diesel oil storage room exhaust fans are started from the local control panel.

d. Diesel oil storage room exhaust fans are stopped (1) manually by the same control switches on the local control panel, or (2) automatically on receipt of (a) high differential pressure signal, or (b) fire protection signal from the ionization detector located upstream of the fans, or (c) High Temperature signal in the DOST Room ventilation duct work.

e. A temperature controller modulates the supply and return air dampers to maintain the mixed air temperature.

7.3.1.1.10.3.3 Bypasses and Interlocks

a. The diesel-generator auto interlock used to start and stop the ventilation fan is bypassed by the manual start/ stop and/or pull-to-lock position of the control switch. Outside air intake and return air dampers are interlocked to modulate on fan discharge temperature.

7.3.1.1.10.3.4 Redundancy/Diversity

Instruments and controls are not redundant for the diesel-generator room ventilation system, since redundant diesel generators are provided.

7.3.1.1.10.3.5 Separation

The channels and logic circuits of each diesel-generator room ventilation system are physically and electrically separated to preclude the possibility that a single event at one diesel-generator room ventilation system will prevent operation of the other system.

7.3.1.1.10.3.6 Testability

Means have been provided for checking the operational availability of complete diesel generator ventilation control systems separately at sensor module and control channel basis and jointly as a complete system during the diesel operation or shutdown period.

7.3.1.1.10.3.7 System Drawings

The drawings provided for the diesel-generator ventilation control systems are as follows:

a. Piping and instrumentation diagrams, Drawings M-97 and M-98.

b. Logic diagrams.

7.3.1.1.10.3.8 Environmental Considerations

Temperature, pressure, humidity, and radiation dosage are considered in the selection of various instruments, controls, and devices for the diesel-generator room ventilation system. These are described in detail in Section 9.4.

7.3.1.1.10.3.9 Operational Considerations

The diesel-generator room ventilation system is required during abnormal station operating conditions. Diesel oil storage room ventilation system is provided during both normal and abnormal station operation conditions. Diesel oil storage room ventilation system is designed to stop the motive force to draw in HELB air upon detection of a HELB signal in the Turbine Building near the HVAC intake location for the room. The automatic circuitry is designed to start the emergency equipment as described in Section 9.4.

7.3.1.1.10.3.10 Supporting Systems

Foam-water and $CO_2$ fire protection systems have been provided to serve various areas of the diesel-generator facility.

7.3.1.1.10.4 Design Bases Information

The generating station condition which requires the diesel-generator ventilation and its associated control systems to activate is the loss of offsite power.

IEEE Standard 279-1971 requirements are discussed in Subsection 7.3.2.2.10.

7.3.1.1.11 Essential Switchgear Rooms, Miscellaneous Electrical Equipment Rooms and Battery Rooms Ventilation Systems Instrumentation and Controls

7.3.1.1.11.1 System Identification

The controls and instrumentation for ventilation systems serving four ESF switchgear rooms (Divisions 11, 12, 21, and 22), two cable spreading rooms, four miscellaneous electrical equipment rooms (Divisions 11, 12, 21, and 22), four cooling tower electric substations (Buses 1213, 1322, 2317, and 2322) and four battery rooms (Divisions 11, 12, 21, and 22) function to ensure the following:

a. The outside and return air is mixed, drawn through high efficiency filters and introduced into the rooms.

b. Maximum room ambient temperature is limited to 108°F.

c. Minimum room ambient temperature is limited to 65°F.

d. Room air from switchgear rooms, cable spreading rooms, and miscellaneous electrical equipment rooms is relieved to the turbine building.

e. Room air from cooling tower electrical substations is relieved to the outdoors (Byron only).

f. Room air from battery rooms is exhausted to the turbine building.

Each of the ESF switchgear rooms (Divisions 12 and 22), cable spreading rooms (Divisions 12 and 22), Byron cooling tower electrical substation rooms (Divisions 1317, 1322, 2317, and 2322) are served by an independent ventilation system and associated instrumentation and controls. ESF switchgear room (Division 11), miscellaneous electrical equipment room (Division 11) and battery room (111) together are served by one independent ventilation system and associated instrumentation and controls. ESF switchgear room (Division 21), miscellaneous electrical equipment room (Division 21) and battery room (211) together are served by one independent ventilation system and associated instrumentation and controls. Miscellaneous electrical equipment room (Division 12) and battery room (112) together are served by one independent ventilation system and

associated instrumentation and controls. Miscellaneous electrical equipment room (Division 22) and battery room (212) together are served by one independent ventilation system and associated instrumentation and controls. Cable spreading rooms (Divisions 12 and 22) are served by two independent ventilation systems and associated instrumentation and controls.

The instrument and control systems are designed to meet the requirements of Safety Category I. The ventilation systems are described in Subsection 9.4.5.

7.3.1.1.11.2 Identification of Safety Criteria

The instrumentation and controls for these systems meet the following design bases.

7.3.1.1.11.2.1 Safety Design-Bases

a. Each ESF switchgear room, cable spreading room, miscellaneous electrical equipment room, cooling tower electrical substation room ventilation system (Byron only) removes heat generated from electrical equipment located in the respective areas.

b. Battery room ventilation system prevents accumulation of hydrogen gas generated during charging of batteries.

c. Loss of offsite electric power does not affect the normal functioning of controls and instrumentation.

d. The physical events accompanying a loss-of-coolant or fuel handling accident do not prevent correct functioning of the controls and instrumentation since they are fed from ESF buses.

e. Seismic motions resulting from earthquake ground motion, missiles, wind, and flood do not impair the operation of the controls and instrumentation.

f. The requirements of IEEE Standards 279-1971, 308-1971, 323-1974, 336-1985, 344-1972, 420-1973 are met by the ventilation systems instrumentation and controls identified in Subsection 7.3.1.1.11.1. Additionally, General Design Criteria 13, 19, 21, 22, 23, and 29 of 10 CFR 50 Appendix A, have been implemented in the design of these control systems.

7.3.1.1.11.2.2 Power Generation Bases

a. Limit the maximum ambient temperature to 108°F in the areas served by the ventilation systems identified in Subsection 7.3.1.1.11.1.

b. Provide capability to control these ventilation systems from the main control room.

7.3.1.1.11.2.3 Indication and Annunciation

7.3.1.1.11.2.3.1 Indication

a. Ventilation fan status-indicated on the MCP and LCP,

b. Exhaust fan status-indicated on the LCP,

c. Differential pressure across the ventilation fan-indicated on the LCP,

d. Differential pressure across the exhaust fan-indicated on the LCP (except for Divisions 12 and 22 miscellaneous equipment room exhaust fans VE05C, and Division 11 and 21 miscellaneous electric equipment room fans VE04C) At Braidwood, VE05C and VE04C have locally mounted gauges.

e. Room air temperature-indicated on the LCP, and

f. Ionization detection system override-indicated on the LCP.

7.3.1.1.11.2.3.2 Annunciation

a. High differential pressure across the ventilation and exhaust fans-indicated on the LCP,

b. High room temperature-indicated on the MCP,

c. Ventilation fans motor trip-indicated on the LCP,

d. Loss of control power-indicated on the LCP,

e. Ionization detection override and trouble-indicated on the LCP,

f. Any alarm on the LCP will cause an alarm on the MCP indicating trouble-indicated on the LCP,

g. Low room temperature for the miscellaneous electric equipment rooms Division 12 and 22-indicated on the LCP, and

h. Ionization detection-indicated on the LCP, and

i. Fan auto restart disabled indicated on the LCP.

7.3.1.1.11.3 System Description

7.3.1.1.11.3.1 Power Supply

The HVAC system and associated instrumentation and controls for the ESF switchgear and miscellaneous equipment rooms are powered from the same division of power as the equipment they are serving.

7.3.1.1.11.3.2 Initiating Circuits, Logic, and Sequencing

The instrument and control systems are initiated as described below:

a. Ventilation fans are controlled from either the main control panel or the local control panel. A remote local selector switch is provided on the local control panel for the ventilation fans.

b. A temperature controller modulates the outside air and return air dampers.

7.3.1.1.11.3.3 Bypasses and Interlocks

a. Outside air and return air dampers are interlocked to energize when running the ventilation fan.

b. Ventilation fan is interlocked with ionization detection system to stop on a signal from ionization detector located downstream of the fan. This interlock may be bypassed by the purge switch provided on the local control panel.

c. Ventilation fan is interlocked to stop on a signal from the high differential pressure switch mounted across the fan. There will be one automatic restart attempted, then all further fan start attempts will be blocked until the interlock is manually reset by operation of the fan control switch at the LCP. The high differential pressure trip interlocks do not apply to battery room exhaust fans 1VE02C, 1VE03C, 2VE02C, and 2VE03C.

7.3.1.1.11.3.4 Redundancy/Diversity

No redundant instruments and controls are provided since each of the ventilation systems identified herein is a redundant system.

7.3.1.1.11.3.5 Separation

The channels and logic circuits of each redundant ventilation system are physically and electrically separated to preclude the possibility that a single event at one ventilation system will prevent operation of the other system.

7.3.1.1.11.3.6 Testability

Means have been provided for checking the operational availability of complete ventilation control systems identified in Subsection 7.3.1.1.11.1 separately at sensor module and control

channel basis and jointly as a complete system during the ventilation system operation or shutdown period.

7.3.1.1.11.3.7 System Drawings

The drawings provided for ventilation control systems hereby identified are as follows:

a. Piping and instrumentation diagrams Drawings M-115, M-116 and M-119, and

b. Control and instrument details, Drawing M-2116, Sheets 1 through 10.

7.3.1.1.11.3.8 Environmental Considerations

Temperature, pressure, humidity, and radiation dosage are considered in the selection of various instruments, controls, and devices for the ventilation system identified in Subsection 7.3.1.1.11.1. These are described in detail in Section 3.11 and Section 9.4.

7.3.1.1.11.3.9 Operational Considerations

Each ESF switchgear room, cable spreading room, miscellaneous electrical equipment room, cooling tower electrical substation room and battery room ventilation system is operated as required to maintain acceptable environmental conditions in the affected areas.

7.3.1.1.11.4 Design Bases Information

No generation station condition affects the operation of any of the ventilation systems identified in Section 9.4. IEEE Standard 279-1971 requirements are discussed in Subsection 7.3.2.2.1.

7.3.1.1.12 Reactor Containment Fan Coolers Instrumentation and Controls

7.3.1.1.12.1 System Identification

The instrumentation and controls for the reactor containment fan coolers (RCFC) function to ensure the removal of heat from the containment under all station operating conditions as described in Section 9.4.

7.3.1.1.12.2 Identification of Safety Criteria

7.3.1.1.12.2.1 Safety Design-Bases

a. The system controls are interlocked with the ESF system to automatically begin low speed operation on an ESF actuation signal.

b. No single failure, maintenance, calibration, or test operation of the control system on a channel module, or system level prevents the functioning of the RCFC units.

c. Loss of offsite electric power does not affect the normal functioning of the controls and instrumentation since they are supplied from ESF buses.

d. The physical events accompanying a loss-of-coolant or fuel handling accident do not prevent correct functioning of the controls and instrumentation.

e. Seismic motions resulting from earthquake ground motion, missile, wind, and flood do not prevent correct functioning of the controls and instrumentation.

f. The requirements of IEEE Standards 279-1971, 308-1971, 323-1974, 336-1985, 344-1972, and 420-1973 are met by the instrumentation and controls. Additionally, General Design Criteria 13, 21, 22, 23, 24, and 29 of 10 CFR 50 Appendix A, have been implemented in the design of the control system.

7.3.1.1.12.2.2 Power Generation Bases

Provide capability to control the RCFC units from the main control room.

7.3.1.1.12.2.3 Indication and Alarms

7.3.1.1.12.2.3.1 Indication

a. RCFC fan motor amperage is indicated on main control board.

b. RCFC fan motor stator temperature is monitored by the computer.

c. Inlet and outlet temperature are indicated on the main control board.

d. Inlet temperature is monitored by the computer.

e. Status of the RCFC fans is indicated on the main control board.

7.3.1.1.12.2.3.2 Alarms

The conditions annunciated on the main control board are as follows:

a. low outlet temperature, and

b. fan motor trip.

7.3.1.1.12.3 System Description

7.3.1.1.12.3.1 Power Supply

Control power for the instrumentation and controls comes from the same ESF bus that powers the reactor containment fan coolers.

7.3.1.1.12.3.2 Initiating Circuits, Logic, and Sequencing

a. The RCFC units are controlled from either control switches provided on the main control board or the remote shutdown control panel.

b. The speed of the units is reduced automatically from high speed to low speed upon ESF actuation.

7.3.1.1.12.3.3 Bypasses and Interlocks

The RCFC fans are interlocked to annunciate on high vibration of the fan housing.

7.3.1.1.12.3.4 Redundancy/Diversity

The RCFC units consist of redundant equipment having independent controls and instrumentation.

7.3.1.1.12.3.5 Separation

The channels and logic circuits are physically and electrically separated to preclude the possibility that a single event will prevent operation of the RCFC units.

7.3.1.1.12.3.6 Testability

Means have been provided for checking the operational availability of the RCFC units separately at sensor module and control and channel basis and jointly as a complete system during operation or shutdown periods.

7.3.1.1.12.3.7 System Drawings

The drawings provided for the RCFC units are as follows:

a. Piping and instrument diagrams, Drawings M-102 and M-104; and

b. Control and instrument details, Drawing M-2104.

7.3.1.1.12.3.8 Environmental Considerations

Temperature, pressure, humidity, and radiation dosage are considered in the selection of various instruments, controls and devices for the RCFC units. These are described in detail in Sections 3.11 and 9.4.

7.3.1.1.12.3.9 Operational Considerations

The RCFC is required during both normal and abnormal station operating conditions. The automatic circuitry is designed to start the emergency equipment as described in Section 9.4.

7.3.1.1.12.4 Design Basis

The generating station condition which requires the RCFC units to activate is the ESF actuation signal.

IEEE Standard 279-1971 requirements are discussed in Subsection 7.3.2.2.12.

7.3.1.1.13 Containment Spray System Operation

Containment spray system component description and design information are presented in Subsection 6.5.2. Only instrumentation and controls and their operation are described in this subsection.

a. Containment Spray Pumps

A control and test transfer switch is provided for each pump on the main control board.

Each containment spray pump can be started under any the following three conditions:

1. Automatically: A containment spray actuation (Hi-3) signal from the ESF actuation system (ESFAS) logic will start the pump, provided that the associated NaOH eductor supply valve (CS019) is open. Pump autostart, autostart failure, and pump trip are annunciated on the main control board.

2. Manually: Operation of the control switch to the CLOSE position will start the pump provided that the suction is lined up from the containment recirculation sump and not from the refueling water storage tank (Valves SI8811 and CS009 open).

3. Manually in test mode: Operation of the control switch to the CLOSE position will start the pump provided that; the isolation valve to the containment ring headers (CS007) is closed; the isolation valve for recirculation back to the RWST (SI001) is open; the isolation valve between the spray additive tank and the eductor (CS040) is closed; and the transfer switch on the main control board is in the TEST position.

Two chromel-constantan thermocouples are provided for each motor to measure bearing temperature which is monitored by the computer.

An ammeter is provided on the main control board for each pump to measure motor current.

A pressure gauge is provided in each pump suction and discharge line to provide pressure indications locally.

b. Containment Spray Discharge Header Isolation Valve (CS007)

A control switch is provided on the main control board for each valve.

Each valve can be opened automatically by the containment spray signal from the ESFAS.

Each valve can be manually opened with its control switch provided that the NORMAL-TEST transfer switch for the spray pump on the main control board is in the NORMAL position and at least 30 seconds have elapsed since the spray pump has been operated.

Limit switches on each valve provide valve position indication on the main control board. An annunciator on the main control board indicates if the valve failed to open on an automatic signal.

c. Sodium Hydroxide (NaOH) Eductor Supply Valve (CS019)

A control switch is provided on the main control board for each valve. Automatic opening of the valve occurs when a containment spray actuation signal is received from the ESFAS. Manual opening of the valve using the control switch is possible when the test switch associated with the corresponding spray pump is placed in the TEST position.

Limit switches on each valve provide valve position on the main control board. An annunciator indicates if the valve failed to open on an automatic signal. Failure of the valve to open will prevent autostart of the associated CS pump on an ESF actuation signal.

d. Containment Spray Pump Suction Valve from Recirculation Sump (CS009)

A control switch is provided on the main control board for each of the valves. Each valve can be opened provided that: the containment recirculation sump isolation valve (SI8811) is open, and the RHR pump suction valve from the loop hot legs (RH8701/2) are closed. The purpose of these interlocks is to ensure that neither RWST water nor reactor coolant can be drained to the containment sump through this valve.

Limit switches on each valve provide position indica-tion on the main control board.

e. Containment Spray Pump RWST Suction Valve (CS001)

One suction valve is provided for each spray pump. A control switch is provided on the main control board for each valve. Each valve can be opened provided that the containment spray pump suction valve from the containment recirculation sump is (CS009) closed.

Limit switches on each valve provide position indication on the main control board.

f. Containment Spray Eductor Motive Fluid Flow Valve (CS010)

An air-operated valve is provided for eductor motive flow from the discharge of the containment spray pump. The valve fails open on loss of air to the valve operator.

A control switch is provided on the main control board for each valve. The valve is normally maintained in the open position.

Regardless of the initial position of this valve, receipt of a containment spray actuation signal from the ESFAS opens the valve to ensure proper eductor motive flow.

Limit switches on each valve provide position indication on the main control board.

g. Additional containment spray system alarms on the main control board annunciation system are provided as follows:

1. Low flow alarm in the NaOH suction line to the eductor following a containment spray initiate signal.

2. High, low, and low-low level alarms are provided for the spray additive tank.

3. High containment pressure alarms (Hi, Hi-2, Hi-3) are provided from four redundant pressure monitors which also initiate the containment spray actuation signal and CS actuation annunciation.

h. Testing of the operability of the containment spray system is referred to in Subsection 6.5.2.4 and Chapter 16.0.

7.3.1.1.14 Diesel Fuel Oil System

Diesel fuel oil system components and design information are presented in Subsection 9.5.4. Only instrumentation and controls and their operation are described in this subsection.

a. Diesel Generator Diesel Oil Supply

The diesel oil supply for the standby diesel generators consists of four 25,000-gallon diesel oil storage tanks for Unit 1 diesels, two 50,000-gallon diesel oil storage tanks for Unit 2 diesels, two diesel oil transfer pumps, and one 500-gallon diesel oil day tank per diesel generator.

Each diesel oil storage tank is provided with local level indication and a low level alarm in the main control room.

Each diesel oil transfer pump is provided with a control switch on the associated diesel-generator engine control panel. A selector switch is provided to select the A or B diesel oil transfer pump. Both diesel oil transfer pumps start automatically when the diesel generator starts. When the diesel generators are not running, a low level in the diesel oil day tank will auto-start the transfer pump which has been selected.

Each 500-gallon diesel oil day tank is provided with local level indication and a low level alarm on the diesel-generator engine control panel.

Controls and instruments are supplied from the same ESF bus as the diesel generator it serves.

b. Diesel-Driven Auxiliary Feedwater Pump Diesel Oil Supply

The diesel oil supply for the diesel-driven auxiliary feedwater pump consists of a 500-gallon diesel oil day tank. The diesel oil day tank is provided with

local level indication and low level alarm in the main control room.

c. Diesel-Driven Essential Service Water Makeup Pump Diesel Oil Supply (Byron Only)

The diesel oil supply for the diesel-driven essential service water makeup pumps consists of one 2000-gallon diesel oil storage tank for each pump. Each diesel oil storage tank is provided with local level indication and a low level alarm in the main control room.

7.3.1.1.15 Emergency Core Cooling System (ECCS)

An important engineered safety feature is the emergency core cooling system, which includes a collection of fluid system components described as the safety injection system (SIS). Refer to Section 6.3 for a description and analysis of the system. A flow diagram description is shown in Drawing M-61. The principal description and evaluation of this system is provided in Section 6.3. Certain of the components in this system are actuated by the engineered safety features actuation system (ESFAS) and these components include:

a. Residual heat removal pumps in both trains.

b. Charging pumps and high head safety injection pumps in both trains.

c. Certain train-assigned air-operated or motor-operated isolation valves.

7.3.1.1.15.1 Initiating Circuits and Logic

The function of initiation of safety injection (SI) is described in Subsection 7.3.1.1.1 with specific functions identified in Tables 7.3-1, 7.3-2, and 7.3-3. The logic for the initiation of SI is shown in Drawing 108D685, sheet 8.

7.3.1.1.15.2 Bypasses, Interlocks, and Sequencing

There are no operating or on-line testing bypasses provided for the safety injection pump motors or valve operators. The associated interlocks are described in Section 7.6. The charging, safety injection, and residual heat removal pumps are sequenced as shown in Table 8.3-1.

7.3.1.1.15.3 Redundancy and Diversity

The system is composed of the redundant trains A and B. The instrumentation and controls of the components and equipment in Train A are electrically separated and physically isolated and thus independent of the instrumentation and controls of the

components and equipment in train B. The redundancy and independence provided between safety trains A and B are adequate to maintain equipment functional capabilities following design basis events.

7.3.1.1.16 Combustible Gas Control in Containment

Two hydrogen recombiners each with a design flow rate of up to 75 scfm are provided at each station. A remote control panel is also provided for the recombiners which are designed to operate automatically and unattended after manual startup. A complete description of this system including hydrogen monitoring and hydrogen mixing in containment is provided in Subsection 6.2.5.

7.3.1.1.17 Containment Isolation

A description of the containment isolation system is provided in Subsection 6.2.4. Two redundant, Class 1E, nuclear safety-related area radiation monitors are provided and located inside containment. One monitor provides a signal to reactor protection system Train A and the other provides a signal to Train B. These radiation monitors are described in Subsection 11.5.2.2.7 and listed in Table 12.3-3. Discussions of the containment building ventilation systems are included in Subsections 6.5.1.1.2 and 9.4.9. Containment isolation valves are listed in Table 6.2-58. A description of the engineered safety feature activation system (ESFAS) which includes a functional description of the containment isolation signals is contained in Subsection 7.3.1.

All remote operated (automatic or manual) containment isolation valves are provided with control switches and position lights (open/close) on the main control boards. Additionally, a second pair of open/close indicating lights for each valve is provided in the monitor light boxes on 1PM05J (reactor controls). Monitor light box group 3 displays the lights for all valves which are supposed to close under Phase A isolation. Monitor light box group 5 displays the lights for those additional valves that go closed under Phase B isolation. Any valve not conforming with the required position for the operating condition would be readily apparent by comparison with the remainder of the valves position lights. Refer to Section 7.5 for more detail of the monitor light displays. For discussion of isolation of the containment ventilation on high radiation, refer to Subsection 11.5.2.2.7.

7.3.1.2 Design Basis Information

The functional diagrams presented in Drawing 108D685, Sheets 5, 6, 7, and 8 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 6.0. Given in the following is the design-bases information required in IEEE-Standard 279-1971, Reference 4.

7.3.1.2.1 Generating Station Conditions

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

a. Primary system:

1. a break in small pipes or cracks in large pipes,

2. a break of a reactor coolant pipe, and

3. steam generator tube rupture.

b. Secondary system:

1. minor secondary system pipe breaks resulting in steam release rates equivalent to a single steam dump following a relief or safety valve actuation and

2. major steam pipe break.

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. Main control board indicators and recorders available to the operator are given in Table 7.5-1.

a. Primary system accidents:

1. pressurizer pressure and

2. containment pressure.

b. Secondary system accidents:

1. pressurizer pressure,

2. steamline pressures, and

3. containment pressure.

7.3.1.2.3 Limits, Margins, and Setpoints

Operational limits, available margins and setpoints before onset of unsafe conditions requiring protective action are discussed in Chapters 15.0 and 16.0.

7.3.1.2.4 Abnormal Events

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

a. loss-of-coolant accident (see Subsection 15.6.5);

b. steam breaks (see Subsection 15.1.5);

c. earthquakes (see Chapter 2.0, and Sections 3.7, 3.8, and 3.10);

d. fire (see Subsection 9.5.1);

e. explosion (hydrogen buildup inside containment) (see Section 6.2.5);

f. missiles (see Section 3.5); and

g. flood (see Sections 2.4 and 3.4).

7.3.1.2.5 Minimum Performance Requirements

Minimum performance requirements are as follows:

a. System response times

Engineered Safety Features (ESF) response time and Engineered Safety Features Actuation System (ESFAS) response time are defined in Section 7.1. Maximum allowable response times for each ESF function shall be as shown in Table 7.3-6. No credit was taken in the safety analyses for those channels with response times indicated as "N.A.", not applicable.

The values listed herein are maximum allowable ESFAS response times consistent with the safety analyses and were systematically verified during plant preoperational startup tests. These maximum delay times thus include all compensation, therefore it is required that the instrumentation is calibrated and operating during the test.

Typical maximum allowable time delay in generating the actuation signal for loss-of-coolant protection is:

| | | |
|---|---|---|
| 1. | Pressurizer pressure | 2.0 seconds |

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

| | | |
|---|---|---|
| 1. | Steamline pressure rate | 2.0 seconds |
| 2. | Steamline pressure | 2.0 seconds |

| | | |
|---|---|---|
| 3. | Reactor coolant system $T_{avg}$ including a nominal 2 seconds for electronic filtering of the resistance temperature detector signal | 6.4 seconds |
| 4. | High containment pressure for closing main steamline stop valves | 1.5 seconds |
| 5. | Actuation signals for auxiliary feed pumps | 2.0 seconds |

b. Typical system accuracies:

| | | |
|---|---|---|
| 1. | Pressurizer pressure (uncompensated) | ± 14 psi |
| 2. | Steamline pressure | ± 4% of span |
| 3. | Steamline pressure rate | ± 5 psi/sec |
| 4. | $T_{avg}$ | ± 2°F |
| 5. | Containment pressure signal | ± 1.8% of full scale |

c. Ranges of sensed variables to be accommodated until conclusion of protective action.

| | | |
|---|---|---|
| 1. | Pressurizer pressure | 1700 to 2500 psig |
| 2. | Containment pressure | 0 to 60 psig |
| 3. | $T_{avg}$ | 530 and 630°F |
| 4. | Steamline pressure (from which steamline pressure rate is derived) | 0 to 1300 psig |

7.3.1.3 System Drawings

Schematic diagrams, logic diagrams, piping and instrumentation diagrams, and general arrangements for the systems discussed in this section are listed in the Table of Contents for Chapter 7.

7.3.2 Analysis of ESF Actuation System

7.3.2.1 Failure Mode and Effects Analyses

Failure mode and effects analyses have been performed on ESF systems equipment as presented in Reference 5. The Byron/

Braidwood Stations ESF systems have been designed to equivalent safety design criteria.

The Byron/Braidwood design meets the interface requirements specified in WCAP-8584 (Rev. 1) as classified below:

a. Appendix B, Item B.1.4.a (last sentence) is revised to read: "Circuits associated with Boric Acid Transfer Pumps need not be Class IE but it should be possible to power these pumps from a Class IE power source by manual switching."

b. Appendix B, Item B.1.4.a is revised to read: "All Class IE circuits should be separated from Non-Class IE circuits in accordance with IEEE-384-1974 requirements."

7.3.2.2 Compliance with Standards and Design Criteria

Discussion of the General Design Criteria (GDC) is provided in various sections of Chapter 7.0 where a particular GDC is applicable. Applicable GDCs include Criteria 13, 20, 21, 22, 23, 24, 25, 27, 28, 35, 37, 38, 40, 43, and 46 of the GDC. Compliance with certain IEEE Standards is presented in Subsections 7.1.2.5, 7.1.2.6, 7.1.2.7, and 7.1.2.9. Periodic testing of protection system actuation functions is discussed in Subsection 7.1.2.6. The discussion given below shows that the engineered safety features actuation system complies with IEEE Standard 279-1971, Reference 4.

7.3.2.2.1 Single Failure Criteria

The discussion presented in Subsection 7.2.2.2.3 is applicable to the engineered safety features actuation system, with the following exception.

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 (containment spray excepted). The power supply for the protection systems is discussed in Section 7.6 and in Chapter 8.0. For containment spray, the final bistables are energized to trip to avoid spurious actuation. In addition, manual containment spray requires a simultaneous actuation of two manual controls. This is considered acceptable because spray actuation on high 3 containment pressure signal provides automatic initiation of the system via protection channels. Moreover, two sets (two switches per set) of containment spray manual initiation switches are provided to meet the requirements IEEE Standard 279-1971. Also it is possible for all engineered safety features equipment to be individually manually actuated from the control board. Hence, a third mode of containment spray initiation is available. The design meets the requirements of Criteria 21 and 23 of the GDC.

The engineered safety features systems are designed using the principles in IEEE 379-1972. The systems have independent, redundant channels.

7.3.2.2.2 Equipment Qualification

Equipment qualifications are discussed in Sections 3.10 and 3.11.

7.3.2.2.3 Channel Independence

The discussion presented in Subsection 7.2.2.2.3 is applicable. 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 a-c power supplies which power the logic trains.

7.3.2.2.4 Control and Protection System Interaction

The discussions presented in Subsection 7.2.2.2.3 are applicable.

7.3.2.2.5 Capability for Sensor Checks and Equipment Test and Calibration

The discussions of system testability in Subsection 7.2.2.2.3 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 GDC and periodic testing of protection system actuation functions as discussed in Subsection 7.1.2.8. The tests described in Subsection 7.3.2.2.3 and further discussed in Subsection 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 Subsection 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 Subsections 6.3.4, 7.2.2.2.3, and 7.3.2.2.3 provides complete periodic testability during reactor operation of all logic and components associated with the emergency core cooling system. This design meets the requirements for periodic testing of protection system actuation functions, as discussed in the above sections. The program is as follows:

a. Prior to initial plant operations, engineered safety features system preoperational tests will be conducted.

b. Subsequent to initial startup, the engineered safety features system is periodically tested.

c. During on-line operation of the reactor, all of the engineered safety features analog and logic circuitry are periodically tested. The engineered safety features final actuators are periodically tested, with the exception of valves VQ001A/B, VQ002A/B and SI8808A/B/C/D (due to conflicting Technical Specification LCO requirements that place them in their safeguards actuated condition with power removed).

Performance Test Acceptability Standard

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 7.3-1. Checks of process indications verify operability of the sensors. Analog checks and tests performed with the channel in trip verify the operability of the analog circuitry from the input of these circuits through to and including the logic input relays except for the input relays associated with the containment spray function which are tested during the solid-state logic testing. Analog checks and tests performed with the channel in bypass verify the operability of the analog circuitry from the input to the output of these circuits. Input relays for functions tested in bypass, with the exception of the containment spray function, are tested in accordance with the Surveillance Frequency Control Program. Solid-state logic testing also checks the digital signal path from and including logic input relay contacts through the logic matrixes 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 safe-guards actuation and which can be tested without causing plant upset.

The basis for acceptability of 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.

Maintenance checks, 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.

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:

a. The test procedures must not involve the potential for damage to any plant equipment.

b. The test procedures must minimize the potential for accidental tripping of the reactor.

c. 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 as listed in Subsection 7.3.1.1.1 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 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 essential service water, is initiated by the safety injection signal.

The output of each of the initiation circuits consists of a master relay which drives slave relays for contact multiplication as required. The logic, master, and slave relays are mounted in the solid-state logic protection cabinets designated Train A, and Train B, 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 generator starting, etc.

Analog Testing

Analog testing is identical to that used for reactor trip circuitry and is described in Subsection 7.2.2.2.3.

An exception to this is containment spray, which is energized to actuate 2/4 and reverts to 2/3 when one channel is in test.

Solid-State Logic Testing

Except for containment spray channels; solid-state logic testing is essentially the same as that discussed in Subsection 7.2.2.2.3. 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 solid state protection system output cabinets are subjected to coil continuity tests by the output relay tester in the solid state protection system cabinets. Slave relays (K601, K602, etc.) do not operate because of reduced voltage applied to their coils by the mode selector switch (TEST/OPERATE). The voltage used is reduced to approximately 12.5% of nominal, which is sufficiently reduced to preclude exceeding current margins. 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 online test cabinet so that overlap testing is maintained and the operability of the slave relays thus verified.

The engineered safety features actuation system final actuation device or actuated equipment testing is performed from the engineered safeguards test cabinets. These cabinets are located near the solid-state logic protection system equipment. There is one test cabinet provided for each of the two protection trains. Each cabinet contains individual test switches necessary to operate the slave relays. Assignments of contacts of the 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.

During testing, 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 equipment that will be actuated by the relay. After the tester energized the slave relay, the main control room operator observed all equipment has operated as indicated by appropriate indicating monitor lamps and annunciator on the control board. The operator then resets all devices and prepares for operation of the next slave relay actuated equipment.

Actuator Blocking and Continuity Test Circuits

Those few final actuation devices that cannot be designed to be actuated during plant operation (discussed in Subsection 7.1.2.6) have been assigned to slave relays for which additional test circuitry has been provided to individually block actuation to a

final device. Operation of these slave relays including contact operations continuity checks are made of the electrical circuitry associated with the final devices. 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 the event protection action is required.

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

The typical schemes for blocking operation of selected protection function actuator circuits are shown in Figure 7.3-2 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" are 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 open to block energizing of coil "X1" and "X2," the white lamp is deenergized, 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 deenergized; 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*" will be energized, and green test lamp "DS*" will be deenergized. 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" are capable of being deenergized for protection function actuation 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 deenergizing 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 test lamp should now be energized also; open this blocking relay contact: the green test lamp should be deenergized, which verifies that the circuit is now in its normal, i.e., operable position.

Periodic Maintenance Inspections

The maintenance inspection is done using approved maintenance procedures.

7.3.2.2.6 Manual Resets and Blocking Features

The manual reset feature associated with containment spray actuation is provided for two basic purposes: first, the feature permits the operator to start an interruption procedure of automatic containment spray in event of false initiation of an actuate signal; and second , although spray system performance is automatic, the reset feature enables the operator to start a manual takeover of the system to handle unexpected events based on operator appraisal of conditions following an accident.

It is most important to note that manual control of the spray system does not occur, once actuation has begun, by just resetting the associated logic devices alone. Trip the pump motor circuit breakers, if stopping the pumps is desirable or necessary.

The manual reset feature associated with containment spray, therefore, does not perform a bypass function. It is merely the first of several manual operations required to take control from the automatic system or interrupt its completion should such an action be considered necessary.

The manual block features associated with pressurizer and steamline safety injection signals provide the operator with the means to block initiation of safety injection during plant heatup and cooldown. These block features meet the requirements of Paragraph 4.12 of IEEE Standard 279-1971 in that automatic removal of the block occurs when plant conditions require the protection system to be functional.

7.3.2.2.7 Manual Initiation of Protective Actions (Regulatory Guide 1.62)

There are four individual main steam stop valve momentary control switches (one per loop) mounted on the control board. Each switch when actuated, will isolate one of the main steamlines. In addition, there are two system level switches. Operating either switch will actuate all four main steamlines isolation and bypass valves on the system level. The main steamline pressure instrumentation senses pressure for actuated engineered safety features in the event of a steamline break. This function is discussed in Subsection 7.3.2.4.2. Drawing 108D685, Sheet 7, includes the functional logic diagram showing initiation of a

safety injection and steamline isolation from steamline pressure instruments.

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. Therefore, once safety injection is initiated, those components of the emergency core cooling system (see Section 6.3) which are realigned as part of the semiautomatic switchover, go to completion on low refueling storage tank water level without any manual action. Manual operation of other components or manual verification of proper position as part of emergency procedures is not precluded nor otherwise in conflict with the above described compliance to Paragraph 4.17 of IEEE Standard 279-1971 of the semi-automatic switchover circuits.

No exception to the requirements of IEEE Standard 279-1971 has been taken in the manual initiation circuit of safety injection.

7.3.2.2.8 Analysis of Auxiliary Building HVAC System

7.3.2.2.8.1 General

The auxiliary building HVAC system consists of redundant equipment, the essential portions of which meet the requirements of IEEE 279-1971, "Criteria for Nuclear Power Plant Protection Systems," and various General Design Criteria of 10 CFR 50 Appendix A. See Subsection 7.3.1.1.8 for other details.

7.3.2.2.8.2 Specific Conformance of the Instrumentation and Controls to IEEE 279-1971

Conformance of the auxiliary building HVAC system to the design criteria stated in the articles contained in IEEE 279-1971 are detailed in Table 7.3-4. Clarifications to those statements for specific articles of the criteria which are unique to this system are delineated below.

Article 4.4 Equipment Qualification

Controls, interlocks, and safety devices are cold checked, adjusted and tested to ensure the proper sequence of operation. Also, a final calibration and integrated preoperational test is conducted with all equipment to verify the system's performance.

Article 4.7 Control and Protection Interaction

This article does not apply to this system.

Article 4.14 Access to Means for Bypassing

This article does not apply to this system.

Article 4.21 System Repair

Equipment and control system redundancy and physical separation permit testing, maintenance, repair, or replacement of components without interference in the operation of the redundant equipment. Instruments and controls inside the panels are easily accessible for repair or maintenance.

Article 4.22 Identification

During construction, the locations of redundant parts were chosen to meet the separation requirements; and piping and cable are selectively run to retain the separation. Color coding is used to denote the essential classification of the components.

### 7.3.2.2.8.3 Specific Conformance of the Instrumentation and Controls to General Design Criteria, 10 CFR 50 Appendix A

Conformance of the auxiliary building HVAC system to the design criteria stated in the General Design Criteria of 10 CFR 50 Appendix A is detailed in Table 7.3-5. Clarifications to those statements for specific articles of the criteria which are unique to this system are delineated below:

GDC 20 Protection System Functions

The auxiliary building charcoal booster fans are manually started by a control switch upon detection of high radiation.

The fuel handling building charcoal booster fan is started automatically upon detection of high radiation. The charcoal filter bypass dampers are closed and the auxiliary building and fuel handling building exhaust air is routed through normally bypassed charcoal filters.

GDC 23 Protection System Failure Mode

The instruments and controls are qualified to operate normally under all postulated extremes of temperature, pressure, humidity and radiation dosage.

GDC 24 Separation of Protection and Control Systems

Provides signals for protective action only and no control functions are derived from these channels.

### 7.3.2.2.9 Analysis of Main Control Room HVAC System

The control room HVAC system analysis is presented in Subsection 9.4.1. The control room HVAC system instrumentation and control is described in Subsection 7.3.1.1.9. Also see Section 6.4.

#### 7.3.2.2.9.1 General

The control room HVAC system is a redundant system, consisting of two equipment trains, the essential portions of which meet the requirements of IEEE 279-1971, "Criteria for Nuclear Power Plant Protection Systems," and various General Design Criteria of 10 CFR 50 Appendix A.

#### 7.3.2.2.9.2 Specific Conformance of the Instrumentation and Controls to IEEE 279-1971

Conformance of the control room HVAC system design criteria stated in the articles contained in IEEE-279-1971 are detailed in Table 7.3-4. Clarifications to those statements for specific articles of the criteria which are unique to this system are delineated below.

Article 4.1 General Functional Requirements

Except for the standby makeup filter train, which is automatically initiated on high radiation, the system continues to operate before, during, and after an accident.

Article 4.4 Equipment Qualification

A description of the conformances of this system concerning equipment qualification is described in Subsection 7.3.2.2.8.2. Controls, interlocks, and safety devices are checked, adjusted, and tested to ensure the proper sequence of operation. A final calibration and integrated preoperational test is conducted with all equipment to verify the system's performance.

Article 4.18 Access to Setpoint Adjustments, Calibration, and Test Points

Critical local instruments are installed in lock-in type enclosures. Local instruments having noncritical functions are accessible for adjustments by removal of cover plates.

Article 4.21 System Repair

Equipment and control system redundancy and physical separation will permit testing, maintenance repair or replacement of components without interference in the operation of companion equipment train components. Instruments and controls inside the panels are easily accessible for maintenance.

Article 4.22 Identification

During construction, the locations of redundant parts were chosen to meet the separation requirements, and piping and cable are selectively run to retain the separation. Color coding is used to denote the essential classification of the components, cable, and instrumentation and control.

#### 7.3.2.2.9.3 Specific Conformance of Instruments and Controls to General Design Criteria 10 CFR 50 Appendix A

Conformance of the control room HVAC system design criteria stated in the General Design Criteria of 10 CFR 50, Appendix A Table 7.3-5. Clarifications to those statements for specific articles of the criteria which are unique to this system are delineated below.

GDC 19 Control Room

The control room HVAC system has been designed to provide adequate radiation protection to permit access under accident conditions. The outside air radiation monitoring system and the turbine building HELB pressure monitoring system are interlocked with the HVAC system to isolate the main control room and automatically introduce makeup air from the turbine building (unless abnormal pressure is detected at the turbine building intake) through one of the emergency filter trains to maintain control room habitability. In the event of a HELB in the turbine building, the turbine building intake is maintained closed to prevent excessive moisture from entering the control room, and makeup air from the outside air bypass line intake is routed through one of the emergency filter trains.

GDC 20 Protection System Function

The control room HVAC system control and instrumentation has been designed to sense abnormal radiation levels in the outside air intakes and to automatically initiate protective action.

GDC 21 Protection System Reliability and Testability

Redundant channels are provided in the radiation protection system to permit independent periodic testing of one channel without affecting the protection function of the other channel.

GDC 22 Protection System Independence

Refer to response to conformance to Criterion 21.

GDC 23 Protection System Failure Mode

The instrumentation and controls are classified as essential and have been qualified to withstand the most adverse environmental conditions in their corresponding installation location.

GDC 24 Separation of Protective and Control Systems

The radiation detection system provides signals for protective action only and no control functions are derived from these channels.

#### 7.3.2.2.10 Analysis of Diesel-Generator Room Ventilation System

##### 7.3.2.2.10.1 General

Redundant diesel generators have been provided with independent diesel-generator room ventilation systems. The instrumentation

and controls provided for these systems meet the requirement of IEEE Standard 279-1971, and General Design Criteria of 10 CFR 50 Appendix A. See Subsection 7.3.1.1.10.

7.3.2.2.10.2 Specific Conformance of the Instrumentation and Controls to IEEE 279-1971

Conformance of the diesel-generator ventilation system to the design criteria stated in the articles contained in IEEE 279-1971 are detailed in Table 7.3-4. Clarifications to those statements for specific articles of the criteria which are unique to this system are delineated below.

Article 4.1 General Functional Requirement

The diesel generator is started on receipt of a protective action signal initiated from an undervoltage relay sensing loss of offsite power.

Article 4.2 Single Failure Criterion

Single failure criterion does not apply because of the independence of these systems.

Article 4.5 Channel Integrity

All channels being independent, do not require meeting this requirement.

Article 4.6 Channel Independence

All channels being independent, they do not require meeting this requirement.

Article 4.7 Control and Protection Interaction

This article does not apply to this system.

Article 4.11 Channel Bypass or Removal from Operation

Channels for each ventilating system being independent are not bypassed but are removed from operation.

Article 4.14 Access to Means for Bypassing

This article does not apply to this system.

7.3.2.2.10.3 Specific Conformance of the Instrumentation and Controls to General Design Criteria of 10 CFR 50 Appendix A

Conformance of the diesel-generator ventilation system to the design criteria stated in the General Design Criteria of 10 CFR 50 Appendix A is detailed in Table 7.3-5. Clarifications to

those statements for specific articles of the criteria which are unique to this system are delineated below.

GDC 19 Control Room

Instrumentation and controls for each ventilation system have been provided to maintain each respective diesel generator at its design capability to supply emergency electric power to the control room during the loss of offsite power.

GDC 21 Protection System Reliability and Testability

These ventilation systems and the associated instrumentation and controls are completely independent so that a single failure at one diesel-generator vent system or removal from service of any component of one system will not affect the operation of the other diesel-generator vent system.

GDC 22 Protection System Independence

Refer to response to conformance to Criterion 21.

GDC 23 Protection System Failure Mode

The instrumentation and controls are classified as essential and have been qualified to withstand the most adverse environmental condition in their corresponding installation location.

#### 7.3.2.2.11 Analysis of Ventilation Systems for Redundant ESF Switchgear Rooms, Cable Spreading Rooms, Miscellaneous Electrical Equipment Rooms, Battery Rooms, and Byron Cooling Tower Substation Rooms

##### 7.3.2.2.11.1 General

Redundant ESF switchgear rooms, cable spreading rooms, miscellaneous electrical equipment rooms, battery rooms, and the Byron cooling tower electrical substation rooms have been provided with independent ventilation systems as identified in Subsection 7.3.1.1.11.1. The instrumentation and controls provided for these systems meet the requirement of IEEE Standard 279-1971, and General Design Criteria of 10 CFR 50 Appendix A.

##### 7.3.2.2.11.2 Specific Conformance of the Instrumentation and Controls to IEEE-279-1971

Conformance for the ventilation systems of the redundant ESF switchgear rooms, miscellaneous electrical equipment rooms, battery rooms, and the Byron cooling tower electrical substation rooms to the design criteria stated in the articles contained in IEEE 279-1971 are detailed in Table 3.7-4. Clarifications to those statements for specific articles of the criteria which are unique to these systems are delineated below:

Article 4.1 General Functional Requirement

During loss of offsite power, they are fed with electric power from respective diesel generator.

Article 4.2 Single Failure Criterion

Single failure criterion does not apply because of the independence of these systems.

Article 4.5 Channel Integrity

All channels being independent, do not require meeting this requirement.

Article 4.6 Channel Independence

All channels are independent, and thus meet the requirement.

Article 4.7 Control and Protection Interaction

This article does not apply to this system.

Article 4.11 Channel Bypass or Removal from Operation

Channels for each ventilating system being independent are not bypassed but are removed from operation.

Article 4.12 Operation Bypass

This article does not apply to this system.

Article 4.14 Access to Means for Bypassing

This article does not apply to this section.

Article 4.16 Completion of Protection Action Once it is Initiated

Completion of protective action once it is initiated is not obstructed.

7.3.2.2.11.3 Specific Conformance of the Instrumentation and Controls to General Design Criteria, 10 CFR 50 Appendix A

Conformance to the ventilation systems of the redundant ESF switchgear rooms, cable spreading rooms, battery rooms, and the Byron cooling tower electrical substation rooms to the design criteria stated in the General Design Criteria of 10 CFR 50 Appendix A is detailed in Table 7.3-5. Clarifications to those statements for specific articles of the criteria which are unique to these systems are delineated below.

GDC 19 Control Room

Instrumentation and controls for each ventilation system have been provided to permit each respective electrical equipment to function at its design capability during normal and abnormal station operating conditions.

GDC 21 Protection System Reliability and Testability

These ventilation systems and the associated instrumentation and controls are completely independent so that a single failure at one vent system or removal from service of any component of one system will not affect the operation of the other vent system.

GDC 22 Protection System Independence

Refer to response to conformance to Criteria 21.

GDC 23 Protection System Failure Mode

The instrumentation and controls are classified as essential and have been qualified to withstand the most adverse environmental conditions in their corresponding installation location.

7.3.2.2.12 Analysis of Reactor Containment Fan Cooler (RCFC) Units

7.3.2.2.12.1 General

The RCFC units consist of four 50% capacity units, the essential portions of which meet the requirements of IEEE 279-1971, "Criteria for Nuclear Power Plant Protection Systems," and various General Design Criteria of 10 CFR 50 Appendix A.

7.3.2.2.12.2 Specific Conformance of the Instrumentation and Controls to IEEE 279-1971

Conformance of the RCFC units to the design criteria stated in the articles contained in IEEE-279-1971 are detailed in Table 7.3-4. Clarifications to those statements for specific articles of the criteria which are unique to this system are delineated below:

Article 4.4 Equipment Qualification

Controls, interlocks, and safety devices are cold checked, adjusted and tested to ensure the proper sequence of operation. A final calibration is conducted with all equipment to verify the system's performance.

4.7 Control and Protection Interaction

Does not apply.

Article 4.14 Access to Means for Bypassing

Does not apply.

Article 4.18 Access to Setpoint Adjustments, Calibration, and Test Points

Local instruments are accessible for adjustment by removal of cover plates.

Article 4.19 Identification of Protective Actions

Containment temperatures are indicated in the main control room.

Article 4.20 Information Readout

Containment temperatures are indicated in the main control room.

Article 4.21 System Repair

Equipment and control system redundancy and physical separation permit testing, maintenance, repair or replacement of components without interference in the operation of the redundant equipment. Instruments and controls inside the panels are easily accessible for repair or maintenance.

Article 4.22 Identification

The locations of redundant parts were chosen to meet the separation requirements, and piping and cable are selectively run to retain the separation. Color coding is used to denote the essential classification of the components, cables, instrumentation and controls.

7.3.2.2.12.3 Specific Conformance of the Instrumentation and Controls to General Design Criteria, 10 CFR 50, Appendix A

Conformance of the RCFC units to the design criteria stated in the Design Criteria of 10 CFR 50 Appendix A is detailed in Table 7.3-5. Clarifications to those statements for specific articles of the criteria which are unique to this system are delineated below.

GDC 21 Protection System Reliability and Testability

These ventilation systems and the associated instrumentation and controls are completely independent so that a single failure at one vent system or removal from service of any component of one system will not affect the operation of the other vent system.

DC 22 Protection System Independence

Instrumentation and controls for redundant equipment is completely independent so that a single failure or removal from service of any component will not affect the operation of the protection system.

GDC 23 Protection System Failure Mode

The instruments and controls are qualified to operate normally under all postulated extremes of temperature, pressure, humidity and radiation dosage.

7.3.2.3 Further Considerations

A loss of instrument air or loss of component cooling water to vital equipment were considered. Neither can cause safety limits as given in the Technical 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. Furthermore, all pneumatically operated valves and controls will assume a preferred operating position upon loss of instrument air to the valve and controls. There are approximately 200 pneumatically operated valves which are required for or related to safety. They are shown on the P&I diagrams that are contained in the figures of the UFSAR for each system. The preferred operating position and the fail safe position for each valve are also shown on the P&I diagrams. Most pneumatically operated valves have spring returns on them to cause them to move to the fail safe position in the event of air failure. Category I air accumulators are provided for the remainder of the valves. There are no pneumatic controls in the plant except for those associated with valves. A pneumatic control component failure will not affect the ability of the valves to move to their fail safe position. It is also noted that, for conservatism during the accident analysis (Chapter 15.0), credit is not taken for the instrument air systems nor for any control system benefit.

The reactor coolant pumps will not trip on a loss of component cooling water. Indication in the control room is provided whenever component cooling water is lost. The reactor coolant pumps can run about 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.

Westinghouse identified four systems which, if subjected to an adverse environment, could potentially lead to control system faulty operation which may impact protective functions. These four systems have been investigated and it has been concluded that the proposed accident sequences are either not applicable to Byron/Braidwood or would not result in a more limiting event than those presented in the plant Safety Analysis Report. Each potential problem is discussed in the following.

Automatic Rod Control System

The potential problem is a failure in the excore neutron detectors or associated cabling resulting in inaccurate detector output in the low direction causing an automatic rod withdrawal accident coincident with a steamline break.

The excore detectors are not required once the reactor has tripped. Prior to reactor trip, several factors tend to decrease the possibility of a significant consequential malfunction of the automatic rod control system due to a steamline break inside containment. The physical location of the excore detectors relative to the postulated break location does not provide direct access for steam to travel to the excore detectors. The detectors are located in an annulus around the reactor vessel separated by a concrete barrier from the other primary components and piping.

As stated in Subsection 7.2.2.3.1, an isolated auctioneered high signal is derived by auctioneering of the four channels for automatic rod control. That is, rod withdrawal is based on the highest of the four excore detectors. Therefore, rod withdrawal will occur only if all four excore detectors fail low. For these reasons it is unlikely that rod withdrawal will result from environmental failure of the excore detectors prior to reactor trip.

Based on the low probability of the occurrence of a consequential malfunction of the rod control system, we do not believe this scenario represents a significant safety question.

Main Feedwater Control System

The postulated problem is a malfunction of the main feedwater control system due to an adverse environment following a break of a small feedwater line. If an assumption is made that this malfunction causes the feedwater control valves to close in both the damaged loop and the intact loops, liquid level in the intact steam generators could be affected.

The feedwater flow control devices under question are the feedwater flow elements and associated transmitters which are located outside containment in the steam tunnel as it opens to the turbine building, some 100 feet from the nearest break location. The steam generator level and steam flow transmitters are located inside containment, but outside the missile barrier and physically separated for each loop. Because of the small size of the postulated break, and the physical separation of each device from the proximity of the break, it is unlikely that the environment around the devices could cause failure, particularly simultaneous failure, in all four loops.

Also, the loss of normal feedwater flow study has been made and addressed in Subsection 15.2.7. The results of the analysis presented conclude that the loss of normal feedwater does not adversely affect the core, reactor coolant system, or the steam systems, since the auxiliary feedwater system is capable of removing stored and residual heat, thus preventing overpressurization of the reactor coolant system or loss of water from the reactor core returning the plant to a safe condition. For these reasons, it is not believed that this scenario represents a significant safety question that requires further action.

Pressurizer PORV Control System

Refer to the discussion of the pressurizer PORV control system in Subsection 7.2.2.3.7.

Steam Generator PORV Control System

Refer to the discussion of the steam generator PORV control system in Subsection 7.2.2.3.7.

7.3.2.4 Summary

The effectiveness of the engineered safety features actuation system is evaluated in Chapter 15.0, based on the ability of the system to contain the effects 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 15.0.

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.

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 direct consequence of a primary system break. The generation time of the actuation signal of about 1.5 seconds, after detection of the consequences of the accident, is adequate.

Containment spray provides additional emergency cooling of containment and also limits fission product release upon sensing elevated containment pressure (Hi 3) 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 about 1.0 second; well within the capability of the protection system equipment.

The analyses in Chapter 15.0 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 Steamline Break Protection

The emergency core cooling system is also actuated in order to protect against a steamline break. About 2.0 seconds elapses between sensing low steamline pressure and 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 in time to limit or prevent further core damage. There is a reactor trip but the core reactivity is further reduced by the highly borated water injected by the emergency core cooling system.

Additional protection against the effects of steamline 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 steamline isolation valves in order to prevent uncontrolled blowdown of all steam generators. The generation of the protection system signal is approximately 2.0 seconds.

The analyses in Chapter 15.0 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. J. B. Reid, "Process Instrumentation for Westinghouse Nuclear Steam Supply System (4-Loop Plant using WCID 7300 Series) Process Instrumentation," WCAP-7913, March 1973.

2. D. N. Katz, "Solid State Logic Protection System Description," WCAP-7488-L, March 3, 1971 (Proprietary), and WCAP-7672, June 1971 (Non-Proprietary).

3. J. W. Swogger, "Testing of Engineered Safety Features Actuation System," WCAP-7705, Revision 2, January 1976. (Information only; i.e., not a generic topical WCAP).

4. The Institute of Electrical and Electronics Engineers, Inc., "IEEE Standard: Criteria for Protection System for Nuclear Power Generating Station," IEEE Standard 279-1971.

5. F. T. Eggleston, D. H. Rawlins, and J. R. Petrow, "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.

TABLE 7.3-1

INSTRUMENTATION OPERATING CONDITIONS
FOR ENGINEERED SAFETY FEATURES

| NUMBER | FUNCTIONAL UNIT | NUMBER OF CHANNELS | NUMBER OF CHANNELS TO TRIP |
|---|---|---|---|
| 1. | SAFETY INJECTION | | |
| | a. Manual | 2 | 1 |
| | b. High Containment Pressure (Hi-1) | 3 | 2 |
| | c. Low compensated steamline pressure* (Isolated loop exempted) | 12 (3/steam-line) | 2 in any one steamline+ |
| | d. Pressurizer Low-Pressure** | 4 | 2 |
| 2. | CONTAINMENT SPRAY | | |
| | a. Manual*** | 4 | 2 |
| | b. Containment Pressure High-High-High (Hi-3) | 4 | 2 |

* Permissible bypass if reactor coolant pressure is less than 1930 psig interlocked with P-11. Lead/lag calibration is performed periodically to confirm the proper setting (see Note on Technical Specification Table 3.3.2-1).

** Permissible bypass if reactor coolant pressure is less than 1930 psig interlocked with P-11.

*** Manual actuation of containment spray is accomplished by actuating either of two sets (two switches per set). Both switches in a set must be actuated to obtain a manually initiated spray signal. The sets are wired to meet separation and signal failure requirements of IEEE 279-1971. Simultaneous operation of two switches is desirable.

\+ Isolated loop exempted.

TABLE 7.3-2

INSTRUMENT OPERATING CONDITIONS
FOR ISOLATION FUNCTIONS

| NUMBER | FUNCTIONAL UNIT | NUMBER OF CHANNELS | NUMBER OF CHANNELS TO TRIP |
|---|---|---|---|
| 1. | CONTAINMENT ISOLATION | | |
| | a. Automatic Safety Injection (Phase A) | See Item No. 1 (b) through (d) of Table 7.3-1 | |
| | b. Containment Pressure (Phase B) | See Item No. 2 (b) of Table 7.3-1 | |
| | c. Manual<br>Phase A<br>Phase B | <br>2<br>See Item No. 2 (a) of Table 7.3-1 | <br>1 |
| 2. | STEAMLINE ISOLATION | | |
| | a. Low steamline* pressure | 12 (3/steam-line) | 2 in any one steamline |
| | b. Containment Pressure High-high (Hi-2) | 3 | 2 |
| | c. High steam pressure rate** | 12 (3/steam-line) | 2 in any one steamline |
| | d. Manual*** | 1/loop | 1/loop |

* Permissible bypass if reactor coolant pressure is less than 1930 psig interlocked with P-11. Lead/lag compensation calibration is performed periodically to confirm the proper setting (see Note on Technical Specification Table 3.3.2-1).

** Becomes active below P-11 when the low steamline pressure SI is blocked. The isolation function is automatically blocked above P-11. Rate/lag compensation calibration is performed periodically to confirm the proper setting (see Note on Technical Specification Table 3.3.2-1).

*** Additionally, there are two switches that will actuate to close all four main steamline isolation valves at the system level.

TABLE 7.3-2 (Cont'd)

| NUMBER | FUNCTIONAL UNIT | NUMBER OF CHANNELS | NUMBER OF CHANNELS TO TRIP |
|---|---|---|---|
| 3. | FEEDWATER LINE ISOLATION | | |
| | a. Safety Injection | See Item No. 1 of Table 7.3-1 | |
| | b. Steam Generator High-High level 2/4 on any Steam Generator | 4/loop | 2/loop |
| | c. P-4 Reactor Trip with coincident LO $T_{ave}$ (See Table 7.3-3) | 2 | 1 |

TABLE 7.3-3

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

| DESIGNATION | INPUT | FUNCTION PERFORMED |
|---|---|---|
| P-4 | Reactor trip | Actuates turbine trip |
| | | Closes the Unit 2 Preheater Bypass Isolation Valves (2FW039A-D). |
| | | Closes main and bypass feedwater valves when the LO $T_{ave}$ setpoint is reached. |
| | | Opens main feedwater pump recirculation valves when valve control switches are in modulate. (FW012A-C) |
| | | Prevents opening of main and bypass feedwater valves which were closed by safety injection or High-High steam generator water level |
| | | Allows manual block of the automatic reactuation of safety injection |
| | Reactor not tripped | Defeats the block preventing automatic reactuation of safety injection |
| P-11 | 2/3 Pressurizer pressure below setpoint | Allows manual block of safety injection actuation on low pressurizer pressure signal. Allows manual block of safety injection actuation and steam line isolation on low compensated steam line pressure signal and allows steam line isolation on high steam line negative pressure rate. |

TABLE 7.3-3 (Cont'd)

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

| DESIGNATION | INPUT | FUNCTION PERFORMED |
|---|---|---|
| | 2/3 Pressurizer pressure above setpoint | Defeats manual block of safety injection actuation on low pressurizer pressure and safety injection and steam line isolation on low steam line pressure and defeats steam line isolation on high steam line negative pressure rate. |

TABLE 7.3-3 (Cont'd)

| DESIGNATION | INPUT | FUNCTION PERFORMED |
|---|---|---|
| P-12* | 2/4 $T_{avg}$ below setpoint | Blocks steam dump. |
| | | Allows manual bypass of steam dump block for the cooldown valves only |
| | 3/4 $T_{avg}$ above setpoint | Defeats the manual bypass of steam dump block |
| P-14 | 2/4 Steam generator water level above setpoint on any steam generator | Closes all feedwater control valves and isolation valves |
| | | Trips all main feedwater pumps which closes the pump discharge valves |
| | | Actuates turbine trip |

* ESF Interlock not applicable.

TABLE 7.3-4

CONFORMANCE TO IEEE 279-1971

The following information addressing conformance of system design to the specific articles of IEEE 279-1971 are described below and also will be used in Subsections 7.3.2.2.8.2, 7.3.2.2.9.2, 7.3.2.2.10.2, 7.3.2.2.11.2, and 7.3.2.2.12.2. Additional clarifications of conformance to the criteria which are unique to a specific system design are delineated within those subsections.

Article 4.1 General Functional Requirements

The system performs its function during all phases of station operation.

Article 4.2 Single-Failure Criteria

The system consists of redundant equipment which is powered from separate buses and actuated by separate control circuits. A single failure will not affect the entire system.

Article 4.3 Quality of Components and Modules

Components are specified to comply with the functional requirements of the service in which they are used.

Article 4.4 Equipment Qualification

All equipment is factory inspected and tested in accordance with the applicable equipment specifications, quality assurance requirements, codes and standards.

Article 4.5 Channel Integrity

The instrumentation and control devices are designed to operate in the maximum environmental extremes expected. Control signals for the essential devices of this system remain functional under all station conditions.

Article 4.6 Channel Independence

Electrical and mechanical separation are maintained between the instrumentation and controls for redundant system equipment.

Article 4.7 Control and Protection Interaction

The instrumentation and controls do not provide control and protective action from the same device. Those that provide a protective function are classified essential. The radiation monitoring and protection systems are used only for

TABLE 7.3-4 (Cont'd)

protective action and no control function is derived from these channels.

Article 4.8 Derivation of System Inputs

The signals for essential instruments are direct measures of desired variable parameters.

Article 4.9 Capability for Sensor Checks

Sensor checks can be made by perturbation of parameters and by cross-check with other calibrated instruments.

Article 4.10 Capability for Test and Calibration

Capability for calibration of the sensors is provided in the design.

Article 4.11 Channel Bypass or Removal from Operation

The System is designed to permit independent testing of redundant equipment and associated instrumentation during power operation without affecting environmental conditions.

Article 4.12 Operating Bypasses

The system has no operating bypasses.

Article 4.13 Indication of Bypasses

The use of a pull-to-lock control switch position causes all lights above the control switch to go out.

Article 4.14 Access to Means for Bypassing

Local control panels containing the local control switches are located in the equipment rooms under administrative control. The control switches in the main control room are under the administrative control of the operators.

Article 4.15 Multiple Setpoints

This article is not applicable to the systems described.

Article 4.16 Completion of Protective Action Once it is Initiated

Once a protective action takes place it can be reversed by a subsequent deliberate action by the operator.

TABLE 7.3-4 (Cont'd)

Article 4.17 Manual Initiation

Startup of this system can be initiated manually.

Article 4.18 Access to Setpoint Adjustment

Administrative control is provided for access to the instruments and devices for setpoint adjustments and calibration.

Article 4.19 Identification of Protective Actions

Lights associated with equipment control switches indicate the operating status of the system.

Article 4.20 Information Readout

Lights and indicator annunciators display the operating status of the system.

Article 4.21 System Repair

Provisions were made for the recognition, location, replacement, repair or adjustment of malfunctioning instruments and controls.

Article 4.22 Identification

During design and engineering phases, an essential classification was assigned to each safety-related instrument, control and device.

TABLE 7.3-5

CONFORMANCE TO GENERAL DESIGN CRITERIA

10 CFR 50 APPENDIX A

The following information addressing conformance of system design to the specific criteria of the General Design Criteria, 10 CFR 50 Appendix A are described below and also will be used in Subsections 7.3.2.2.8.3, 7.3.2.2.9.3, 7.3.2.2.10.3, 7.3.2.2.11.3, and 7.3.2.2.12.3. Additional clarifications of conformance to the criteria which are unique to a specific system design are delineated within those subsections.

GDC 13 Instrumentation and Controls

Instrumentation and controls for the system have been provided to monitor and maintain temperature and pressure at a predetermined setpoint.

GDC 19 Control Room

The control room HVAC system has been designed to provide adequate radiation protection to permit access under accident conditions. The outside air radiation monitoring system and the turbine building HELB pressure monitoring system are interlocked with the HVAC system to isolate the main control room and automatically introduce makeup air from the turbine building (unless abnormal pressure is detected at the turbine building intake) through one of the emergency filter trains to maintain control room habitability. In the event of a HELB in the turbine building, the turbine building intake is maintained closed to prevent excessive moisture from entering the control room, and makeup air from the outside air bypass line intake is routed through one of the emergency filter trains.

GDC 20 Protection System Function

The control room HVAC system control and instrumentation has been designed to sense abnormal radiation levels in the outside air intakes and to automatically initiate protective action.

GDC 21 Protection System Reliability and Testability

Instrumentation and controls for the system have been designed for high functional reliability and inservice testability by conformance to IEEE Standard 279-1971.

GDC 22 Protection System Independence

Instrumentation and controls for redundant equipment is completely independent so that a single failure or removal from service of any component does not prevent the operation of the system.

TABLE 7.3-5 (Cont'd)

GDC 23 Protection System Failure Mode

The instrumentation and controls for each ventilation system have been designed to fail safe when conditions such as loss of electric power or instrument air are experienced.

GDC 24 Separation of Protective and Control Systems

The radiation detection system provides signals for protective action only and no control functions are derived from these channels.

GDC 29 Protection Against Anticipated Operational Occurrences

The instrumentation and controls for the system have been designed to accomplish its safety function in the event of anticipated operational occurrences.

TABLE 7.3-6

ENGINEERED SAFETY FEATURES MAXIMUM ALLOWABLE RESPONSE TIMES

| INITIATING SIGNAL RESPONSE TIME AND FUNCTION | MAXIMUM ALLOWABLE IN SECONDS |
|---|---|
| 1. Manual Initiation | |
| a. Safety Injection (ECCS) | N.A. |
| b. Containment Spray | N.A. |
| c. Phase "A" Isolation | N.A. |
| d. Phase "B" Isolation | N.A. |
| e. Containment Vent Isolation | N.A. |
| f. Steam Line Isolation | N.A. |
| g. Feedwater Isolation | N.A. |
| h. Auxiliary Feedwater | N.A. |
| i. Essential Service Water | N.A. |
| j. Containment Cooling Fans | N.A. |
| k. Start Diesel Generator | N.A. |
| l. Control Room Isolation | N.A. |
| m. Turbine Trip | N.A. |
| 2. Containment Pressure-High-1 | |
| a. Safety Injection (ECCS) | $\leq 27^{(7)}/27^{(5)}$ |
| 1. Reactor Trip | $\leq 2$ |
| 2. Feedwater Isolation | $\leq 7^{(3)}$ |
| 3. Phase "A" Isolation | $\leq 2^{(6)}$ |
| 4. Containment Vent Isolation | $\leq 7$ |
| 5. Auxiliary Feedwater | $\leq 60$ |
| 6. Essential Service Water | $\leq 42^{(1)}$ |
| 7. Containment Cooling Fans | $\leq 40^{(1)}$ |
| 8. Start Diesel Generator | $\leq 12^{(10)}$ |
| 9. Control Room Isolation | N.A. |
| 10. Turbine Trip | N.A. |

TABLE 7.3-6 (Cont'd)

| INITIATING SIGNAL AND FUNCTION | MAXIMUM ALLOWABLE RESPONSE TIME IN SECONDS |
|---|---|
| 3. Pressurizer Pressure-Low | |
| a. Safety Injection (ECCS) | ≤ 27[7]/27[5] |
| 1. Reactor Trip | ≤ 2 |
| 2. Feedwater Isolation | ≤ 7[3] |
| 3. Phase "A" Isolation | ≤ 2[6] |
| 4. Containment Vent Isolation | ≤ 7 |
| 5. Auxiliary Feedwater | ≤ 60 |
| 6. Essential Service Water | ≤ 42[1] |
| 7. Containment Cooling Fans | ≤ 40[1] |
| 8. Start Diesel Generator | ≤ 12[10] |
| 9. Control Room Isolation | N.A. |
| 10. Turbine Trip | N.A. |
| 4. Steam Line Pressure-Low | |
| a. Safety Injection (ECCS) | ≤ 37[4]/27[5] |
| 1. Reactor Trip | ≤ 2 |
| 2. Feedwater Isolation | ≤ 7[3] |
| 3. Phase "A" Isolation | ≤ 2[6] |
| 4. Containment Vent Isolation | ≤ 7 |
| 5. Auxiliary Feedwater | ≤ 60 |
| 6. Essential Service Water | ≤ 42[1] |
| 7. Containment Cooling Fans | ≤ 40[1] |
| 8. Start Diesel Generator | ≤ 12[10] |
| 9. Control Room Isolation | N.A. |
| 10. Turbine Trip | N.A. |

TABLE 7.3-6 (Cont'd)

| INITIATING SIGNAL AND FUNCTION | MAXIMUM ALLOWABLE RESPONSE TIME IN SECONDS |
|---|---|
| b. Steam Line Isolation | ≤ 7 |
| 5. Containment Pressure-High-3 | |
| a. Containment Spray | ≤ 45(1) |
| b. Phase "B" Isolation | ≤ 22(1)/12(2) |
| 6. Steam Generator Water Level-High-High | |
| a. Turbine Trip | ≤ 2.5 |
| b. Feedwater Isolation | ≤ 7(3) |
| 7. Steam Generator Water Level-Low-Low | |
| a. Motor-Driven Auxiliary Feedwater Pump | ≤ 55(12) |
| b. Diesel-Driven Auxiliary Feedwater Pumps | ≤ 55(12) |
| 8. Containment Pressure-High-2 | |
| Steam Line Isolation | ≤ 7 |
| 9. RWST Level-Low-Low Coincident with Safety Injection | |
| Automatic Opening of Containment Sump Suction Isolation Valves | ≤ 100 |
| 10. Undervoltage RCP Bus | |
| a. Motor-Driven Auxiliary Feedwater Pump | ≤ 60 |
| b. Diesel-Driven Auxiliary Feedwater Pump | ≤ 60 |
| 11. Division 11 for Unit 1 (Division 21 for Unit 2) ESF Bus Undervoltage | |
| Motor-Driven Auxiliary Feedwater Pump | ≤ 60(1) |

TABLE 7.3-6 (Cont'd)

| INITIATING SIGNAL AND FUNCTION | MAXIMUM ALLOWABLE RESPONSE TIME IN SECONDS |
|---|---|
| 12. Loss of Power | |
| a. ESF Bus Undervoltage | ≤ 1.9[9] |
| b. Grid Degraded Voltage | ≤ 310 ±30 delay |
| 13. Steam Line Pressure - Negative Rate-High (Below P-11) | |
| Steam Line Isolation | ≤ 7 |
| 14. Phase "A" Isolation | |
| Containment Vent Isolation | ≤ 7 |
| 15. Auxiliary Feedwater Pump Suction Pressure-Low-Low | |
| Automatic Switchover to ESW | N.A. |

Table 7.3-6 (Cont'd)

Table of Notations

1. Diesel generator starting and sequence loading delays included.

2. Diesel generator starting and sequence loading delay not included. Offsite power available.

3. Hydraulic operated valves.

4. Diesel generator starting and sequence loading delay included. Only centrifugal charging pumps included. Sequential transfer of centrifugal charging pump suction from the VCT to the RWST (CV112D and E open, then CV112B and C close) is included.

5. Diesel generator starting and sequence loading delays not included. Offsite power available. Only centrifugal charging pumps included. Sequential transfer of centrifugal charging pump suction from the VCT to the RWST (CV112D and E open, then CV112B and C close) is included.

6. Does not include valve closure time.

7. Diesel generator starting and sequence loading delays included. Sequential transfer of centrifugal charging pump suction from the VCT to the RWST (CV112D and E open, then CV112B and C close) is not included. Only the opening of CV112D and E is included.

8. Deleted.

9. The response time reflects bench test conditions.

10. Includes a 2-second electronic delay to account for the time required to process and generate the safeguards signal after the parameter setpoint is reached.

11. ESF response times which include sequential operation of the RWST and VCT valves (Notes 4 and 5) are based on values assumed in the non-LOCA safety analyses. These analyses take credit for injection of borated water from the RWST. Injection of borated water is assumed not to occur until the VCT charging pump suction valves are closed following opening of the RWST charging pump suction valves. When the sequential operation of the RWST and VCT valves is not included in the response times (Note 7), the values specified are based on the LOCA analyses. The LOCA analyses take credit for injection flow regardless of the source. Verification of the response times specified in Table 7.3-6 will assure that the assumptions used for the LOCA and non-LOCA analyses with respect to operation of the VCT and RWST valves are valid.

Table 7.3-6 (Cont'd)

Table of Notations

12. The 55 sec. maximum allowable response time for Auxiliary Feedwater is based on the Loss of Normal Feedwater and Feedwater Line Break analyses with offsite power available. The analyses with offsite power available assume more limiting response time and provide the acceptance requirement for response time testing. The maximum allowable response time for Auxiliary Feedwater is 63 seconds for a Loss of Normal Feedwater or Feedwater Line Break analyses with a loss of offsite power.

## 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. 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 in the nuclear steam supply system. The discussion of these systems together with the applicable codes, criteria and guidelines is found in other sections of the Byron/Braidwood Updated Final Safety Analysis Report. In addition, alignment is initiated during the safety injection mode by the engineered safety features actuation system by means of the final actuation circuitry discussed in the subsections under 7.3.1.1. This final actuation circuitry consists of the dry contacts of the slave relays and their associated output circuits in the solid state protection system (SSPS) and the field wiring up to the inputs of the actuation devices. For the description of the actuation devices and the actuated equipment, refer to the appropriate subsections in Chapters 6.0, 9.0, and 10.0 as identified in the subsections under 7.3.1.1. For example, Subsection 7.3.1.1.4 refers to 10 (a through j) key functions initiated by the final SSPS actuation circuitry. For the derivation of the logic functions that generate ESFAS, refer to Tables 7.3-1, 7.3-2, and 7.3-3, as well as Drawings 108D685. Following the safety injection mode, and following a LOCA, realignment of certain fluid system ECCS equipment occurs for cold leg recirculation. For the description of this phase of shutdown following a LOCA, refer to Subsection 6.3.2.8. For the description of hot leg recirculation realignment following a LOCA, refer to Table 6.3-7. Systems and instrumentation which may be used for post-fire safe shutdown are discussed in Section 2.4 of the Fire Protection Report.

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 nonaccident conditions. These functions will permit the necessary operation that will:

a. prevent the reactor from achieving criticality in violation of the technical specifications, and

b. provide an adequate heat sink such that design and safety limits are not exceeded.

### 7.4.1 Description

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:

a. boration,

b. adequate supply for auxiliary feedwater, and

c. residual heat removal.

These systems are identified in the following subsections together with the associated instrumentation and controls provisions. The identification of the monitoring indicators (Subsection 7.4.1.1) and controls (Subsection 7.4.1.2) includes those necessary for maintaining hot standby. The plant can be maintained safely at hot standby for an extended period of time from outside the control room. The Technical Specifications place no time limit on maintenance of hot standby following a control room evacuation. The procedure for maintenance of hot standby following control room evacuation is included in the procedures written by the operating staff. These procedures are available for review at the site.

The plant is placed in hot (shutdown) standby by initiating a reactor trip. This may be done by operator action at the main control room (MCR), at the reactor trip switchgear location, or by tripping the turbine locally or in the MCR.

The equipment and services and approximate time required for a cold shutdown are identified in Subsection 7.4.1.4.

### 7.4.1.1 Monitoring Indicators

The characteristics of these indicators, which are provided outside as well as inside the control room, are described in Section 7.5. The necessary indicators are listed in Table 7.4-1.

7.4.1.2 Controls

7.4.1.2.1 General Considerations

a. The turbine is tripped (note that this can be accomplished at the turbine as well as in the control room).

b. The reactor is tripped (note that this can be accomplished at the reactor trip switchgear as well as in the control room).

c. All automatic systems continue functioning (discussed in Sections 7.2 and 7.7).

d. For equipment having controls outside the control room (which duplicate the functions inside the control room), the controls are provided with a selector switch which transfers control of the switchgear from the control room to a local station. Placing the local selector switch in the local operating position gives an annunciating alarm in the control room and turns off the indicating lights on the control room panel.

7.4.1.2.2 Pumps and Fans

The following pumps and fans are available for safe shutdown. Equipment considered necessary for safe shutdown is powered from ESF buses. Control is provided at the main control board and locally as shown.

| Equipment | ESF Power | MCB Control | Local Control |
|---|---|---|---|
| Auxiliary Feedwater Pumps | Yes | Yes | Yes |
| Centrifugal Charging Pumps | Yes | Yes | Yes |
| Boric Acid Transfer Pumps | No | Yes | Yes |
| Essential Serv. Water Pump | Yes | Yes | Yes |
| Component Cooling Water Pump | Yes | Yes | Yes |
| Reactor Containment Fan Coolers | Yes | Yes | Yes |
| Control Room Ventilation Unit including Control Room Air Inlet Dampers | Yes | Yes | Yes |
| Primary Water Makeup Pumps | No | Yes | Yes |

7.4.1.2.3 Diesel Generators

These units start automatically following a loss of normal a-c power or receipt of a safety injection.

7.4.1.2.4 Valves and Heaters

The following valves and heaters are available for safe shutdown. Valves required for safe shutdown are powered from ESF buses. Control is available from the main control board and locally as shown.

| Equipment | ESF Power | MCB Control | Local Control |
|---|---|---|---|
| Charging Flow Control Valve | No | Yes | Yes |
| Letdown Orifice Isolation Valves | No | Yes | Yes |
| Aux. Feedwater Control Valves | Yes | Yes | Yes |
| Main Steam Dump Valves | No | Yes | No |
| Power-Operated Atmospheric Steam Relief | Yes | Yes | Yes |
| Pressurizer Heater Control | No | Yes | Yes |
| Emergency Boration Isolation Valve | No | Yes | Yes |
| Self-Activated Atmospheric Steam Safety Valves | N/A | N/A | N/A |

The remote shutdown panels, except the one for Train B of the control room ventilation (VC) system, are located at plant elevation 383 feet 0 inch in the radwaste control area. The remote shutdown panel for Train B of the VC system is located at plant elevation 364 feet 0 inch at column/row 23/M in the auxiliary building.

The main control room panels and the remote shutdown panels are located in separate physical locations, on separate elevations, with separate ventilation systems and multiple communication systems, and with lighted access routes between the three locations. Therefore, no single credible event which will cause evacuation of the main control room will also cause the remote shutdown panels to be inoperable or inaccessible.

The remote shutdown panels are provided with the necessary instrumentation and controls for prompt shutdown to the hot standby condition and the ability to maintain the unit in a safe condition pursuant to NRC General Design Criterion 19. See Section 2.4 of the Fire Protection Report for available post fire remote shutdown controls and instrumentation.

7.4.1.3 Control Room Evacuation

It is noted that the instrumentation and controls listed in Subsections 7.4.1.1 and 7.4.1.2 which are used to achieve and maintain a safe shutdown are available in the event an evacuation of the control room is required. See Section 2.4 of the Fire Protection Report for available post fire remote shutdown controls and instrumentation. These controls and instrumentation channels together with the equipment identified in Subsection 7.4.1.4 identify the potential capability for cold shutdown of

the reactor subsequent to a control room evacuation through the use of suitable procedures. The design basis for control room evacuation does not consider a concurrent condition II, III, or IV event, nor a single failure.

7.4.1.4 Equipment and Systems Available for Cold Shutdown

a. Reactor coolant pump (see Subsection 5.4.1).

b. Auxiliary feedwater pumps (see Subsection 10.4.9).

c. Boric acid transfer pump (see Subsection 9.3.4).

d. Charging pumps (see Subsection 9.3.4).

e. Essential service water pumps (see Subsection 9.2.1).

f. Reactor containment fan coolers (see Subsection 6.2.2).

g. Control room ventilation (see Subsection 9.4.1).

h. Component cooling pumps (see Subsection 9.2.2).

i. Residual heat removal pumps (see Subsection 5.4.7) (see Note).

j. Certain motor control center and switchgear sections.

k. Controlled steam release and feedwater supply (see Section 7.7 and Subsection 10.4.7).

1. Boration capability (see Subsection 9.3.4).

m. Nuclear instrumentation system (source range or intermediate range) (see Sections 7.2 and 7.7) (see Note).

n. Reactor coolant inventory control (charging and letdown) (see Subsection 9.3.4).

o. Pressurizer pressure control including opening control for pressurizer relief valves (heaters and spray) (see Subsection 5.2.2) (see Note).

Note

The following equipment is associated with instrumentation and controls which may require some modification in order that their functions may be performed from outside the control room:

a. Residual heat removal pumps.

b. Nuclear instrumentation system (source range or intermediate range).

c. Pressurizer pressure control including opening control for pressurizer relief valves (heaters and spray).

d. Safety injection signal circuit (must be defeated).

e. Accumulator isolation valves (closed).

Note that the reactor plant design does not preclude attaining the cold shutdown condition from outside the control room. An assessment of plant conditions can be made on the long-term basis (a week or more) to establish procedures for making the necessary physical modifications to instrumentation and control equipment in order to attain cold shutdown. During such time the plant could be safely maintained at hot shutdown condition.

The plant can be taken to cold shutdown from locations outside the control room. This will be demonstrated in Start-Up Test 2.63.35, "Shutdown From Outside the Control Room." This Start-Up Test will satisfy the requirements of Regulatory Guide 1.68.2.

The actions required for this operation are as follows:

a. The reactor will be tripped.

b. Shift Manager will go to the technical support center.

c. Turbine trip and closure of the governor valves, stop valves, reheat stop valves, and intercept valves will be verified.

d. Actuation of safety injection will be checked.

e. The shutdown panel will be manned.

f. Local control will be established at the shutdown panel.

g. Auxiliary feedwater will be verified.

h. A decreasing RCS average temperature will be verified.

i. Pressurizer pressure and level will be verified.

j. Steam generator levels will be verified.

k. Shutdown boron concentration will be established.

l. Intermediate range flux will be verified.

m. Stable plant conditions will be verified.

n. One RCFC (minimum) will be verified to be running.

o. All CRDM exhaust fans will be verified to be running.

p. One RCP (minimum) will be verified to be running.

q. Steam will be dumped manually, using the steam generator PORVs to cool the plant.

r. Charging pump suction will be switched to the RWST.

s. Letdown flow will be reduced by selection of the 45 gpm orifice block valve.

t. VCT level will be monitored.

u. Steam generator level will be maintained.

v. Pressurizer level will be verified.

w. Pressurizer heaters will be turned off and auxiliary spray will be used to reduce RCS pressure.

x. Safety injection will be blocked.

y. The accumulator isolation valves will be closed as RCS pressure is reduced to below 1000 psig.

z. RCS pressure and temperature will be reduced to conditions for RH initiation.

aa. Temporary air regulators will be installed for local control of the RH throttle valves.

bb. An additional component cooling pump will be started.

cc. The component cooling outlet isolation valve from the RH heat exchanger will be opened.

dd. A RH pump will be started.

ee. RH boron concentration will be established.

ff. The RH pump will be stopped.

gg. The RH pump suction will be switched to the hot legs.

hh. The RH pump will be started.

ii. The RH throttle valves will be used to control the cooldown.

The required equipment and instrumentation is located at the shutdown panel (383-N-23) except as follows:

a. The reactor trip switchgear is located in the auxiliary building 451 elevation.

b. The turbine trip verification will occur on the turbine deck 451 elevation.

c. Charging pump suction will be switched by the use of jumpers at the MCCs for the valves.

d. Safety injection will be blocked by the use of jumpers in the auxiliary electric room.

e. Groups C and D pressurizer heaters will be deenergized at the 480V feed breakers.

f. The accumulator isolation valves will be closed by the use of jumpers at the MCCs for the valves.

g. The RH throttle valves will be controlled locally.

h. The RH pump will be started and stopped at the 4160V switchgear.

i The component cooling outlet isolation valve from the RH heat exchanger will be opened by the use of a jumper at the valve MCC.

j. The RH pump suction will be switched to RCS hot leg by the use of jumpers at valves MCCs.

k. Train B components of the VC System will be operated as required from the remote shutdown panel at elevation 364 feet 0 inch of the auxiliary building. Note that Train A components of the VC System are on the shutdown panel at elevation 383 feet 0 inch (N-23).

All equipment and instrumentation required for cold shutdown is accessible. Keys, jumpers, self-contained emergency breathing apparatus, and other equipment is available at the shutdown panel.

7.4.2 Analysis

Hot standby is a stable plant condition, automatically reached following a plant shutdown. The hot standby condition can be maintained safely for an extended period of time. In the unlikely event that access to the control room is restricted, the plant can be safely kept at hot standby until the control room can be reentered by the use of the monitoring indicators and the controls listed in Subsections 7.4.1.1 and 7.4.1.2. These indicators and controls are provided outside as well as inside the control room. See Section 2.4 of the Fire Protection Report for available post fire remote shutdown controls and instrumentation.

Safety analyses for individual systems and components listed previously in this section are discussed in their respective UFSAR sections. For example, an analysis of loss of cooling

water to vital equipment is presented with the safety analysis for the essential service water system in Subsection 9.2.1.2.3. This system is redundant and designed to accommodate single failure. The safety analysis for the component cooling water system is presented in Subsection 9.2.2.4. This system is redundant and designed to accommodate single failure. Thus, complete loss of either essential service water or component cooling water is not a credible event.

Furthermore, all equipment which is relied upon to place the unit in a safe shutdown condition and which requires cooling water to operate is redundant so that loss of cooling water to a single piece of equipment will still leave its redundant counterpart in operable condition.

Instrumentation and controls duplicated at either the remote shutdown panels or on local panels are designed to maintain separation and isolation of redundant channels, assure access to appropriate controls at either location in the event of emergencies, and to prevent undue loss of reliability.

For instrumentation and controls mounted locally which duplicate instrumentation and controls mounted in the main control room, separation is maintained throughout the station cable tray and conduit system and the local control panels where the instrumentation and controls are located. A discussion of the cable tray and conduit system is contained in Subsection 8.3.1.4. Local control panels maintain the separation of redundant instruments and controls by the use of internal physical barriers in panels which contain redundant systems or by the use of separate control panels for redundant systems. The remote shutdown panel at elevation 383 feet 0 inches is of the first design with three sections; two sections for the two redundant ESF trains and one section for the non-safety-related trains and all separated by internal physical barriers. The remote shutdown panel for Train B of the VC System at elevation 364 feet 0 inches is of the second design with components of one division with adequate separation or barriers between the one division of Class 1E components and the non-safety related components and wiring.

Normal control of equipment and systems which have duplicated local controls and instrumentation is accomplished in the main control room. In the event of a main control room evacuation, local control functions are established at local control panels which are located in controlled access areas of the station. Access, location, and communications for the remote shutdown panel are discussed in Subsection 7.4.1. For control circuits, local control is established by use of selector switches provided on the local control panels which transfer control from the main control room to the local control panel. A selector switch is provided for each circuit. For the remote shutdown panel, switching to local control causes an annunciator alarm to sound in the main control room. A discussion of the selector switches as applied to the remote shutdown panel is contained in Subsection 7.4.1.2.1.d. Local control panel instrumentation such as analog indicators require no transfer as they are normally energized and operating.

Reliability of instruments and control which locally duplicate instruments and controls in the main control room is maximized by using the same standards for design, procurement, and installation as are used for main control room equipment.

The safety evaluation of the maintenance of shutdown with these systems and associated instrumentation and controls has included consideration of the accident consequences that might jeopardize safe shutdown conditions. The accident consequences that are

germane are those that would tend to degrade the capabilities for boration, adequate supply for auxiliary feedwater, and residual heat removal.

The results of the accident analysis are presented in Chapter 15.0. Of these, the following produce the most severe consequences that are pertinent:

a. uncontrolled boron dilution,

b. loss of normal feedwater,

c. loss of external electrical load and/or turbine trip, and

d. loss of nonemergency a-c power to the station auxiliaries.

It will be shown by these analyses that safety is not adversely affected by these incidents with the associated assumptions being that the instrumentation and controls indicated in Subsections 7.4.1.1 and 7.4.1.2 are available to control and/or monitor shutdown. See Section 2.4 of the Fire Protection Report for available post fire remote shutdown controls and instrumentation. These available systems will allow a maintenance of hot standby even under the accident conditions listed above, which would tend toward a return to criticality or a loss of heat sink.

The results of the analysis which determined the applicability to the nuclear steam supply system safe shutdown systems of the NRC General Design Criteria, IEEE 279-1971, applicable NRC regulations, and other industry standards are presented in Table 7.1-1. The functions considered and listed below include both safety-related and non-safety-related equipment:

a. reactor trip system,

b. engineered safety features actuation system,

c. safety-related display instrumentation for postaccident monitoring,

d. main control board,

e. remote shutdown panel,

f. residual heat removal,

g. instrument power supply, and

h. control systems.

For discussions addressing how these requirements are satisfied, see Table 7.1-1.

TABLE 7.4-1

REMOTE SHUTDOWN MONITORING INSTRUMENTATION

| | INSTRUMENT | READOUT LOCATION | TOTAL NO. OF CHANNELS |
|---|---|---|---|
| 1. | Intermediate Range Neutron Flux | PL06J | 2 |
| 2. | Source Range Neutron Flux | PL06J | 2 |
| 3. | Reactor Coolant Temperature - Wide Range | | |
| | a. Hot Leg | PL05J | 1/loop |
| | b. Cold Leg | PL05J | 1/loop |
| 4. | Pressurizer Pressure | PL06J | 1 |
| 5. | Pressurizer Level | PL06J | 2 |
| 6. | Steam Generator Pressure | PL04J/PL05J | 1/stm gen |
| 7. | Steam Generator Level | PL04J | 1/stm gen |
| 8. | RHR Temperature | LOCAL | 2 |
| 9. | Auxiliary Feedwater Flow Rate | PL04J/PL05J | 2/stm gen |

## 7.5 SAFETY-RELATED DISPLAY INSTRUMENTATION (Regulatory Guide 1.97)

### 7.5.1 Description

Table 7.5-1 lists the information readouts provided to the operator to enable him to perform required manual safety functions, and to determine the effect of manual actions taken following a reactor trip due to a Condition II, III, or IV event, as defined in Chapter 15.0. Table 7.5-1 lists the information readouts required to maintain the plant in a hot standby condition or to proceed to cold shutdown within the limits of the technical specifications. Reactivity control after Condition II and III faults resulting in a reactor trip or a safety injection will be maintained by administrative sampling of the reactor coolant for boron to ensure that the concentration is sufficient to maintain the reactor subcritical.

Table 7.5-2 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.

All safety function actuations are initiated automatically so that no decision or manual action of controls is required by plant operations personnel. All events that automatically initiate auxiliary feedwater require the operator to manually terminate the flow to prevent steam generator overfill. Intelligence of the system responses is provided to the operator by control room instrumentation so that faults in the actuation of safety equipment can be diagnosed. The following main control board devices indicate this intelligence:

a. Three indicating lights are provided for each pump control switch. They indicate pump stopped, pump automatic trip, and pump running. Two indicating lights are provided for each valve control switch. They indicate valve closed and valve open, and both lights are on when the valve is in the intermediate position.

b. Status lights - A light in the status light grouping is provided to indicate that a channel of instrumentation that can initiate a safety function has been actuated.

c. Monitor lights - A light in the monitor light grouping is provided for each pump (running) and for each valve (open, closed) that is an engineered safety feature (ESF). The assignment of a component to a light grouping is determined by that component's operation as follows:

Group 1

Group 1 lights monitor those components whose status is essential for advance readiness to actuate the engineered safety features. These lights should all be dark during normal operation.

Group 2

Group 2 lights monitor those engineered safety features components which must actuate during the injection phase of an accident. These lights should all light for an accident. Some of these lights may be lit during normal operation, for instance component cooling, centrifugal charging, and essential service water pumps and fans running.

Group 3

Group 3 monitors those valves required to close for containment isolation Phase A. They are separated to show pairs of redundant valves subject to closure by the A and B trains. These lights should all light for an accident. Some of these lights may be lit during normal operation, for instance sample line isolation valves.

Group 4

Group 4 monitors those components which must be changed to achieve the cold leg recirculation mode. The transition from injection mode to cold leg recirculation is done manually by the plant operators. This group is used as a guide, realigning 18 valves and restarting the RHR pumps until all lights in this group are lit. Some of the lights may be lit during normal operation or nonaccident cooldowns, such as centrifugal charging and RHR pump lights.

Group 5

Group 5 monitors those components which must be changed to achieve the hot leg recirculation mode. The transition from cold leg recirculation to hot leg recirculation mode is done manually by the plant operators. This group is used as a guide, realigning eight valves and checking that the RHR pumps continue running until all lights in this group are lit. Some of the lights may be lit during normal operation or nonaccident cooldowns, such as centrifugal charging and RHR pump lights.

Group 6

Group 6 monitors those components which actuate on a high-high or a high-high-high containment pressure signal, including the containment spray system components, containment isolation Phase B components, and the main steam isolation valves. In nonaccident conditions, these lights will usually be all dark except during system testing or isolation of a steam generator.

Additional information pertaining to the monitor lights is as follows:

1. A mechanism for testing light bulbs is provided in each light group.

2. Group 1 is dark for normal operations. Groups 2 and 6 are lit for accident conditions as defined above, and in some instances may have several lights lit during various normal operations.

3. When a monitor light is energized, the statement written on the window is true.

Since all the lights in a particular grouping operate in the same manner, a component failure is readily apparent.

d. Pump motor ammeters - provided for engineered safety feature pump motors supplied from 4160-volt buses.

No credit is taken for the annunciator and computer systems as an information display since they are not designed as engineered safety features. However, this does not preclude their availability as a useful diagnostic tool in a postincident review.

7.5.2 Analyses

The indicator channels (see Table 7.5-1) required to enable the operator to take the correct action during the course of a Condition II, III, or IV accident or during postaccident recovery were designed to the criteria listed in Subsection 7.5.3.

The indicators in Table 7.5-1 are used for the operational monitoring of the plant and are thus under surveillance by the operator during normal plant operation. The indicators are functionally arranged on the control board to provide the operator with ready understanding and interpretation of plant conditions. Comparisons between duplicate information channels or between functionally related channels will enable the operator to readily identify a malfunction in a particular channel. The range of the readouts extends over the maximum expected range of the variable being measured. The combined indicated accuracies are within the errors used in the safety analyses, as shown in Table 7.5-1.

The readouts identified in Table 7.5-1 were selected on the basis of sufficiency and availability during and subsequent to an accident for which they are necessary. Thus the occurrence of an accident does not render the information required for that accident unavailable, and the status and reliability of the necessary information are known to the operator before, during, and after an accident.

### 7.5.3 Design Criteria

#### 7.5.3.1 Scope

The scope of IEEE 279-1971 covers protection systems that initiate automatic protective actions. Therefore, in the absence of applicable industry standards for the postaccident monitoring system (PAMS), the following criteria were developed using applicable sections of IEEE 279-1971 as a model.

The environmental and seismic qualification of equipment including these sensors is covered in Sections 3.10 and 3.11.

The following criteria establish requirements for the functional performance and reliability of the safety-related PAMS for nuclear reactors producing steam for electric power generation. For purposes of these criteria, the nuclear power generating station safety-related PAMS encompasses those electric and mechanical devices and circuitry which provide information needed to:

a. enable the operator to take the correct manual action during the course of a Condition II, III, or IV fault or during recovery from a Condition II, III or IV fault; and

b. maintain safe shutdown.

#### 7.5.3.2 Definitions

The definitions in this section establish the meanings of words in the context of their use in these criteria.

Channel - An arrangement of components and modules as required to generate a single information signal to monitor a generating station condition.

Components - Items from which the system is assembled (for example, resistors, capacitors, wires, connectors, transistors, tubes, switches, springs, etc.).

Module - Any assembly of interconnected components which constitutes an identifiable device, instrument, or piece of equipment. A module can be disconnected, removed as a unit, and replaced with a spare. It has definable performance characteristics which

permit it to be tested as a unit. A module could be a card or other subassembly of a larger device, provided it meets the requirements of this definition.

Postaccident Monitoring Function - A postaccident monitoring function consists of the sensing of one or more variables associated with a particular generating station condition, signal processing, and the presentation of visual information (including recorded information) to the operator.

Monitoring System - Where not otherwise qualified, the words "monitoring system" refer to the nuclear power generating station postaccident monitoring system as defined in Table 7.5-1.

Type Test - Tests made on one or more units to verify adequacy of design.

7.5.3.3 Requirements

7.5.3.3.1 General Functional Requirements

The nuclear power generating station PAMS shall function with precision and reliability to continuously display the appropriate monitored variables. This requirement shall apply for the full range of conditions and performance enumerated.

7.5.3.3.2 Information Readout

One of the channels used to monitor each parameter shall also be recorded to provide a historical record of the behavior of the parameters. The equipment used to record information need not be redundant nor meet the single-failure criterion.

7.5.3.3.3 Single-Failure Criterion

Any single failure within the PAMS shall not result in the loss of the monitoring function. ("Single failure" includes such events as the shorting or open-circuiting of interconnecting signal or power cables. It also includes single credible malfunctions or events that cause a number of consequential component, module, or channel failures. For example, the overheating of an amplifier module is a single failure even though several transistor failures result. Mechanical damage to a mode switch would be a "single failure" although several channels might become involved.)

7.5.3.3.4 Quality of Components and Modules

Components and modules are of a quality that is consistent with minimum maintenance requirements and low failure rates. Quality levels are achieved through the specification of requirements known to promote high quality, such as requirements for design, for the derating of components, for manufacturing, quality control, inspection, calibration, and test.

7.5.3.3.5 Equipment Qualification

Type test data or reasonable engineering extrapolation based on test data shall be available to verify that PAMS equipment shall meet, on a continuing basis, the performance requirements determined to be necessary for achieving the system requirements. Qualification of recorders shall verify operability only following (not during) a seismic event. Accelerating forces associated with the pen during the shake period can cause an ink blur of the record during this period, and in some cases a mechanical loosening of the pens might be encountered. The qualification testing program is discussed in Section 3.10.

7.5.3.3.6 Channel Integrity

All PAMS channels are designed to maintain necessary functional capability including accuracy and range, under extremes of conditions (as applicable) relating to environment, energy supply, and malfunctions.

7.5.3.3.7 Channel Independence

Channels (exclusive of recorders as clarified in Subsection 7.5.3.3.2) that provide signals for the same monitoring function are independent and physically separated to accomplish decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis, and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunction. Malfunctions, accidents, and other unusual events include, for example, fire, explosions, missiles, lightning, earthquakes, etc.

7.5.3.3.8 Power Source

The PAMS display instrumentation is capable of operating independent of offsite power availability.

7.5.3.3.9 Postaccident Monitoring System and Control System Interaction

1. Classification of Equipment

Any equipment that is used for both postaccident monitoring and control functions is classified as part of the PAMS.

2. Isolation Devices

The transmission of signals from the postaccident monitoring equipment for control or monitoring is through isolation devices which are classified as part of the PAMS and meet all the requirements of this UFSAR. No credible failure at the output of an isolation device prevents the associated PAMS channel from

meeting the minimum performance requirements considered in the design bases. Examples of credible failures include short circuits, open circuits, grounds, and the application of the maximum credible a-c or d-c potential (typically 130-Vdc or 118-Vac). A failure in an isolation device is evaluated in the same manner as a failure of other equipment in the PAMS.

7.5.3.3.10 Derivation of System Inputs

Inputs to the monitoring system are derived from signals that are direct measures of the desired variables. In many cases, the channels listed also bear a known relationship to each other during normal plant operation.

7.5.3.3.11 Capability for Sensor Checks

Means are provided for checking, with a high degree of confidence, the operational availability of each system input sensor during reactor operation.

7.5.3.3.12 Capability for Verifying Operability

Means are available for verifying the operability of the monitoring system channels. Identification of malfunctions is adequately identified by cross-checking between duplicate redundant channels or cross-checking between channels that bear a known relationship to each other during normal plant operation.

7.5.3.3.13 Channel Bypass or Removal from Operation (RG 1.47)

The system is designed to permit any one channel to be maintained when required during power operation. During such operation the active parts of the system need not themselves continue to meet the single-failure criterion. As such, monitoring systems comprised of two redundant channels are permitted to violate the single-failure criterion during channel bypass provided that acceptable reliability of operation can be otherwise demonstrated. The bypass time interval allowed for a maintenance operation is specified in Technical Specification 3.3.3.

Bypass indication may be applied administratively or automatically.

7.5.3.3.14 Access to Means of Bypassing

The design permits the administrative control of the means for manually bypassing channels.

7.5.3.3.15 Access to Setpoint Adjustments, Calibration, and Test Points

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

7.5.3.3.16 Identification of Monitoring Functions

Displays are indicated and identified down to the channel level.

7.5.3.3.17 System Repair

The system is designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.

7.5.3.3.18 Identification

In order to provide assurance that the requirements given in this UFSAR can be applied during the design, construction, maintenance, and operation of the plant, the postaccident monitoring system equipment (for example, interconnecting wiring, components, modules, etc.), is identified distinctively to distinguish between redundant portions of the monitoring system. Installed items of equipment, components, or modules mounted in assemblies that are clearly identified as being in the monitoring system do not themselves require identification.

TABLE 7.5-1

MAIN CONTROL BOARD INDICATORS AND/OR RECORDERS
AVAILABLE TO THE OPERATOR (CONDITION II, III AND IV EVENTS)*

1. Wide Range $T_{hot}$ and $T_{cold}$

a. Minimum Requirement

A minimum of two $T_{hot}$ and two $T_{cold}$ indicator channels. The $T_{hot}$ channels must be on separate power supply from the $T_{cold}$ channels. Capability of recording either $T_{hot}$ or $T_{cold}$ in one non-isolated loop must be provided.

b. Range - 0 to 700°F.

| Purpose | Indicated Accuracy |
|---|---|
| 1. Maintain the plant in a safe shutdown condition | ± 8% of full range |
| 2. Ensure proper cooldown rate | ± 8% of full range |
| 3. Ensure proper relationship between system pressure and temperature. | ± 8% of full range |

2. Pressurizer Water Level

a. Minimum Requirement

Two channels on separate power supplies with one channel recorded.

b. Range - entire distance between taps.

* Station specific indicated accuracies found in calculation BRW-99-0017-1/BYR-99-010.

TABLE 7.5-1 (Cont'd)

| c. Purpose | Accuracy |
|---|---|
| 1. Maintain proper reactor coolant inventory | Sufficient accuracy to indicate water level is above pressurizer heaters and below 100% of span. (about ± 25% of span) |
| 2. Determine return of water level to pressurizer folllowing steam break and steam generator tube ruptures. | Same as above |

3. System Wide Range Pressure

a. Minimum Requirement

Two channels on separate power supplies with one channel recorded.

b. Range - 0 to 3000 psi.

| c. Purpose | Accuracy |
|---|---|
| 1. Ensure proper relationship between system pressure and temperature. | ± 8% of full range |

4. Containment Pressure

a. Minimum Requirement

Two channels on separate power supplies. Means must be provided to record one of the channels following a high energy line break inside containment

b. Range - 0 to 115% of containment design pressure

| c. Purpose | Accuracy |
|---|---|
| 1. Monitor containment conditions following primary or secondary system break inside containment. | ± 4% of full scale |

TABLE 7.5-1 (Cont'd)

5. Steamline Pressure

a. Minimum Requirement

Two channels per steamline on separate power supplies with one channel per steamline recorded.

b. Range - 0 to 1300 psig.

| c. Purpose | Accuracy |
|---|---|
| 1. Needed to determine type of accident that has occurred and the proper recovery procedure to use | ± 4% of full scale |
| 2. Determine that plant is in a safe shutdown condition. | ± 4% of full scale |

6. Steam Generator Water Level (narrow or wide range)

a. Minimum Requirement

Two narrow range channels per steam generator on separate power supplies with one channel recorded for each steam generator. Although the requirement identifies two narrow range channels, the intent of the requirement is also satisfied by one narrow range and one wide range channel, either of which must be recorded.

b. Range - 0 to 100% of span for both wide or narrow range.

| c. Purpose | Accuracy |
|---|---|
| 1. Maintain adequate heat sink following an accident | Narrow range: sufficient accuracy to indicate that water level is between 0 and 100% of span |
| 2. Needed in recovery procedure following steam generator tube rupture | |

TABLE 7.5-1 (Cont'd)

| | | | |
|---|---|---|---|
| | 3. Ensure that steam generator tubes are covered following a LOCA. | | |
| 7. | Refueling Water Storage Tank Level | | |
| | a. Minimum Requirement<br><br>Two channels on separate power supplies. Means must be provided to record one of the channels following a safety injection signal. | | |
| | b. Range - 0 to 100% of span. | | |
| | c. Purpose | Accuracy | Time Needed After Accident |
| | 1. Determine when to perform the neces-cessary manual actions following switchover from the injection phase to the recirculation phase of safety injection after a LOCA. | ± 3% of level span | 12 hours |

TABLE 7.5-2

CONTROL ROOM INDICATOR AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION

| PARAMETER | NUMBER OF CHANNELS AVAILABLE | RANGE | INDICATED ACCURACY* | INDICATOR/ RECORDER | LOCATION | NOTES |
|---|---|---|---|---|---|---|
| NUCLEAR INSTRUMENTATION | | | | | | |
| 1. Source Range | | | | | | |
| a. Count rate | 2 | 1 to $10^6$ counts/ sec | ±7% of the linear full scale analog voltage | Both channels indicated. Either may be selected recording. | Control board | One recorder is used to record any of the 8 nuclear channels (2 source range, 2 intermediate range and 4 power range) |
| b. Count Rate** (Post Accident Neutron Monitors) | 2 | 0.1 to $10^5$ counts/ sec | ±2% of the linear full scale analog voltage | Both channels indicated. Both channels may be selected recording on plant computer. | Control board | Source range indication provided by Post Accident Neutron Monitoring Instrumentation allowed for satisfying Technical Specification 3.9.3 in Mode 6. Does not provide startup rate indication. |

*Includes channel accuracy and environmental effects. Indicated accuracies provided by NSSS vendor (historical).

**Channel indication may be used during Mode 6 to satisfy Technical Specification 3.9.3.

TABLE 7.5-2 (Cont'd)

CONTROL ROOM INDICATOR AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION

| PARAMETER | NUMBER OF CHANNELS AVAILABLE | RANGE | INDICATED ACCURACY* | INDICATOR/ RECORDER | LOCATION | NOTES |
|---|---|---|---|---|---|---|
| NUCLEAR INSTRUMENTATION | | | | | | |
| c. Startup rate | 2 | -0.5 to 5.0 decades/min | ±7% of the linear full scale analog voltage | Both channels indicated. | Control board | |
| 2. Intermediate Range | | | | | | |
| a. Flux level | 2 | 8 decades of neutron flux (corresponds to 0 to full scale analog voltage) over-lapping the source range<br><br>by 2 decades | ±7% of the linear full scale analog voltage and ±3% of the linear full scale voltage in the range of $10^{-4}$ to $10^{-3}$ amps ($10$ to $10^{2}$% RTP at Byron) | Both channels indicated. Either may be selected for recording using the recorder in Item 1 above. | Control board | |

*Includes channel accuracy and environmental effects.

TABLE 7.5-2 (Cont'd)

| PARAMETER | NUMBER OF CHANNELS AVAILABLE | RANGE | INDICATED ACCURACY* | INDICATOR/ RECORDER | LOCATION | NOTES |
|---|---|---|---|---|---|---|
| b.Startup rate | 2 | -0.5 to 5.0 decades/min | ±7% of the linear full scale analog voltage | Both channels indicated | Control board | |
| 3. Power Range | | | | | | |
| A.Uncalibrated ion chamber current (top and bottom uncompensated ion chambers) | 4 | 0 to 120% of full power current | ±1 of full power current | All 8 current signals indicated. | NIS racks in control room | |
| b.Calibrated ion chamber current (top and bottom uncompensated ion chambers) | 4 | 0 to 125% of full power current | ±2% full power current | All 8 current signals recorded (four recorders). Recorder 1 - upper currents for two diagonally opposed detectors. Recorder 2 - upper currents for remaining detectors. Recorder 3 - lower currents for two diagonally opposed detectors. Recorder 4 - lower currents for remaining detectors. | Control board | |

TABLE 7.5-2 (Cont'd)

| PARAMETER | NUMBER OF CHANNELS AVAILABLE | RANGE | INDICATED ACCURACY* | INDICATOR/ RECORDER | LOCATION | NOTES |
|---|---|---|---|---|---|---|
| c. Upper and lower ion chamber current difference | 4 | -60 to +60% | ±3% of full power | Diagonally opposed channels may be selected for recording at the same time using recorder in Item 1. | Control board | |
| d. Average flux of the top and bottom ion chamber | 4 | 0 to 120% of full power | ±3% full power for indication ±2% for recording | All 4 channels indicated. Any 2 of the four channels may be recorded using recorder in Item 1 above | Control board | |
| e. Average flux of the top and bottom ion chambers | 4 | 0 to 200% of full power | ±2 of full power to 120% ±6% of full power to 200% | All 4 channels recorded | Control board | |
| f. Flux difference of the top and bottom ion chambers | 4 | -30 to 30% | ±4% | All 4 channels indicated. | Control board | |
| REACTOR COOLANT SYSTEM | | | | | | |
| 1. $T_{average}$ (measured) | 1/loop | 530° - 630°F | ±4°F | All channels indicated. | Control board | |

TABLE 7.5-2 (Cont'd)

| PARAMETER | NUMBER OF CHANNELS AVAILABLE | RANGE | INDICATED ACCURACY* | INDICATOR/ RECORDER | LOCATION | NOTES |
|---|---|---|---|---|---|---|
| 2. $\Delta T_{(measured)}$ | 1/loop full power $\Delta T$ | 0 to 150% of | ±4% of full power $\Delta T$ channel is selected for recording | All channels indicated. One | Control board | |
| a. $T_{cold}$ or $T_{hot}$ | 1-$T_{hot}$ | 0 to 700°F | ±4% and one $T_{cold}$ channel for each loop is recorded. | One $T_{hot}$ channel board | Control | |
| (measured, wide range) | 1-$T_{cold}$ per loop | | | Each loop has a separate recorder. | | |
| 3. Overpower $\Delta T$ Setpoint | 1/loop | 0 to 150% of full power $\Delta T$ | ±4% full power $\Delta T$ channel is selected for recording. | All channels indicated. One | Control board | |
| 4. Overtemperature $\Delta T$ Setpoint | 1/loop | 0 to 150% of full power $\Delta T$ | ±4% power $\Delta T$ channel is selected for recording. | All channels indicated. One | Control board | |
| 5. Pressurizer Pressure | 4 | 1700 to 2500 psig | ±28 psi | All channels indicated | Control board | |
| 6. Pressurizer Level | 3 | Entire distance between taps | ±3.5% $\Delta P$ level at 2250 psia | All channels indicated One channel is selected for recording. | Control board | Level recorded along with reference level signal |

TABLE 7.5-2 (Cont'd)

| PARAMETER | NUMBER OF CHANNELS AVAILABLE | RANGE | INDICATED ACCURACY* | INDICATOR/ RECORDER | LOCATION | NOTES |
|---|---|---|---|---|---|---|
| 7. Primary Coolant Flow | 3/loop | 0 to 110% of rated flow | Repeatability of +4.5% of full flow | All channels indicated | Control board | |
| 8. Reactor Coolant Pump Motor Current | 1/loop | 0-1200A | ±2.3% | All channels indicated | Control board | One channel for each pump |
| 9. System Pressure Wide Range | 2 | 0 to 3000 psig | ±4% | All channels indicated and recorded. | Control board | |
| REACTOR CONTROL SYSTEM | | | | | | |
| 1. Demanded Rod Speed | 1 | 0 to 100% of rated speed | ±2% | The one channel is indicated. | Control board | |
| 2. Auctioneered $T_{avg}$ | 1 | 530° to 630°F | ±4°F | The one channel is recorded. | Control board | Any one of the $T_{avg}$ channel into the auctioneer may be bypassed |
| 3. $T_{reference}$ | 1 | 530° to 630°F | ±4°F | The one channel is recorded. | Control board | |
| 4. Control Rod Position | | | | | | If system not available, borate and sample accordingly |
| a. Number of steps of demanded rod withdrawal | 1/group | 0 to 231 steps | ±1 step | Each group is indicated during rod motion. | Control board | These signals are used in conjunction with the measured position signals (4c) to detect deviation of any individual rod from the demanded position. A deviation will actuate an alarm and annunciator. |

TABLE 7.5-2 (Cont'd)

| PARAMETER | NUMBER OF CHANNELS AVAILABLE | RANGE | INDICATED ACCURACY* | INDICATOR/ RECORDER | LOCATION | NOTES |
|---|---|---|---|---|---|---|
| b. Full length rod measured position | 1 for each | 0 to 228 steps | ±4 steps | Each rod position is indicated | Control board | |
| 5. Full length Control Rod Bank Demanded Position | 4 | 0 to 230 steps | ±2.5% of total bank travel | All 4 control rod bank positions are recorded along with the low-low limit alarm for each bank. | Control board | 1. One channel for each control bank.<br>2. An alarm and aunnunciator is actuated when the last rod control bank to be withdrawn reaches the withdrawal limit, when any rod control bank reaches the low insertion limit and when any rod control bank reaches the low-low insertion limit |
| CONTAINMENT SYSTEM | | | | | | |
| 1. Containment Pressure | 4 | 0 to 60 psig | ±3% | All 4 channels indicated and 1 is recorded. | Control board | |
| FEEDWATER AND STEAM SYSTEMS | | | | | | |
| 1. Auxiliary Feedwater Flow | 1/feed line | 0 to 250 | ±4% | All channels indicated. | Control board | Two feed lines per steam generator. One each from Trains A and B. |

TABLE 7.5-2 (Cont'd)

| | PARAMETER | NUMBER OF CHANNELS AVAILABLE | RANGE | INDICATED ACCURACY* | INDICATOR/ RECORDER | LOCATION | NOTES |
|---|---|---|---|---|---|---|---|
| 2. | Steam Generator Level (narrow range) | 4/steam generator | +7 to -5 feet from nominal full load level | ±4% of ΔP level (hot) | All channels indicated. The channels used for control are recorded. | Control board | |
| 3. | Steam Generator Level (wide range) | 1/steam generator | +7 to -41 ft from nominal full load level | +5% of level (cold) | All channels recorded | Control board | |
| 4. | Deleted | | | | | | |
| 5. | Main Feedwater Flow | 2/steam generator | 0 to 120% of maximum calculated flow | ±5% | All channels indicated. The channels used for controls are recorded | Control board | |
| 6. | Magnitude of Signal Controlling Main and Bypass Feedwater Control Valves | 1/main 1/bypass | 0 to 100% of valve opening | ±1.5% | All channels indicated. | Control board. | 1. One channel for each main and bypass feed-water control valve<br>2. OPEN/SHUT indication is provided in the control room for each main and bypass feed-water control valve |

TABLE 7.5-2 (Cont'd)

| PARAMETER | NUMBER OF CHANNELS AVAILABLE | RANGE | INDICATED ACCURACY* | INDICATOR/ RECORDER | LOCATION | NOTES |
|---|---|---|---|---|---|---|
| 7. Steam Flow | 2/steam generator | 0 to 120% of maximum calculated flow | ±5.5% | All channels indicated. The channels used for control are recorded. | Control board | Accuracy is equipment capability; however, absolute accuracy depends on applicant calibration against feedwater flow. |
| 8. Steamline Pressure | 3/loop | 0 to 1300 psig | ±4% | All channels indicated and 1 is recorded | Control board | |
| 9. Steam Dump Modulate Signal | 1 | 0-100% of steam dump valves open | ±1.5% | The one channel is indicated. | Control board | OPEN/SHUT indication is provided in the control room for each steam dump valve |
| 10. Turbine Impulse Chamber Pressure | 2 | 0 to 120% of maximum calculated turbine load | ±3.5% | Both channels indicated. | Control board | OPEN/SHUT indication is provided in the control room for each turbine stop valve |

## 7.6 OTHER SAFETY-RELATED INSTRUMENTATION SYSTEMS

### 7.6.1 Description

See Subsections 7.6.3 through 7.6.6 for descriptions of all other instrumentation systems required for safety not previously addressed.

Additional descriptions for the fire detection and protection systems and the process and effluent radiological monitors are found in Subsection 9.5.1 and Section 11.5 respectively.

### 7.6.2 Analysis

See Subsections 7.6.3 through 7.6.6 for analyses of all other instrumentation systems required for safety not previously addressed.

### 7.6.3 Instrumentation and Control Power Supply System

For a complete description and analysis of the instrumentation and control power supply system, see Subsection 8.3.1.1.2.

### 7.6.4 Residual Heat Removal Isolation Valves

#### 7.6.4.1 Description

The normally closed residual heat removal system (RHR) isolation valves 8701A/B and 8702A/B are opened only for residual heat removal after system pressure/temperature has been reduced to the cooldown setpoint. Their position is indicated at the main control board (MCB) by lights monitoring valve limit switches.

There are two motor-operated valves in series in each of the two RHR pump suction lines from the RCS hot legs.

The valves are interlocked by diverse pressure instruments as shown on Figures 7.6-1 and 7.6-2 so that they cannot be opened unless the RCS pressure is below approximately 360 psig. This interlock prevents the valve from being opened when the RCS pressure plus the RHR pump pressure would be above the RHR system design pressure. An alarm is provided to alert the operator that an RCS-RHR series isolation valve(s) is not fully closed and that double isolation from the RCS to RHR is not being maintained. The logic inputs are from Limitorque limit switches and the hot leg wide-range pressure transmitters (see Subsection 5.4.7.2.3).

7.6.4.2 Analysis

In order to meet NRC requirements and because of the possible severity of the consequences of loss of function, the requirements of IEEE 279-1971 have been applied with the following comments:

1. IEEE 279-1971, Paragraph 4.10: The above mentioned pressure interlock signals and logic are periodically tested. This is done in the interests of

safety, since an actual actuation to permit opening the valve could potentially leave only one remaining valve to isolate the low-pressure residual heat removal system from the reactor coolant system.

2. IEEE 279-1971, paragraph 4.15: This requirement does not apply, as the setpoints are independent of mode of operation and are not changed.

Environmental qualification of the valves and wiring is discussed in Section 3.11.

7.6.5 Refueling Interlocks

Electrical interlocks as discussed in Subsection 9.1.4.3.1 are provided to minimize the possibility of damage to the fuel during fuel handling operations.

7.6.6 Accumulator Motor-Operated Valves

The control circuit for these valves is shown on Figure 7.6-3. The valves and control circuits are further discussed in Subsections 6.3.2 and 6.3.5.

The safety injection system accumulator discharge isolation valves are motor-operated, normally open valves which are controlled from the main control board.

These valves are interlocked such that:

a. They open automatically on receipt of an "S" signal with the main control board switch in either the "AUTO" or "CLOSE" position.

b. They open automatically whenever the reactor coolant system pressure is above the safety injection unblock pressure (P-11) specified in the technical specifications and the main control board switch is in the "AUTO" position.

c. They cannot be closed as long as an "S" signal is present.

The four main control board position switches for these valves provide a "spring return to auto" from the open position and a "maintain position" from the closed position.

The "maintain closed" position is required to provide an administratively controlled manual block of the automatic opening of the valve at pressure above the safety injection unblock pressure (P-11). The manual block or "maintain closed" position is required when performing periodic check valve leakage testing

when the reactor is at pressure. The maximum permissible time that an accumulator valve can be closed when the reactor is at pressure is specified in Technical Specification 3.5.1.

During plant shutdown, the accumulator valves are in a closed position.

When the RCS pressure is above the SI unblock pressure, an alarm sounds in the main control room for any accumulator isolation valve not fully open as indicated by the valve stem limit switch.

### 7.6.7 Switchover from Injection to Recirculation

The details of achieving cold leg recirculation following safety injection are given in Subsection 6.3.2.8 and on Table 6.3-7. Figure 7.6-5 shows the logic which is used to open the sump valves automatically. The semiautomatic transfer signal for this switchover is shown in Figure 7.6-4 and is used for closing the charging pump miniflow motor-operated valves as well (see Figure 7.6-6).

### 7.6.8 Reactor Coolant System Loop Isolation Valve Interlocks

#### 7.6.8.1 Description

The purpose of these interlocks is to ensure that an accidental startup of an unborated and/or cold, isolated reactor coolant loop results only in a relatively slow reactivity insertion rate.

The interlocks are required to perform a protective function. Interlocks are provided to:

a. Prevent the opening of a hot leg loop stop valve unless the cold leg stop valve in the same loop is fully closed.

b. Prevent the starting of a reactor coolant pump unless:

   1. The cold leg loop stop valve in the same loop is fully closed and the loop bypass valve is fully open, or

   2. Both the hot leg loop stop valve and cold leg loop stop valve are fully open.

c. Prevent the opening of a cold leg stop valve unless:

   1. The hot leg loop stop valve in the same loop is open.

   2. The bypass valve in the loop is open.

3. Minimum flow has existed through the relief line for 3 hours.

4. The cold leg temperature is within ~20°F of the highest cold leg temperature in the other loops and the hot leg temperature is within ~20°F of the highest hot leg temperature in the other loops.

The interlocks are a part of the reactor protection system and include the following redundancy:

a. Two independent limit switches to indicate that a valve is fully open.

b. Two independent limit switches to indicate that a valve is fully closed.

c. Two differential pressure switches in each line which bypasses a cold leg loop stop valve to determine that flow exists in the line. Flow through the line indicates:

   1. The valves in the line are open.

   2. The pump in the isolated loop is running.

The interlocks meet the IEEE-279-1971 criteria and, therefore, cannot be negated by a single failure. The interlock on hot leg temperatures is a backup for the interlock on cold leg temperatures. Thus, the single failure criterion applies to the combination and not to each separately.

Figure 7.6-9 shows a reactor coolant loop with loop isolation valves and also shows the cold leg loop isolation valve bypass line.

### 7.6.9 Interlocks For RCS Pressure Control During Low Temperature Operation

The basic function of the RCS pressure control during low temperature operation is discussed in Subsection 5.2.2.11. As noted in Subsection 5.2.2.11 this pressure control includes manually armed

semiautomatic actuation logic for two pressurizer power operated relief valves (PORVs). The function of this actuation logic is to continuously monitor RCS temperature and pressure conditions, with the actuation logic only unblocked by the manual ARM position on the PORV control switch when plant operation is at a temperature below the Technical Specification requirement of 350°F. The monitored system temperature signals are processed to generate the reference pressure limit program which is compared to the measured pressure.

The function of this actuation logic is to continuously monitor RCS temperature and pressure conditions, compare them with the reference nil ductility temperature (RNDT) and pressure limits, as shown in Pressure Temperature Limits Report (PTLR) Figure 3.1 and Table 3.1, and generate a signal to open the PORV if the pressure conditions exceed allowable limits. The actuation logic will function only if the PORV hand switch is in the manual ARM position. See Figure 7.6-10 for the block diagram showing the interlocks for RCS pressure control during low temperature operation.

As shown in this figure, the station variables required for this interlock are channelized as follows:

a. Protection Set I
   1. wide range RCS temperature from hot legs and
   2. wide range RCS system pressure (PT 407).

b. Protection Set II
   1. wide range RCS temperature from cold legs.

c. Protection Set IV
   1. wide range RCS system pressure (PT 406).

The wide range temperature signals, as inputs to the Protection Sets I and II, continuously monitor RCS temperature conditions whenever plant operation is at a temperature below the RNDT. In Protection Set I, the existing RCS hot leg wide range temperature channels supply through an isolation device continuous analog input to an auctioneering device, which is located in the process rack of control rack Group 1. The lowest reading is selected and input to a function generator which calculates the reference pressure limit program considering the plant's allowable pressure and temperature limits. Also available from Protection Set I is the wide range RCS system pressure signal which is sent through an isolation device to control rack Group 1. The reference pressure from the function generator is compared to the actual RCS system pressure monitored by the wide range pressure channel. The error signal derived from the difference between the reference pressure and the actual measured pressure, will first annunciate a main board alarm whenever the actual measured pressure approaches, within a predetermined amount, the reference pressure. On a further increase in measured pressure, the error signal will generate an annunciated actuation signal. The actuation signal available from control rack Group 1 will control PORV "A" whenever a manually armed permissive signal from control

Group 4 is present. The manually armed permissive to the PORVs actuation device is a signal which is turned on only when the MCB four-position PORV control switch is placed in the ARM position. When it is in the AUTO position (normal operating conditions) the actuation signal is at a temperature greater than the range of concern. This will prevent unnecessary system actuation when at normal RCS operating conditions as a result of a failure in the process sensors.

The PORV control switch is placed in the ARM position when the low auctioneered RCS temperature signal reaches a low setpoint value which is indicated by an annunciated actuation signal. The monitored generating station variables that generate the actuation signal for the "B" PORV are processed in a similar manner. In the case of PORV "B", the reference temperature is generated in control rack Group 4 from the lowest auctioneered wide range cold leg temperature, the auctioneering device deriving its inputs from the RCS wide range temperature in Protection Set II, and the actual measured pressure signal is available from Protection set IV. Therefore, the generating station variables used for PORV "B" are derived from protection sets that are independent of the set from which generating station variables used for PORV "A" are derived. The error signal derivation itself used for the actuation signals is available from the control group.

Upon receipt of the actuation signal and with the PORV control switch in the ARM position, the actuation device will automatically cause the PORV to open. Upon sufficient RCS inventory letdown, the operating RCS pressure will decrease, clearing the actuation signal. Removal of this signal causes the PORV to close.

7.6.9.1 Analysis of Interlock

Many criteria presented in IEEE 279-1971 and IEEE 338-1971 standards do not apply to the interlocks for RCS pressure control during low temperature operation, because the interlocks do not perform a protective function but rather provide automatic pressure control at low temperatures as a backup to the operator. However, although IEEE 279-1971 criteria do not apply, some advantages of the dependability and benefits of an IEEE 279-1971 design have occurred by including the pressure and temperature signal elements as noted above in the protection sets and by organizing the control of the two PORVs (either of which can accomplish the RCS pressure control function) into dual channels wherever practical. Either of the two PORVs can accomplish the RCS pressure control function.

The design of the low temperature interlocks for RCS pressure control includes the following features:

a. No credible single failure at the output of the protection set racks, after the output leaves the racks

to interface with the interlocks, will prevent the associated protection system channel from performing its protective function because such outputs that leave the racks go through an isolation device as shown in Figure 7.6-10 and because there are no shared components between channels.

b. Testing capability for elements of the interlocks within (not external to) the Protection System is consistent with the testing principles and methods discussed in Subsection 7.2.2.2.3. It should be noted that there is an annunciator which provides an alarm when there is low auctioneered RCS temperature (below RNDT) coincident with a closed position of the motor operated (MOV) pressurizer relief block valve. This MOV is in the same fluid path as the PORV, with a separate MOV used and alarmed associated with the second PORV.

c. A loss of offsite power will not defeat the provisions for an electrical power source for the interlocks because these provisions are through onsite power which is described in Section 8.3.

## 7.6.10 Instrumentation for Mitigating Consequences of Inadvertent Boron Dilution

### 7.6.10.1 Description

Instrumentation is provided to mitigate the consequences of inadvertent addition of unborated, primary grade water into the reactor coolant system.

The primary indication of a potential boron dilution transient in Modes 3, 4 and 5 is an increase in VCT volume as measured by redundant VCT level channels. These channels alarm in the main control room on high VCT level at 70%. In addition, alarm inputs from Train A and Train B source range flux doubling, and CV112A control valve not in VCT position, are available to alert the operators to the potential of a boron dilution transient. A boron dilution transient can be administratively terminated by aligning the CVCS valves to the RWST to inject borated water into the reactor (reference NRC Docket Nos. STN 50-456, STN 50-457, STN 50-454, and STN 50-455, Subject: Request for Technical Specifications Change, Removal of the Automatic Actuation Features of the Boron Dilution Protection System).

### 7.6.10.2 Analysis

The analysis of effects and consequences of inadvertent boron dilution transient is covered in Subsection 15.4.6.

### 7.6.10.3 Qualification

Qualification of the instrumentation is discussed in Sections 3.10 and 3.11.

## 7.6.11 Charging Pump Miniflow Valve Interlocks

Two solenoid actuated charging pump miniflow control valves (CV8114 and CV8116) are provided with actuation logic to isolate the miniflow lines for the centrifugal charging pumps (see Subsection 6.3.2.2) on low RCS pressure in conjunction with an "S" signal. These valves open to protect the pumps should the RCS pressure increase above their "open" setpoint with an "S" signal present (see Figures 7.6-7 and 7.6-8). In addition to the solenoid actuated charging pump miniflow control valves, two motor-operated charging pump miniflow valves (CV8110 and CV8111) are also provided to isolate the miniflow lines at the time of switchover from safety injection to cold leg recirculation. This isolation is automatic when the refueling water storage tank (RWST) water level drops to the low-low setpoint in conjunction with an "S" signal (see Figures 7.6-4 and 7.6-6). In all four miniflow valves (2 that are solenoid actuated and 2 that are motor-operated), the "S" signal logic retains the "S" signal by retentive memory logic which can be reset at the control board.

## 7.6.12 References

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

2. The Institute of Electrical and Electronic Engineers, Inc., "IEEE Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection System", IEEE 338-1971.

## 7.7 CONTROL SYSTEMS NOT REQUIRED FOR SAFETY

The general design objectives of the plant control system are:

a. to establish and maintain power equilibrium of the primary and secondary system during steady-state unit operation;

b. to constrain operational transients so as to preclude unit trip and reestablish steady-state unit operation; and

c. 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.

d. To provide a back-up for the reactor protection system and mitigate the consequences of an Anticipated Transient Without Scram (ATWS) event.

### 7.7.1 Description of Control Systems Not Required for Safety

The plant control systems described in this section perform the following functions:

a. Reactor Control System

1. Enables the nuclear plant to accept a step load increase or decrease of 10% and a ramp increase or decrease of 5% per minute within the load range of 15% to 100% without reactor trip, steam dump, or pressurizer relief actuation, subject to possible xenon limitations.

2. 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.

b. Rod Control System

1. 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.

2. Systems for monitoring and indicating

   a) Provide alarms to alert the operator if the required core reactivity shutdown margin is not available due to excessive control rod insertion.

b) Display control rod position.

c) Provide alarms to alert the operator in the event of control rod deviation exceeding a preset limit.

c. Plant Control System Interlocks

1. Prevent further withdrawal of the control banks when signal limits are approached that predict the approach of a DNBR limit or kW/ft limit.

2. Inhibit automatic turbine load change as required by the nuclear steam supply system.

d. Pressurizer Pressure Control

1. 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.

2. Provides steam relief by controlling the power relief valves.

e. Pressurizer Water Level Control

1. Establishes, maintains, and restores pressurizer water level within specified limits as a function of the average coolant temperature. 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.

f. Steam Generator Water Level Control

1. Establishes and maintains the steam generator water level within predetermined limits during normal operations.

2. Restores the steam generator water level to within predetermined limits at unit trip conditions.

3. Regulates the feedwater flow rate such that under operational transients the heat sink for the reactor coolant system is maintained.

g. Steam Dump Control

1. Permits the nuclear plant to accept a sudden loss of load (within limits) without incurring reactor trip. Steam is dumped to the condenser as necessary to accommodate excess power generation in the reactor during turbine load reduction transients.

2. Ensures that stored energy and residual heat are removed following a reactor trip to bring the plant to equilibrium no load conditions without actuation of the steam generator safety valves.

3. Maintains the plant in an equilibrium no load condition while steam flow is varying to the turbine during roll to synchronous speed.

4. Permits a manually controlled cooldown of the plant.

h. Incore Instrumentation

Provides information on the neutron flux distribution and on the core outlet temperatures at selected core locations.

i. Power Distribution Monitoring System (PDMS)

PDMS relies on the BEACON core monitoring software coupled with inputs from various plant instrumentation. PDMS continuously monitors the margins to the limits in the core and alerts the operator to violations of the applicable limits for $F_Q(Z)$, $FN\Delta H$, or DNBR. PDMS receives data from the following instrumentation via the process computer:

1. Core Exit Thermocouples (CETC)
2. Excore Power Range Neutron Detectors
3. Reactor Power
4. Control Rod Positions
5. RCS Cold Leg Temperatures
6. Movable Incore Detector system (fluxmap for calibration)

j. ATWS Mitigation System (see subsection 7.7.1.21)

Trips the main Turbine and initiates the Auxiliary Feedwater System whenever three-out-of-four steam generator levels are greater than 3% below the RPS low-low setpoint, and the Turbine Impulse pressure is greater than C-20 setpoint (30% of nominal full power).

### 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 increase or decrease of 10% and ramp increases or decreases of 5% per minute within the load range of 15% to 100% 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 narrow range hot leg and cold leg measurements in each reactor coolant loop. There is an average coolant temperature ($T_{avg}$) computed for each loop, where:

$$T_{avg} = \frac{T_{hot} + T_{cold}}{2} \qquad (7.7\text{-}1)$$

The error between the programmed reference temperature (based on turbine impulse chamber pressure) and the highest of the $T_{avg}$ measured temperatures (which is processed through a lead-lag compensation unit) for each of the reactor coolant loops constitutes the primary control signal as shown in general in Figure 7.7-1 and in more detail on the functional diagrams shown in Drawing 108D685, Sheet 9. 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 (Subsection 7.7.1.3.1) indicates 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 Full Length Rod Control System

#### 7.7.1.2.1 Description

The full length rod control system receives rod speed and direction signals from the reactor control system. The rod speed demand signal varies over the corresponding range of 8 to 72 steps/minute depending on the 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% 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 7.7-1) derived from measurements of turbine impulse chamber pressure prevents automatic rod withdrawal control when the turbine load is below 15%. 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 7.7-1).

The five shutdown banks are always in the fully withdrawn position during normal operation, and are moved to this position at a constant speed by manual control prior to criticality. A reactor trip signal causes them to fall by gravity into the core.

The control banks are the only rods that are manipulated when 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 parallel 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 fed from two separate 480-volt, three-phase buses. Each generator is the synchronous type and is driven by a 200 hp induction motor.

The a-c 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 as well as furnishing control at high speed. A summary of the rod cluster control assembly sequencing characteristics is given below.

a. Two groups within the same bank are stepped such that the relative position of the groups do not differ by more than one step.

b. 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.

c. 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 which continues to move toward its fully withdrawn position. When the second bank reaches a preset position, the third bank begins to move out, and so on. This withdrawal sequence continues until the unit reaches the desired power level. The control bank insertion sequence is the opposite.

   Control banks can only be withdrawn in the proper sequence. Bank A is withdrawn first. When it reaches some preset position, Bank B begins to move.

This preset position determines the overlap between banks, which is limited to a maximum value by the rod control circuitry (overlap < 1/2 fully withdrawn). Due to this consideration, Bank A will be fully withdrawn before Bank C starts to move. Therefore, at any time it is possible for a maximum of two banks to be moving at one time.

d. Overlap between successive control banks is adjustable between 0% (inclusive) to 50% (exclusive) with an accuracy of ± 1 step.

7.7.1.2.2 Features

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:

a. Failures in the manual rod controls:

   1. rod motion control switch (In-Hold-Out), and

   2. bank selector switch.

b. Failures in the overlap and bank sequence program control:

   1. logic cabinet systems, and

   2. power cabinet systems.

Failures in the Manual Rod Controls

The rod motion control switch is a three position level 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 15.0) by the uncontrolled bank withdrawal subcritical and at power transients. The maximum reactivity insertion rate assumed in these analyses due to rod movement is based on 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 $\Delta T$.

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.

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 an 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 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 deenergizing of the lift coil and reduced current energizing of all the stationary gripper coils and the addressed movable gripper coils;

b. activation of the alarm light (urgent failure) on the power cabinet front panel; and,

c. activation of rod control urgent failure annunciation window on the plant annunciator.

The urgent alarm is produced by:

a. regulation failure detector;

b. phase failure detector;

c. logic error detector;

d. multiplexing error detector; or,

e. interlock failure detector.

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 pulses 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 cycle 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 reflect 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 CRDMs.

Surveillance testing of the Rector Control System and the Rod Control System is performed at periodic intervals to detect failures that could lead to an increase in the rod speed.

Failures Causing Movement of the Rods Out of Sequence

No single failure was discovered (WCAP 8976) 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 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.

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.

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 15.0.

### 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% of full power. Suitable alarms are derived from these signals as described below.

Basic power range signals are:

a. Current from the upper half of each power range detector (four such signals).

b. Current from the lower half of each power range detector (four such signals).

Derived from these basic signals are the following (including standard signal processing for calibration).

c. Indicated nuclear power (four such).

d. Indicated axial flux imbalance (AFD) derived from upper half flux minus lower half flux (four such).

Alarm functions derived are as follows:

e. Deviation (maximum minus minimum) in indicated nuclear power.

f. Upper radial tilt (maximum to average) on upper-half currents.

g. Lower radial tilt (maximum to average) on lower-half currents.

Provision is made to continuously record, via recorders on the control board, the 8 ion chamber signals, i.e., upper and lower currents for each detector. Nuclear power and axial imbalance is selectable for recording as well. Indicators are provided on the control board for nuclear power and for axial flux imbalance.

The Axial Flux Difference deviation (AFD) alarms are derived from the plant process computer which determines the 1-minute averages of the excore detector outputs to monitor AFD in the reactor core and alerts the operator to AFD alarm conditions. Above a preset power level, an alarm message is output immediately upon determining a delta flux exceeding a preset band specified in the Core Operating Limits Report (COLR) on a cycle specific basis or the latest valid PDMS surveillance report, whichever is more conservative. For periods during which the flux difference alarm is inoperable, the axial difference is logged as described in station procedures.

Additional background information on the nuclear instrumentation system can be found in Reference 1.

7.7.1.3.2 Rod Position Monitoring

Two separate systems are provided to sense and display control rod position as described below:

a. Digital Rod Position Indication System

The digital rod position indication system measures the actual position of each 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 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 system can continue to function (at reduced accuracy) when one channel fails. Multiplexing is then used to transmit the digital position signals from the containment electronics to the control board display unit.

The control board display unit contains a column of light-emitting-diodes (LEDs) for each rod. At any given time, the one LED illuminated in each column shows the position for that particular rod. Since shutdown rods are always fully withdrawn with the plant at power, their position is displayed at ± 4 steps only from rod bottom to 18 steps and from 210 steps to 228 steps. All intermediate positions of the rod are represented by a single "transition" LED. Each rod of the control banks has its position displayed to ± 4 steps throughout its range of travel.

Digital Rod Position Indication (DRPI) provides input data to Power Distribution Monitoring System (PDMS) via the process computer.

Included in the system is a rod at bottom signal for each rod that operates a local alarm. Also a control room annunciator is actuated when any rod is at bottom.

b. 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 control rod position system provides input data to Power Distribution Monitoring System (PDMS) via the process computer.

The demand position and digital rod position indication systems are separate systems. Safety criteria were not involved in the separation; rather it was a result of operational requirements. Operating procedures require the reactor operator to compare the demand and indicated (actual) readings 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 $\Delta T$) and coolant average temperature. These parameters are used to calculate insertion limits for the control banks. Two alarms are provided for each control bank.

a. The "low" alarm alerts the operator of an approach to the rod insertion limits, which may require boron addition as necessary by following normal procedures with the chemical and volume control system.

b. The "low-low" alarm alerts the operator to take action to stop diluting if in progress, and verify Shutdown Margin is within the limits specified in the COLR or initiate boration to restore SDM to within limit.

The purpose of the control bank rod insertion monitor is to give warning to the operator of excessive rod insertion. The insertion limit maintains sufficient core reactivity shutdown margin following reactor trip, provides a limit on the maximum inserted rod worth in the unlikely event of a hypothetical rod ejection, and limits rod insertion 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 $\Delta T$ 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:

$$Z_{LL} = A\ (\Delta T)_{auct} + B(T_{avg})auct + C \qquad (7.7\text{-}2)$$

where:

$Z_{LL}$ = Maximum permissible insertion limit for affected control bank

$(\Delta T)_{auct}$ = Highest $\Delta T$ of all loops

$(T_{avg})_{auct}$ = 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:

If $Z - Z_{LL} \leq D$ a low alarm is actuated.

If $Z - Z_{LL} \leq E$ a low-low alarm is actuated.

The value for "E" is chosen such that the low-low alarm would normally be actuated before the insertion limit is reached. The value for "D" is chosen to allow the operator to follow normal boration procedures, as necessary.

Since the highest values $T_{avg}$ and $\Delta T$ are chosen by auctioneering, a conservatively high representation of power is used in the insertion limit calculation.

The low alarm alerts the operator of an approach to a reduced shutdown reactivity situation. Administrative procedures may require the operator to add boron, as necessary, through the chemical and volume control system. Actuation of the low-low alarm alerts the operator to stop diluting if in progress, and verify Shutdown Margin is within the limits specified in the COLR or initiate boration to restore SDM to within limit.

Figure 7.7-2 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 Drawing 108D685, Sheet 9. 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 Subsection 7.7.1.3.4. This alarm is provided to warn the operator if any shutdown rod cluster control assembly leaves the fully withdrawn position.

Rod insertion limits are established by:

a. Establishing the allowed rod reactivity insertion at full power consistent with the purposes given above.

b. Establishing the differential reactivity worth of the control rods when moved in normal sequence.

c. Establishing the change in reactivity with power level by relating power level to rod position.

d. 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

Figure 7.7-3 is a block diagram of the rod deviation comparator and alarm system implemented by the plant computer.

A rod deviation function is performed as part of the digital rod position indication system where an alarm is generated if a preset limit is exceeded as a result of a comparison of any control rod against the other rods in a bank. The deviation alarm of a shutdown rod is based on a preset insertion limit being exceeded.

The demanded and measured rod position signals are also monitored by the plant computer which provides a visual printout and an audible alarm whenever an individual rod position signal deviates from the other rods in the bank by a preset limit. The alarm can be set with appropriate allowance for instrument error and within sufficiently narrow limits to preclude exceeding core design hot channel factors.

The DRPI system feeds data to the process computer in order to detect and alarm the following conditions:

a. when any 2 rods within the same control bank are misaligned by a preset distance (≥ 12 steps), and

b. when any shutdown rod indicates less than fully withdrawn while at power.

7.7.1.3.5 Rod Bottom Alarm

A rod bottom signal in the digital rod position system is used to operate a control relay which generates the "ROD AT BOTTOM" 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 7.7-1. It is noted that the designation numbers for these interlocks are preceded by "C". The development of these logic functions is shown in the functional diagrams (Drawing 108D685, Sheets 9 through 16).

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 7.7-1. The $C_3$ rod stop derived from overtemperature $\Delta T$ and the C4 rod stop, derived from overpower $\Delta T$ 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 prevents high power operation which, if reached, initiates a reactor trip.

Turbine load reference reduction is initiated by either an overtemperature or overpower $\Delta T$ signal. Two-out-of-four coincidence logic is used.

A rod stop and turbine runback are initiated when:

$$\Delta t > \Delta T_{rod\ stop} \qquad (7.7\text{-}3)$$

for both the overtemperature and the overpower condition.

For either condition in general:

$$\Delta T_{rod\ stop} = \Delta T_{setpoint} - B_p \qquad (7.7\text{-}4)$$

where:

$B_p$ = setpoint bias

For either condition in general:

where $\Delta T$ setpoint refers to the overtemperature $\Delta T$ reactor trip value and the overpower $\Delta T$ reactor trip value for the two conditions.

The turbine runback is continued until $\Delta T$ is equal to or less than $\Delta T_{rod}$ stop.

This function serves to maintain an essentially constant margin to trip.

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 (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. 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. The spray rate

increases proportionately with increasing spray demand signal, reducing pressurizer pressure by condensing steam.

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 in Figure 7.7-4.

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.

A programmed pressurizer water level is maintained by the Chemical and Volume Control System. During normal plant operation, the charging flow varies to produce the flow demand by the pressurizer water level controller. The pressurizer water level is programmed as a function of coolant average temperature, with the highest average temperature (auctioneered) being used. The pressurizer water level decreases as the load is reduced from full load. This is a result of coolant contraction following programmed coolant temperature reduction from full power to low power. The programmed level is designed to match as nearly as possible the level changes resulting from the coolant temperature changes.

To control pressurizer water level during startup and shutdown operations, the charging flow is manually regulated from the main control room.

A block diagram of the pressurizer water level control system is shown in Figure 7.7-5.

7.7.1.7 Steam Generator Water Level Control

Each steam generator is equipped with a three-element feedwater flow controller which maintains a constant water level for normal power operation. The three element feedwater controller regulates the feedwater valve by continuously comparing the feedwater flow signal, the water level signal, the programmed level and the pressure compensated steam flow signal. The feedwater pump speed is varied to maintain a programmed pressure differential between the steam header and the feed pump discharge header. The speed controller continuously compares the actual $\Delta P$

with a programmed $\Delta P_{ref}$ which is a linear function of steam flow. 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. A reactor trip closes the Unit 2 S/G Preheater Bypass Isolation Valves (2FW039A-D). A reactor trip with coincident LO $T_{ave}$ closes the feedwater isolation valves. Manual override of the feedwater control system is available at all times.

A block diagram of the steam generator water level control system is shown in Figures 7.7-6 and 7.7-7.

7.7.1.8 Steam Dump Control

The steam dump system is designed to accept a 50% loss of net load without tripping the reactor.

The automatic steam dump system is able to accommodate this abnormal 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 thereby maintained on the primary system. The rod control system can then reduce the reactor temperature to a new equilibrium value without causing overtemperature and/or overpressure conditions. The steam dump steam flow capacity is 40% of full load steam flow at full load steam pressure.

If the difference between the reference $T_{avg}$ ($T_{ref}$) based on turbine impulse chamber pressure and the lead/lag compensated auctioneered $T_{avg}$ exceeds a predetermined amount, and the interlock mentioned below is satisfied, a demand signal will actuate the steam dump to maintain the reactor coolant system temperature within control range until a new equilibrium condition is reached.

To prevent actuation of 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% step load decrease or a sustained ramp load decrease of 5%/min.

A block diagram of the steam dump control system is shown on Figure 7.7-8. A description of the turbine bypass system is provided in Subsection 10.4.4.

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 lead/lag compensated auctioneered $T_{avg}$ and the reference $T_{avg}$ based on turbine impulse chamber pressure.

The $T_{avg}$ signal is the same as that 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 $T_{avg}$ tends to increase, thus generating an immediate demand signal for steam dump. Since control rods are available, in this situation steam dump terminates as the error comes within the maneuvering capability of the control rods.

7.7.1.8.2 Plant Trip Steam Dump Controller

Following a plant trip, as monitored by the reactor trip signal, 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 lead/lag compensated auctioneered $T_{avg}$ and the no load reference $T_{avg}$. When the error signal exceeds a predetermined setpoint the dump valves are tripped open in a prescribed sequence. As the error signal reduces in magnitude indication that the reactor coolant system $T_{avg}$ is being reduced toward the reference no-load value, the dump valves are modulated by the trip controller to regulate the rate of removal decay heat and thus, gradually establish the equilibrium hot shutdown condition.

7.7.1.8.3 Steam Header Pressure Controller

Heat removal is maintained by the steam header pressure controller (manually selected with the "steam dump control mode" switch) which controls the amount of steam flow to the condenser. This controller operates the same steam dump valves to the condenser which are used during the initial transient following turbine and 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 7.7-9.

7.7.1.9.1 Thermocouples

Chromel-alumel Type K thermocouples are inserted into guide tubes that penetrate the reactor vessel 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. The system includes two reference junction boxes. The junction box temperatures are monitored by three redundant platinum RTDs included within the box and are input to a processor unit to correct the thermocouple temperatures for the reference temperature ($T_{ref}$).

The Core Exit Thermocouples (CETC) provide input data to Power Distribution Monitoring System (PDMS) via the process computer.

Details of the seismic and environmental qualification can be found in Section 3.10.

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, are dry inside, and serve as the pressure barrier between the reactor water pressure and the atmosphere. Mechanical seals between the retractable thimbles and the conduits are provided at the seal table. 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 table is provided for the retraction operation.

The drive system for the insertion of the miniature detectors consists basically of drive assemblies, 5-path rotary transfer assemblies, and 10-path rotary transfer assemblies, as shown in Figure 7.7-9. The drive system pushes hollow helical wrap cables into the core with the miniature detectors attached to the leading ends of the cables and small diameter sheathed coaxial 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 annular area between guide tubes and thimbles is also used to provide pressure signals for differential pressure transmitters that are used to monitor the refueling cavity level and RCS midloop during refueling operations. The transmitters are isolated during normal operation utilizing the class boundary valves. The level instrumentation is non-safety-related. Level indicators and alarms for refueling cavity level and reactor vessel level are provided on the main control board. The guide tubes utilized to provide this indication for the units are as follows:

| Unit | Guide Tube |
|---|---|
| Byron Unit 1 | N8 and R11 |
| Byron Unit 2 | P9 and R11 |
| Braidwood Unit 1 | P4 and R11 |
| Braidwood Unit 2 | P4 and R11 |

7.7.1.9.3 Control and Readout Description

The control and readout system, located in the control room, provides means for inserting the miniature neutron detectors into the reactor core and withdrawing the detectors while plotting neutron flux versus detector position. Limit switches in each transfer device provide indication of path selection operation. Each gear box drives an encoder for position indication. One five path operation selector is provided for each drive unit to insert the detector in one of five functional modes of operation. One 10-path operation selector is also provided for each drive unit that is then used to route a detector into any one of up to 10 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. A plot (position versus flux level) is initiated with the slow withdrawal of the detectors through the core from top to a point below the bottom of the fueled region of the assembly. 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 for computer analysis.

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% (95% confidence). Measured nuclear peaking factors will be increased by 5% 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 (Brwd only)

This equipment is not operated. The boron concentration measurement system employs a sample measurement device which contains a neutron source and neutron detector located in a shield tank. Piping within the shield tank is arranged to maintain coolant sample flow between the neutron source and the neutron detector. Neutron absorption by the boron in the coolant sample flow reduces the number of neutrons which contact the detector per unit time. Therefore, the time required

to count a fixed number of neutron contacts is variable and dependent upon the concentration of boron solution. Electronic circuitry in the console portion of the boron concentration measurement system accepts an amplified signal from the sample measurement device and converts the signal to a digital display of ppm boron. The digital display is housed in the console, which is located on the main control board.

The boron concentration measurement system is designed for use as an advisory system. It is not designed as a safeguards system or component of a safeguards system. The boron concentration measurement system is not part of a control element or control system, nor is it designed for this use. No credit is taken for this system in any accident analysis; therefore, redundancies of measurement components, self checking subsystems, malfunction annunciations, and diagnostic circuitry are not included in this system. As a general operating aid it provides information as to when additional check analyses are warranted rather than a basis for fundamental operating decisions.

7.7.1.11 Main Steam Isolation Valve Control

Each steam generator main steamline is provided with a hydraulically operated isolation valve with a 4-inch air operated bypass around the valve. Both valves may be manually closed or opened individually from individual control switches located on PM06J, the ESF position of the main control board. Proportional (throttling) control of the main steam isolation bypass valve is available on PM06J. The main steam isolation valves may also be manually closed or opened from the remote shutdown panel - one switch is provided for Train A valves (S/G A and D), and one switch is provided for Train B valves (S/G B and C). A description of isolation valve operation is contained in Subsection 10.3.3. Testing of the main steam isolation valves is discussed in Subsection 7.1.2.6.

Both the isolation valves and the bypass valves will be closed automatically in those situations requiring main steam isolation. These situations are: 2 of 3 containment pressure, HI-2; or low steamline pressure, 2 of 3 in any main steamline; or a high steam pressure rate, 2 of 3 in any steamline. A description of the ESF function of these valves is contained in Subsection 7.3.1. Digital logic diagrams for steamline isolation are shown in Drawings 108D685.

7.7.1.12 Turbine-Generator Controls

The turbine is equipped with a digital electrohydraulic control system which utilizes solid-state electronic devices. The controller generates a control signal which actuates hydraulic control of the governor valves and the reheat steam interceptor valves. The control signal is based on a comparison of signals representing turbine speed and first stage pressure with reference signals representative of load demand. A description

of the turbine generator and its control system is contained in Section 10.2.

Low pressure in the turbine hydraulic emergency trip fluid (sensed by pressure switch) or closure of the turbine stop valves (sensed by limit switches) provide a turbine trip signal to the reactor trip system. Also, a reactor trip will generate a turbine trip signal. A description of the relationship between turbine trip and reactor trip can be obtained from Section 7.2. Testing of the turbine steam inlet valves is described in Subsection 7.1.2.6.

Turbine monitoring and control equipment in the main control room is located in the main control board and operator workstation areas. This equipment includes two human machine interface (HMI) Ovation workstations providing full soft control and equipment status graphics for operating, controlling and testing the turbine. All the turbine supervisory instrumentation associated with turbine vibration, expansion, eccentricity, rotor speed and rotor position can be displayed and trended through these HMI workstations. Control switches for control of auxiliary systems and redundant hard-wired turbine trip pushbuttons are also installed on the main control board.

7.7.1.13 Main Condenser Water Level Control

This system is unrelated to reactor safety. Design of the controls and instrumentation for condenser water level control is determined by standard engineering practices.

The main condenser has a nominal hotwell operating capacity of 80,000 gallons of water. The condenser and its associated control systems are described in Section 10.4. A description of the condensate storage subsystem is contained in Subsection 9.2.6.

Redundant water level instrument channels monitor water level in the hotwell. Each channel includes a standpipe to which the various level instruments are connected. The two standpipes and their associated instruments are on opposite sides of the condenser. Each channel includes a level transmitter, four level controllers, and three level switches. Each of the four controllers provides a pneumatic signal for the positioning of its associated control valves which are the normal overflow, emergency overflow, normal makeup, and emergency makeup valves. (Refer to Drawing M-39, Sheet 1.)

The overflow controls operate by bypassing condensate booster pump discharge flow to the condensate storage tank. The overflow lines are manually isolated; see Subsection 9.2.6.2. The normal makeup control operates by allowing the condensate storage tank to gravity feed the condenser through a 4-inch line. The emergency makeup operates by automatic starting of the condensate makeup pumps which take suction from the condensate storage tank and pump water to the condenser through an 8-inch line. Switches for high and low level alarms are annunciated on main control board. Selection of one of the redundant controllers to drive each of the four control valves is made through a locally mounted, manually operated three-way valve.

### 7.7.1.14 Main Condenser Vacuum Control

This system is unrelated to reactor safety. Design of the controls and instrumentation for it are determined by standard engineering practices.

Two steam jet air ejectors are provided to maintain condenser vacuum at 3.5 inches Hg abs. at design conditions. Additionally, redundant hogging vacuum pumps are provided to establish initial vacuum conditions during startup. Controls for the vacuum pumps are on the main control board (MCB).

Condenser inlet and outlet water boxes are normally gravity fed and vented using the main water box vents. They can be filled with the aid of the priming vacuum pump. The four inlet water boxes are each vented to two priming valves which connect to the priming vacuum pump suction. At Braidwood, the inlet priming valves have been abandoned in place. The four outlet water boxes are each connected to a 40-foot standpipe which connects to a priming tank. A level controller connected to the tank will open a valve connecting the tank vapor space to the priming pump suction on low water level. The valve will close on high water level. The priming system functions to ensure that the condenser water boxes remain full of water and that the four outlet water boxes are at a constant head. Loss of instrument air or electrical power to the priming tank air discharge valve will cause the valve to close. High priming tank water level is annunciated on the MCB. Priming pump controls are also located on the MCB.

### 7.7.1.15 Circulating Water System Controls

This system is unrelated to reactor safety. Design of the controls and instrumentation for the circulating water system is determined by standard engineering practices. A description of the circulating water system is contained in Subsection 10.4.5. This section discusses the C&I features of the system.

Circulating water pumps are normally operated from the main control board. Pump motor current and breaker position are displayed on the MCB.

At Braidwood, circulating water (CW) pump starting is interlocked such that the pumps can only be started if their discharge valve is closed and high pressure exists in the nonessential service water (WS) header which provides cooling water to the CW pump seals and oil cooler.

At Byron, circulating water (CW) pump starting is interlocked such that the pumps can only be started if their discharge valve is closed and high pressure exists in the CW or WS header, since both can provide cooling water to the CW pump seals and oil cooler.

The CW pumps may be stopped by means of the control switch, or by electrical auxiliary motor protection devices. For the Braidwood station, high differential pressures across the intake traveling screens will also trip the CW pumps.

The CW pump discharge valves are interlocked such that they cannot start to open until the CW pump has been running for an adjustable time delay.

CW pump differential pressure indications with low d/P alarms are displayed on the main control board.

Condenser inlet and outlet water box isolation valves are provided on the MCB. One switch is provided for each of the four pairs of isolation valves.

Cooling of the heated circulating water is provided by the natural draft cooling towers at the Byron Station and by the cooling lake for the Braidwood Station. Refer to Subsection 10.4.5 for a description of these systems. The Byron cooling tower controls and instrumentation are available on the cooling tower section of the MCB, general services section of the main control board. These include valve controls and display of CW temperatures and meteorological instrumentation.

Circulating water makeup controls are available on the MCB. At Byron, these include pump and valve controls; makeup, blowdown flow, and intake bay level recorder; and CW pump intake bay level control, indications, and alarms. At Braidwood, these include pump and valve controls, makeup and blowdown flow recorders, and CW makeup pump intake bay low level alarms.

### 7.7.1.16 Condensate/Condensate Booster and Feedwater System Controls

Design of the controls and instrumentation for these systems is determined by standard engineering practices. The portion of the feedwater system that is considered safety-related is defined in Subsection 10.4.7.1.1.

A description of the condensate/condensate booster and feedwater system including control description is contained in Subsection 10.4.7. A description of the condenser water level controls which interface with the condensate storage tank for makeup and overflow control is provided in Subsection 7.7.1.13. A description of the steam generator water level control system is contained in Subsection 7.2.2.3.5. A discussion of testing provisions for the feedwater isolation valves is included in Subsection 7.1.2.6. A discussion of water hammer prevention features is included in Subsection 10.4.7.3.

Feedwater system controls and instrumentation are available in the main control room on the MCB. Steam generator wide range level instrumentation is available on the main control board and also on the remote shutdown panels. Condensate system controls and indications are available on the main control board.

### 7.7.1.17 Process Radiation Monitoring Instruments and Controls

The process radiation monitors include those monitors which sample gaseous and liquid systems. The gaseous monitors sample various HVAC systems and some gaseous process systems such as waste gas. The gaseous and liquid monitors communicate with the digital radiation monitoring system central processor located in

the main control room. Monitor status displays and alarms are available to the operator through the digital radiation monitoring system CRT display and printer located in the main control room. A description of the system and listing of process radiation monitors is included in Section 11.5 and Table 11.5-2, respectively.

7.7.1.18 Area Radiation Monitoring Instruments and Controls

The area radiation monitors include gamma radiation detectors located in various plant areas. The area monitors communicate with the digital radiation monitoring system central processor located in the main control room. Monitor status displays and alarms are available to the operator through the digital radiation monitoring system CRT and printer located in the main control room. A description and listing of area radiation monitors is included in Subsection 12.3.4 and Table 12.3-3, respectively.

7.7.1.19 Liquid Radwaste System Instruments and Controls

The liquid radwaste control panel (LRCP) consists of two panels. It is located in the auxiliary building on the 383-foot elevation. The LRCP is constructed with a semigraphic display in the upper section of the panel, indication and recording in the center section, and controls in the lower section. An annunciator is located at the very top of the panel.

The semigraphic display spans the full length of the panel and depicts the entire liquid radwaste treatment processing system as shown in Drawing M-48A. The semigraphic display enables the operator to quickly grasp the status of the system and maximize the efficiency of the operator's control.

Indication and recording on this panel is located below the corresponding representation of the instrument in the semigraphic display. Parameters monitored include steam generator blowdown flow, blowdown condenser level and pressure, and various liquid radwaste system tank levels and liquid release flow rates. See Table 11.2-9 for a summary of tank level indication and annunciation.

Controls on this panel are also located below the corresponding device representation in the semigraphic. These controls consist primarily of on/off control of pumps and open/close control of valves that are shown in the semigraphic.

An annunciator system is provided on this panel to alert the operator to various abnormal process conditions. The individual annunciator windows are located above the area in the semigraphic in which the alarming device is represented. Parameters annunciated include tank levels, filter differential pressures, and sump levels.

All control, indication, and recording on this panel is non-safety-related. Nothing on this panel is required for safe shutdown of the reactor or required to maintain the reactor in a safe shutdown condition. Refer to Section 11.2 for a complete description of the liquid waste management systems.

7.7.1.20 Leak Detection Instrumentation and Control

Detection of reactor coolant leakage is identified by a number of different mechanisms.

a. Sump Collection

For Byron Unit 1 and Braidwood, all leakage to the containment atmosphere is collected in the reactor cavity sump inlet water box, or in one of the two inlet water boxes provided with the containment floor drain sump. Water collected in the inlet water boxes flows to the main portion of the respective sump through a calibrated weir plate. Water level behind the weir plate is monitored by a water level transmitter. This signal is calibrated in terms of flow through the weir by standard level/flow relationships. A signal representative of flow is derived for each inlet water box and is recorded on a panel in the main control room. Also high flow alarms are annunciated on the ESF and reactor auxiliary portion of the main control boards. Sump pump controls and indications including totalizing run time meters are located on the liquid radwaste control panel.

For Byron Unit 2, all leakage to the containment atmosphere is collected in the reactor cavity sump inlet water box or in the containment floor drain sump. For the reactor cavity drains, water collected in the inlet water box flows to the main portion of the sump through a weir plate. Water level behind the weir plate is monitored by a water level transmitter. This signal is calibrated in terms of flow through the weir by standard level/flow relationships. A signal representative of flow is derived for the inlet water box and is recorded on a panel in the main control room. Water from the containment floor drains flows directly to the containment floor drain sump. The containment floor drain sump water level is monitored by a water level transmitter. This signal is calibrated in terms of flow into the floor drain sump by standard level/flow relationships. Signals from the transmitter provide input to a main control room digital recorder. The recorder is programmed to directly calculate and display flowrate based on the time required for sump level to change.

For all units, a curb is provided around the containment recirculation sump to ensure operational leakage during non-accident conditions is directed to

containment leak detection equipment, where it can be measured.

b. Containment Radiation Monitoring

Containment atmosphere radiation monitoring is used to detect reactor coolant system leakage by use of particulate and gaseous radiation monitors. Indications and alarms are available on the radiation monitoring system CRT and alarm typer located in the main control room. Refer to Subsection 11.5.2.2.10 for a complete discussion of these monitors. Also see Table 11.5-1.

c. Containment Atmospheric Monitoring

Containment atmospheric pressure monitoring is part of the ESFAS discussed in Section 7.3. Containment pressure also serves as an indication of reactor coolant leakage to containment. Indication, alarms, and recordings of these signals are available in the main control room.

Dry bulb temperatures at the reactor containment fan cooler inlet and outlet serve to detect increases in temperature that would accompany a reactor coolant system leak. These

measurements are provided with the reactor containment fan coolers and are read out in the main control room. Refer to Subsection 7.3.1.1.12.

d. Intersystem Leakage

Leakage through the steam generator tubes will be detected using the process radiation monitors that monitor steam generator blowdown. These indications and alarms are available in the main control room. Also, leakage may be detected at the liquid process sampling panel through analysis for the presence of radioisotopes of iodine and sodium. Refer to Subsections 5.2.5.4 and 5.2.5.5.

e. Other Leakage

Leakage from specific valves and equipment is directed to the pressurizer relief tank as shown in Drawings M-60 and M-135. Bullseye flow indicators are provided in these lines. Tank pressure, temperature, and level are indicated and alarmed in the main control room on lPM05J, the reactor controls board.

7.7.1.21 Anticipated Transients Without Scram Mitigation System (AMS)

The ATWS Mitigation System consists of a logic system and a dedicated uninterruptible power supply (UPS) all within one free-standing cabinet. Also contained in this cabinet are safety-related analog and digital isolators to allow interfacing with existing safety-related circuits. The operation of the AMS is defined in Figure 7.7-12 and by the following descriptions.

7.7.1.21.1 System Overview

The required initiating actions of the AMS are as follows:

a. initiate the auxiliary feedwater system, and

b. trip the main turbine.

The plant variable that is monitored to determine loss of heat sink and provide for the actions described above is steam generator (SG) level. Each steam generator is monitored by four existing sets of level instrumentation. Any of the four level measurements indicating low level is an indication of loss of heat sink for that steam generator.

As shown in Figure 7.7-12, one AMS logic train with three logic subsystems is provided. Both the main turbine trip and auxiliary feedwater actuation signals are initiated by this logic train. For reliability, three redundant, identical logic subsystems are provided, and a two-out-of-three coincidence of these logic subsystems is required to initiate actuation.

A single level transmitter from each SG inputs to the three AMS logic subsystems. Each AMS logic subsystem monitors the four RPS SG level inputs. A three-out-of-four coincident logic scheme is employed to interrogate these SG level signals, therefore requiring three of the steam generators to indicate a loss of heat sink in order to actuate each subsystem. The AMS level setpoint will be 3% of the narrow range span below the RPS steam generator low-low level trip setpoint.

Two-out-of-three coincidence of the logic subsystem trips will actuate the auxiliary feedwater system (i.e., motor-driven and diesel-driven auxiliary feedwater pumps and related equipment) and trip the main turbine (through the emergency trip). A time delay (approximately 9 seconds) is provided to ensure the reactor protection system will provide the first trip signal.

Arming of the AMS is automatic and is accomplished when both the C-20 power level (>30% of nominal full power) permissives are achieved (see figure 7.7-12). Upon a decrease in power below the C-20 power level, the AMS will be bypassed automatically after a 360-second time delay. The C-20 power level permissive is developed in the AMS system based on turbine impulse chamber pressure.

After an AMS initiation of the auxiliary feedwater system and tripping of the main turbine, the AMS will self reset. That is, after AMS initiation as power decreases and after a time delay (approximately 360 seconds), the C-20 interlock will inhibit the logic thus allowing shutdown of the auxiliary feedwater system and reset of the main turbine trip. The time delay allows the AMS to remain armed long enough to perform its function in the event of a turbine trip.

The logic provides for one inhibiting signal which is manually implemented under administrative control and prevents the logic from initiating its intended functions (i.e., start the auxiliary feedwater system and trip the main turbine). This inhibiting signal results from the requirement that the AMS must have the capability for testing during power operation. When the operator selects the AMS test/bypass mode, the final AMS actuation output devices (relays) are inhibited from operating and inadvertently initiating the auxiliary feedwater system or tripping the main turbine during power operation.

Control of the auxiliary feedwater system and main turbine are provided for by existing controls and are not in the scope of the AMS design.

7.7.1.21.2 Logic Power Supplies

The AMS logic will be powered through a non-safety related 24-Vdc uninterruptable power supply (UPS).

Normal power to this UPS will be from a 120-Vac, non-safety-related, and non-battery-backed bus. Inside of the AMS cabinet, the UPS power supply and its 120-Vac input power will be isolated by distance and barriers from the rest of the cabinet equipment.

7.7.1.22 Power Distribution Monitoring System (PDMS)

PDMS allows the operator to continuously monitor the margins to the limits in the core and alerts the operator to violations of the applicable limits for $F_Q(Z)$, $F^N_\Delta H$, or DNBR.

7.7.1.22.1 Determination of the Core Power Distribution

The primary function of the BEACON core monitoring system is the determination of the three-dimensional core power distribution. In BEACON, this calculation is performed with the NRC approved Westinghouse SPNOVA nodal method or the ANC Nodal Expansion Method (NEM). The SPNOVA Method employs a single Effective Fast Group (EFG) calculation to determine the global flux solution, and then uses a local correlation to determine the thermal flux and power distribution. The minimum running time required for the BEACON on-line calculation is achieved in SPNOVA by constructing the core-wide Green's function for the fast diffusion equation. The required time-consuming inversions of an EFG equation are avoided by using the precalculated Green's function (Reference 48). The ANC Nodal Expansion Method is slower than the SPNOVA Nodal Method, however is a more rigorous NEM for the spatial flux solution. NEM is based on basic neutron physics and avoids (as much as possible) the use of empirical correlations and data. Utilizing the NEM eliminates the normalization step and automatically assures identical results between SPNOVA and ANC. The Beacon detailed intra-nodal power is calculated by using peaking data tabulated as a function of fuel type and burnup.

7.7.1.22.2 Calibration of the Core Power Distribution

BEACON uses the incore flux detector measurements, core-exit thermocouples and excore detectors to perform the local calibration of the SPNOVA three dimensional power distributions. The SPNOVA predicted detector reaction rates are normalized to the incore measurements at the incore radial locations and over an axial mesh. The thermocouple adjustment is two-dimensional and is made by normalizing the SPNOVA radial power distribution to the assembly power inferred from the core-exit thermocouples. The thermocouple assembly power measurement is periodically calibrated to the incore-measured assembly power. The incore detectors and core-exit thermocouples do not provide complete coverage of the core and BEACON employs a two-dimensional spline fit to interpolate/extrapolate these measurements to the unmonitored assemblies. The spline fit includes a tolerance factor, which controls the degree to which the fit is forced to match the individual measurements. If, for example, the measurements are believed to be extremely accurate (inaccurate), then a low (high) tolerance factor is used and the SPNOVA solution is (not) forced to be in close agreement with the measurements.

The BEACON axial power shape is adjusted to ensure agreement with the axial offset measured by the excore detectors. Adding a sinusoidal component to the SPNOVA calculated axial power shape makes this adjustment. The SPNOVA excore axial offset is determined by an appropriate weighting of the peripheral assembly powers. The excore detector axial offset is periodically calibrated to the incore detector measurement.

7.7.1.22.3 BEACON Core Monitoring Methodology

The BEACON core monitoring process is carried out in three steps. In the first step the SPNOVA model, individual thermocouples and the excore axial offset are calibrated to the full-core incore flux measurement. In the second step, the SPNOVA model is updated based on the most recent operating history, and adjusted using thermocouple and excore measurements. Using thermocouple and excore measurements performs the continuous monitoring by updating the BEACON model in the third step.

The continuous core monitoring of the current reactor statepoint (fuel burnup, xenon distribution, soluble boron concentration, etc.) provided by BEACON allows a more precise determination of the parameters used in transient analysis, and therefore relaxes the requirement to limit the transient initial conditions via power distribution control. As part of the continuous monitoring, the fuel and DNBR limits are calculated using standard Westinghouse methods.

The accuracy of the beacon analysis decreases as the calibration intervals increase and the power distribution diverges from the reference power shape. In order to minimize the Beacon uncertainty, the reference power distribution is updated every 15 minutes, when the axial flux difference (AFD) changes greater than 2%, or when power changes by more than 5%.

The BEACON nuclear/thermal-hydraulic data sets and models are determined using Westinghouse reload design codes and methods. Before BEACON is used for core monitoring, the BEACON model and reference uncertainties are validated. The online DNBR and limits evaluation is performed with NRC approved DNBR methodologies.

In the current Westinghouse transient analysis methodologies, the preconditioned axial power shape is determined subject to the power distribution control limits on axial offset. Since BEACON calculates the three-dimensional power distribution and performs the local limits evaluation online the axial offset limits are relaxed and preconditioned power distribution is only constrained by rod insertion, DNBR, $F^N_{\Delta H}$ and $F_Q$ power peaking limits.

7.7.1.22.4 System Configuration

The BEACON software is located on a dedicated computer and receives input from plant instrumentation via the process computer. The BEACON computer sends the results of its

calculations back to the process computer. The process computer activates control room alarms when the thermal limits are approached or exceeded. The value limit of the alarm is located in the Core Operating Limits Report (COLR) and the values are input into the process computer for the alarm functions. An alarm is activated when either a limit has been approached or exceeded or the BEACON (PDMS) computer determines that it is not functioning correctly. If PDMS becomes inoperable, operator reinstate the QPTR and AFD Tech Specs and the associated actions. The QPTR and AFD Tech Specs are suspended while PDMS is OPERABLE.

7.7.2 Analysis of Control Systems Not Required for Safety

The plant control systems are designed to assure high reliability in any anticipated operational occurrences. Equipment used in these systems 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 assembly from the other rods in the bank position. There is also insertion limit monitors with visual and audible annunciation. A rod bottom alarm signal is provided to the control room for each full length 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 used 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 15.0.

These analyses 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 1.30. 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.

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-Vac or 130-Vdc 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 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 degrading 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 systems.

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 full length 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 the 1971 General Design Criterion 25.

No single electrical and 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 an activation of the same alarm and the same visual indications.

Each bank of rods in the system is divided into two groups (group 1 and group 2) of up to 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 7.7-10, which also shows that one group is always within one step (5/8 inch) of the other group. A definite sequence 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 7.7-11 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.

Figure 7.7-11 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.

a. 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 X1. Upon "up" demand, one rod in group 1 and 4 rods in group 2

would withdraw. A second failure at point X2 in the group 2 circuit is required to withdraw one rod cluster control assembly.

b. 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.

c. 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 2 out of 16 wires connected to the gate of the lift coil thyristors. The probability of open wire (or terminal) failure is $0.016 \times 10^{-6}$ 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. A probability number cannot be assigned to a series of errors such as these.

The rod position indication system provides direct visual display 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 diluting if in progress, and verify Shutdown Margin is within the limits specified in the COLR or initiate boration to restore SDM to within limit. 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. Should a rod be misaligned from the other rods in its bank by ± 12 steps or more, the rod deviation alarm is actuated.

Misaligned rod cluster control assemblies are also detected and alarmed in the control room via the flux tilt monitoring portion of the NIS.

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 the 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% step change in load demand, over the 15 to 100% power range for automatic control. Steam dump is blocked for load decrease less than or equal to 10%. 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, heaters, and power relief valves in the pressurizer.

The control system limits nuclear power overshoot to acceptable values following a 10% increase in load to 100%.

7.7.2.4 Loading and Unloading

Ramp loading and unloading of 5%/min can be accepted over the 15 to 100% 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 is programmed to increase with increased load causing a continuous insurge of coolant to the pressurizer as a result of expansion. The sprays limit the

resulting pressure increase. Conversely, as the coolant average temperature is decreased with decreased load, there is a continuous coolant outsurge from the pressurizer resulting from 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 $\Delta T$ 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.

During rapid loading transients, a drop in reactor coolant temperature is sometimes used to increase core power. This mode of operation is used when the control rods are not inserted deep enough into the core to supply all the reactivity requirements of the rapid load increase (the boron control system is relatively ineffective for rapid power changes). The reduction in temperature is initiated by continued turbine loading past the point where the control rods are completely withdrawn from the core. The temperature drop is recovered and nominal conditions restored by a boron dilution operation.

Excessive drops in coolant temperature can be prevented by interlock C-16. This interlock circuit monitors the auctioneered low coolant temperature indications and the programmed reference temperature which is a function of turbine impulse pressure and can cause a turbine loading stop when the temperature difference reaches the setpoint. This circuitry is available but not currently connected to stop turbine loading. However, it does provide an alarm in the control room when the setpoint is reached.

The core axial power distribution is controlled during the reduced temperature return to power by placing the control rods in the manual mode when the $\Delta\phi$ operating limits are approached. Placing the rods in manual will stop further changes in $\Delta\phi$ and it will also initiate the required drop in coolant temperature. Normally power distribution control is not required during a rapid power increase and the rods will proceed, under the automatic rod control system, to the top of the core. The bite position is reestablished at the end of the transient by decreasing the coolant boron concentration.

### 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 40% of full load steam flow at load steam pressure.

The steam dump flow reduces proportionally as the control rods act to reduce the average coolant temperature stopping on low $T_{avg}$ to prevent excessive cooldown. 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 are modulated depending upon the magnitude of the temperature error signal resulting from loss of load. They can be opened quickly in two groups if they fail to modulate.

7.7.2.6 Turbine-Generator Trip With Reactor Trip

Whenever the turbine-generator unit trips at an operating power level above 30% (P-8) power, the reactor also trips. The unit is operated with a programmed average temperature as function of load, with the full load average temperature significantly greater than the equivalent saturation pressure of the steam generator 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 feedwater to the steam generators.

The steam dump system is controlled from the reactor coolant average temperature signal whose setpoint values are programmed as a function of turbine load. Actuation of the steam dump is rapid to prevent actuation of the steam generator safety valves. When 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 the turbine trip, the feedwater flow is cut off when the reactor trip with low $T_{ave}$ occurs, when the steam generator water level reaches a given high level, or when safety injection occurs.

Makeup from the auxiliary feedwater system is then controlled manually to restore and maintain steam generator water level while assuring that the reactor coolant temperature is at the desired value. Heat removal is maintained as described in Subsection 7.7.1.8.3.

The pressurizer pressure and level fall rapidly during the transient because of coolant contraction. The pressurizer water level is programmed so that the level following the turbine and reactor trip is above the heaters. However, if the heaters become uncovered following the trip, the chemical and volume control system will provide 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 remove heat and prevent excessive cooldown following the trip to ensure adequate reactivity shutdown margin.

## 7.7.3 References

1. J. B. Lipchak and R. A. Stokes, "Nuclear Instrumentation System," WCAP-8255, January 1974 (for background information only).

2. Miller, R.W., et.al., "Relaxation of Constant Axial Offset Control, $F_Q$ Surveillance Technical Specification," WCAP-10216-P-A (Westinghouse Proprietary), February 1994.

3. Beard, C. L., et.al., "BEACON – Core Monitoring and Operations Support System," WCAP-12472-P-A (Proprietary), August 1994.

4. Morita, T., et. al., "BEACON Core Monitoring and Operations Support System (WCAP-12472-P-A) Addendum 1, "WCAP-12472-P-A Addendum 1A (Westinghouse Proprietary), January 2000.

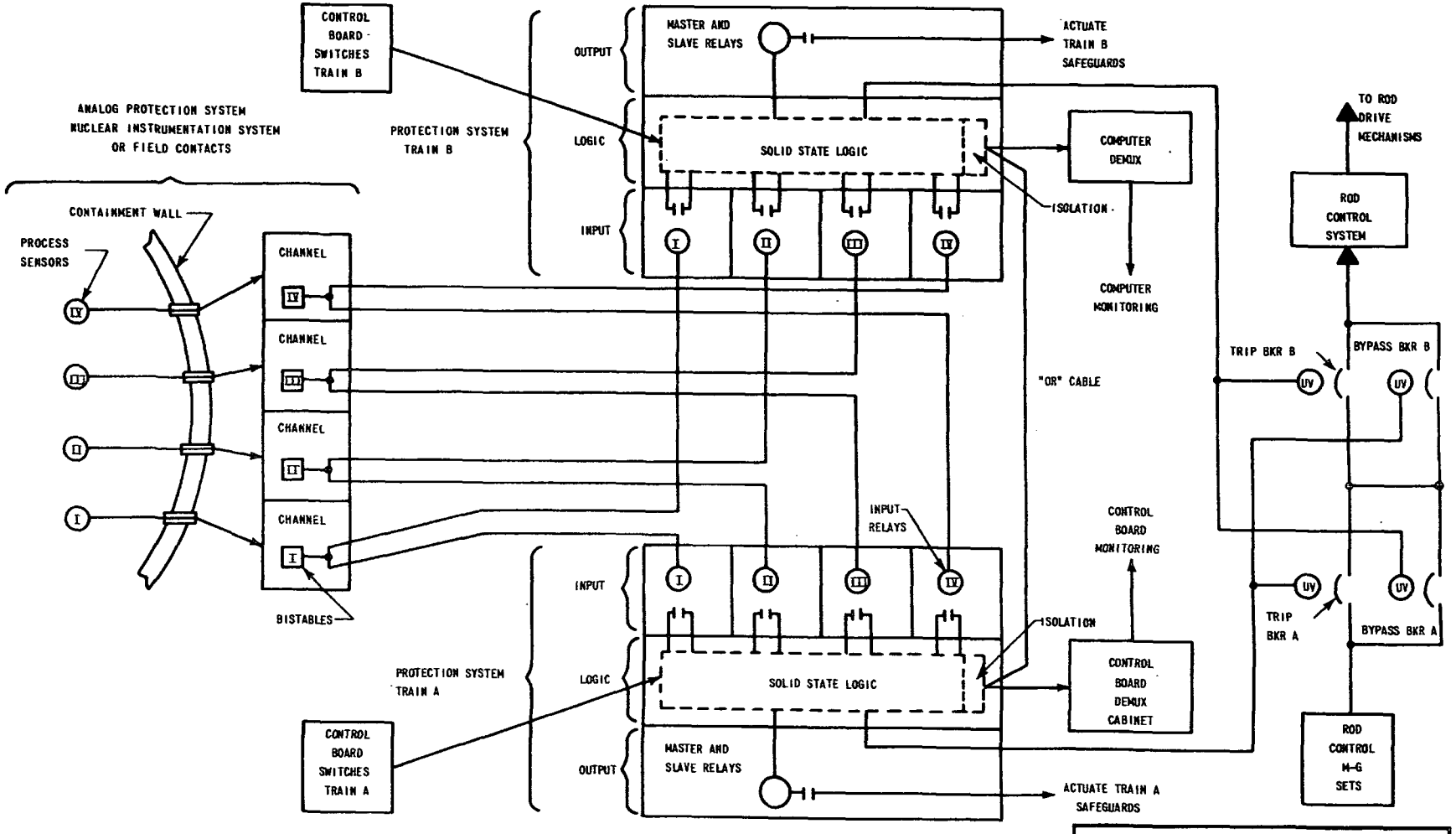
TABLE 7.7-1

PLANT CONTROL SYSTEM INTERLOCKS

| DESIGNATION | DERIVATION | FUNCTION |
|---|---|---|
| C-1 | 1/2 Neutron flux (intermediate range) above setpoint | Blocks automatic and manual control rod withdrawal |
| C-2 | 1/4 Neutron flux (power range) above setpoint | Blocks automatic and manual control rod withdrawal |
| C-3 | 2/4 Overtemperature $\Delta T$ above setpoint | Blocks automatic and manual control rod withdrawal<br><br>Actuates turbine runback via load reference<br><br>Defeats remote load dispatching (if remote load dispatching is used) |
| C-4 | 2/4 Overpower $\Delta T$ above setpoint | Blocks automatic and manual control rod withdrawal<br><br>Actuates turbine runback via load reference<br><br>Defeats remote load dispatching (if remote load dispatching is used) |
| C-5 | 1/1 Turbine impulse chamber pressure below setpoint | Defeats remote load dispatching (if remote load dispatching is used)<br><br>Blocks automatic control rod withdrawal |
| C-7 | 1/1 Time derivative (absolute value) of turbine impulse chamber pressure (decrease only) above setpoint | Makes steam dump valves available for either tripping or modulation |

TABLE 7.7-1 (Cont'd)

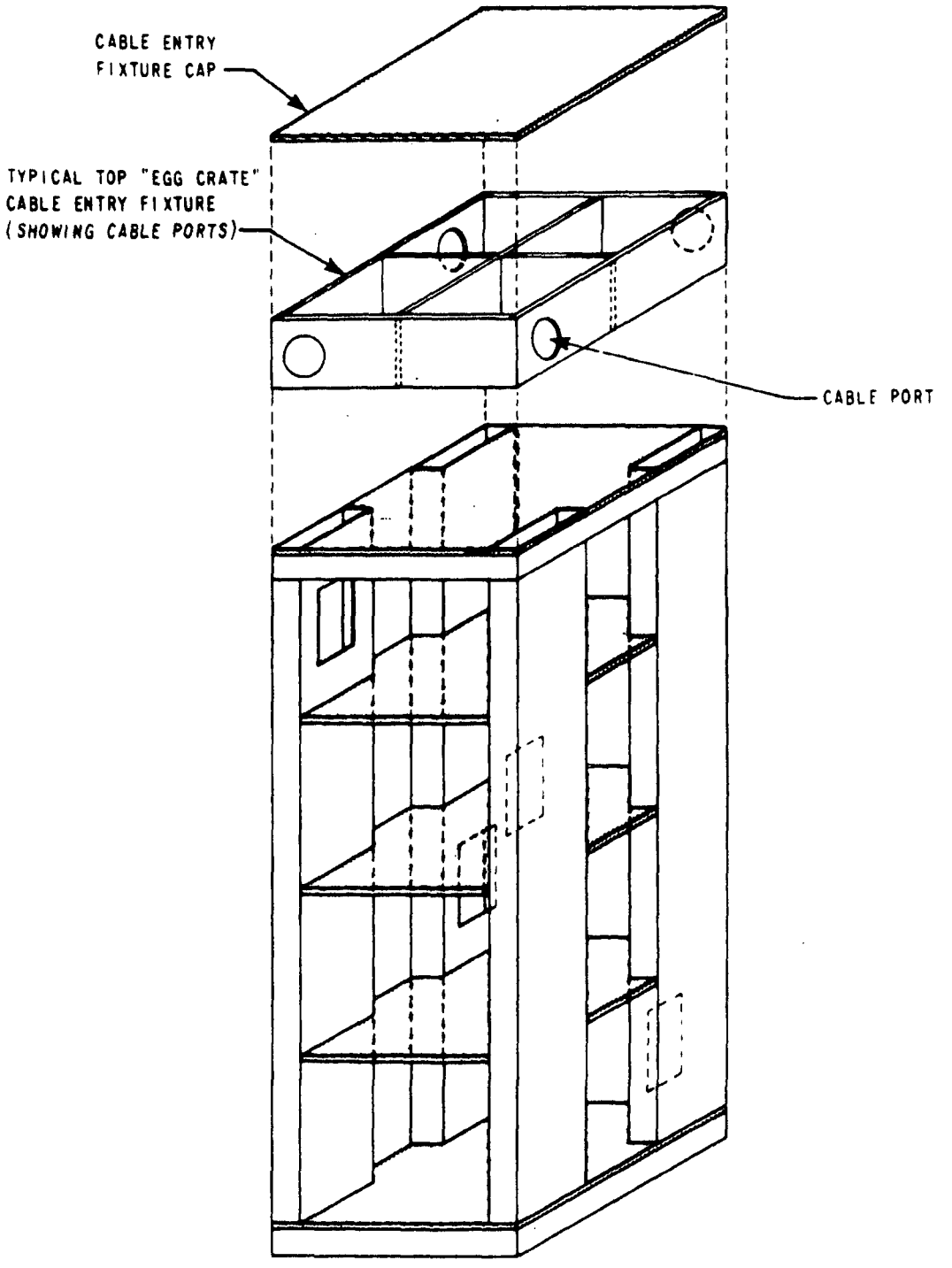
| DESIGNATION | DERIVATION | FUNCTION |
|---|---|---|
| C-8 | Turbine trip | Provides turbine trip indication |
| C-9 | Any condenser pressure above setpoint<br>or<br>All circulation water pump breakers open | Blocks steam dump to condenser |
| C-11 | 1/1 Bank D control rod position above setpoint | Blocks automatic rod withdrawal |
| C-14 | 2/2 Steam generator level above setpoint (optional) | Closes the feedwater control valve(s) in the affected steam generator only |
| C-16 | 1/1 Auctioneered low $T_{avg}$ - $T_{ref}$ below setpoint<br>or<br>1/1 Auctioneered low $T_{avg}$ below setpoint | Stops turbine loading (not used)<br><br>Defeats remote load dispatching (is remote load dispatching is used) |




**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

FIGURE 7.1-1

SINGLE LINE DIAGRAM OF
REACTOR TRIP SYSTEM

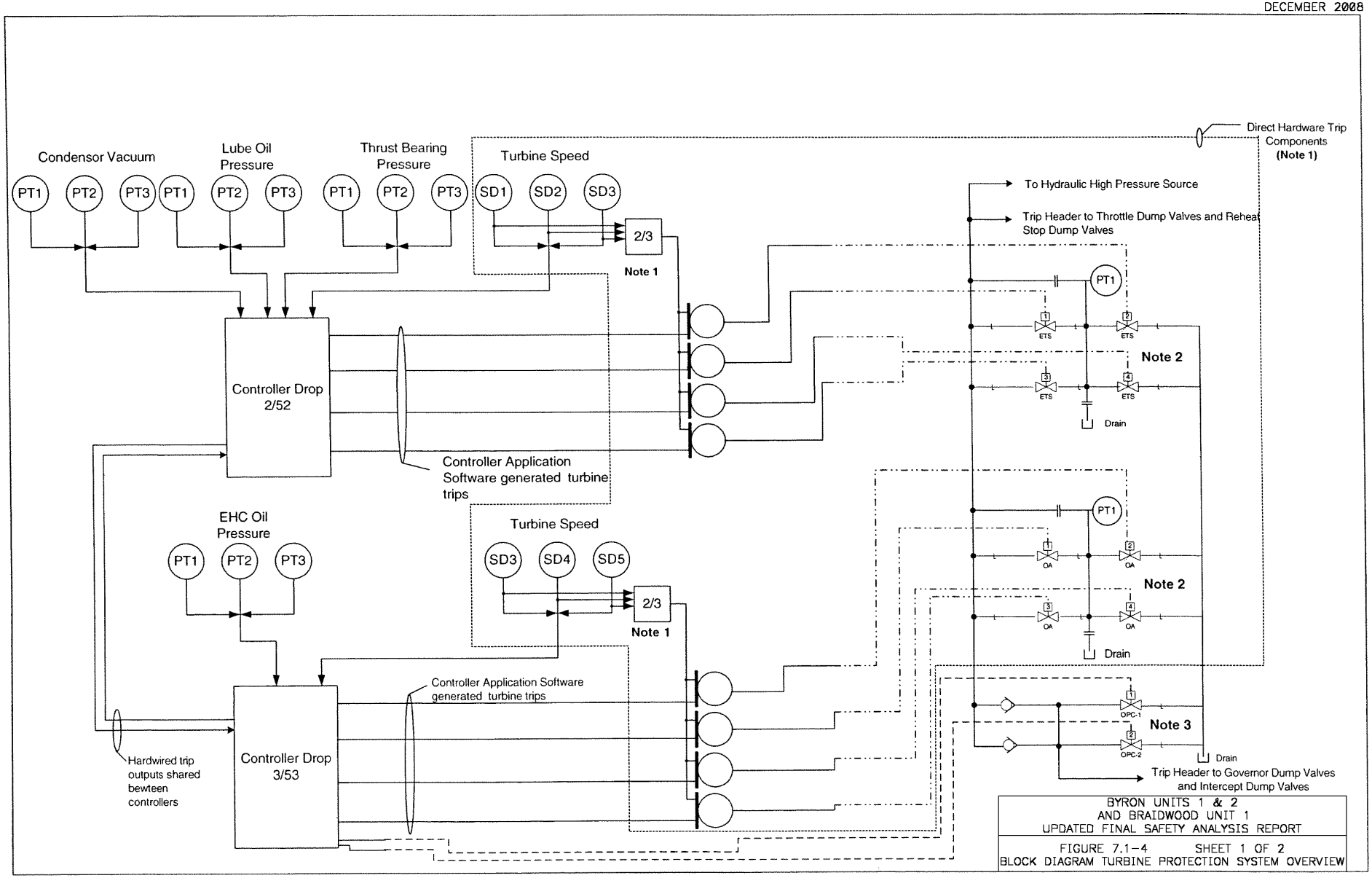



**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

FIGURE 7.1-2

REACTOR TRIP SYSTEM
INPUT RELAY BAY

Figure 7.1-3 has been deleted intentionally.




BYRON UNITS 1 & 2
AND BRAIDWOOD UNIT 1
UPDATED FINAL SAFETY ANALYSIS REPORT

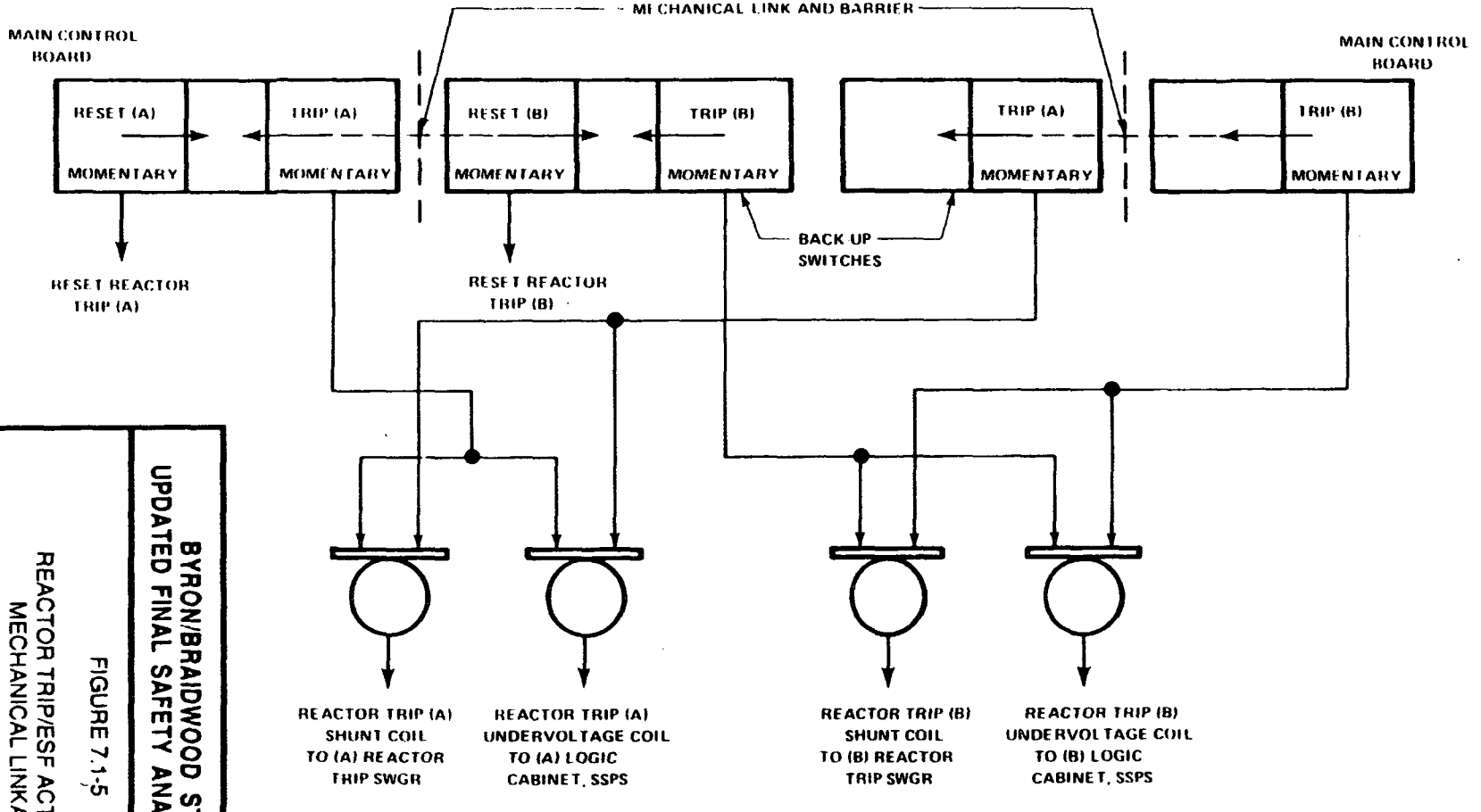
FIGURE 7.1-4 SHEET 1 OF 2
BLOCK DIAGRAM TURBINE PROTECTION SYSTEM OVERVIEW

Notes:

1) The Direct Hardware Trip Components provide a redundant and independent means from controller of tripping the turbine on overspeed and manual trip. The overspeed protection is provided by three Ovation Speed Detector (RSS) modules wired with relay logic in a 2 out of 3 configuration.

2) The hydraulic trip/test manifold is configured with four trip solenoids that can be tested on line to verify operability. The solenoid valves open on de-energization (trip condition) and are normally energized to close. Turbine trips occur if all solenoids or 1 & 2, 1 & 4, 2 & 3, and 3 & 4 de-energize. The Pressure transmitter (PT1) on the manifold provides pressure feedback during on line testing. Each of the Ovation digital outputs that drive these solenoids are on separate I/O cards and on separate branches.

3) The Overspeed Protection Control (OPC) solenoids when energized (open) are first line of defense set @ 103% which close off steam flow to Governor (HP Turbine) and Intercept valves (LP Turbines) to prevent overspeed conditions without tripping turbine. The digital outputs are redundant and are configured in a wired "and".

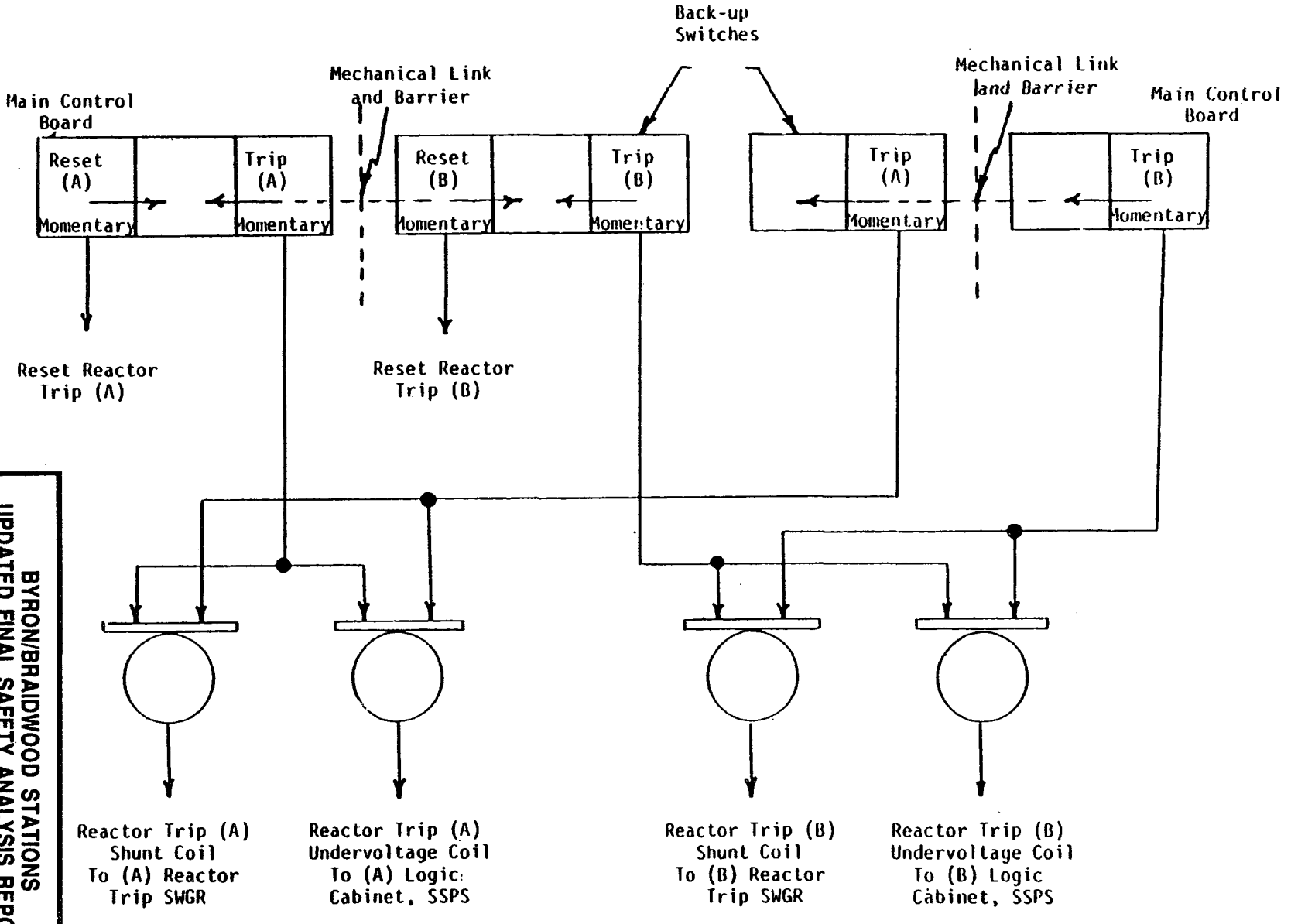



BYRON/BRAIDWOOD STATIONS
UPDATED FINAL SAFETY ANALYSIS REPORT

FIGURE 7.1-5

REACTOR TRIP/ESF ACTUATION
MECHANICAL LINKAGE

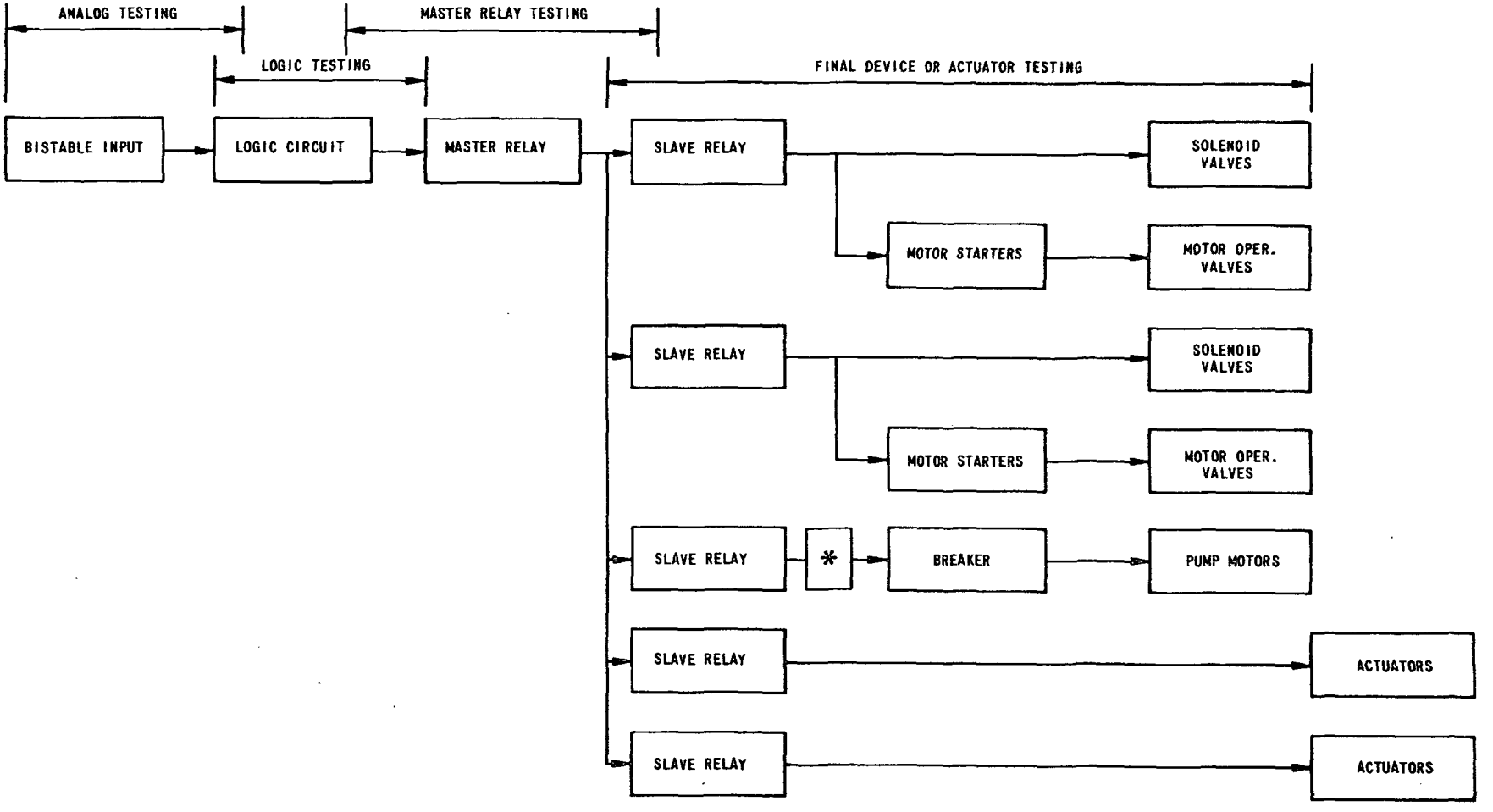
Figure 7.2-1 has been deleted intentionally.




BYRON/BRAIDWOOD STATIONS
UPDATED FINAL SAFETY ANALYSIS REPORT

FIGURE 7.2-2

REACTOR TRIP/ESF ACTUATION
MECHANICAL LINKAGE

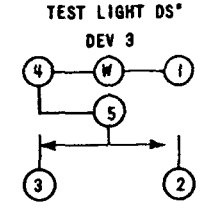



*ESF SEQUENCING RELAY

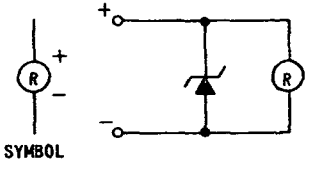
**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

FIGURE 7.3-1

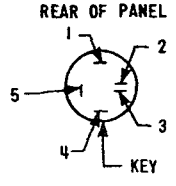
TYPICAL ESF TEST CIRCUITS




ILLUMINATED PUSHBUTTON SWITCH
WITH 28V LAMP NO. 327
(EXCEPT AS NOTED)




DETAIL C CURRENT MONITOR DS* LED WITH INTERNAL RESISTOR



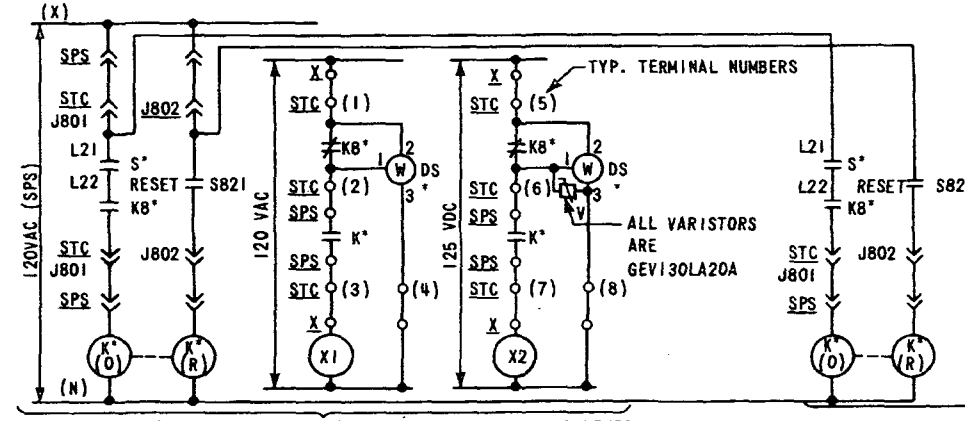

CONTACT LOCATION SCHEME

GENERAL NOTES:

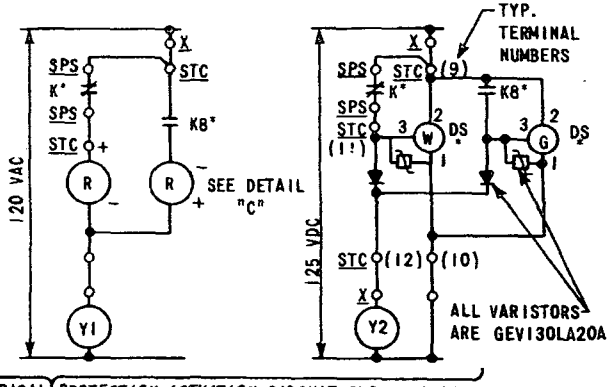
1. CIRCUITRY AND HARDWARE FOR REDUNDANT PROTECTION TRAINS "A" AND "B" TEST CABINETS ARE DUPLICATE EXCEPT AS NOTED
   A - TRAIN "A" ONLY
   B - TRAIN "B" ONLY
2. IN DETAILS A & B THE SYMBOL * REPRESENTS THE SUFFIX NUMBERS OF THE DEVICE REFERENCED.
   EXAMPLE:
   K* - SPS RELAY, K601, K602, ETC.
   K(O) - OPERATING COIL
   K(R) - RESET COIL
   S* - STC TEST SWITCH, S802, S834 ETC.
   K8* - STC RELAY, K811, K817, ETC.
   DS* - STC LIGHT, DS8009, DS8077, ETC.
3. "DETAIL A" & "B" TYPE CIRCUITS ARE DETAILED ON THE SCHEMATICS. "DETAIL B" CIRCUITS WILL BE SUBSTITUTED FOR "DETAIL A" CIRCUITS WHERE REQUIRED.

LOCATION LEGEND

SPS - SOLID STATE PROTECTION SYSTEM
STC - SAFEGUARDS TEST CABINET
X - SWGR, MCC, AUXILIARY RELAY RACK, ETC.
ASC - AUXILIARY SAFEGUARDS CABINET




DETAIL A TYPICAL PROTECTION ACTUATION CIRCUIT BLOCKING SCHEMES
(CONTACT CLOSURE FOR ACTUATION)



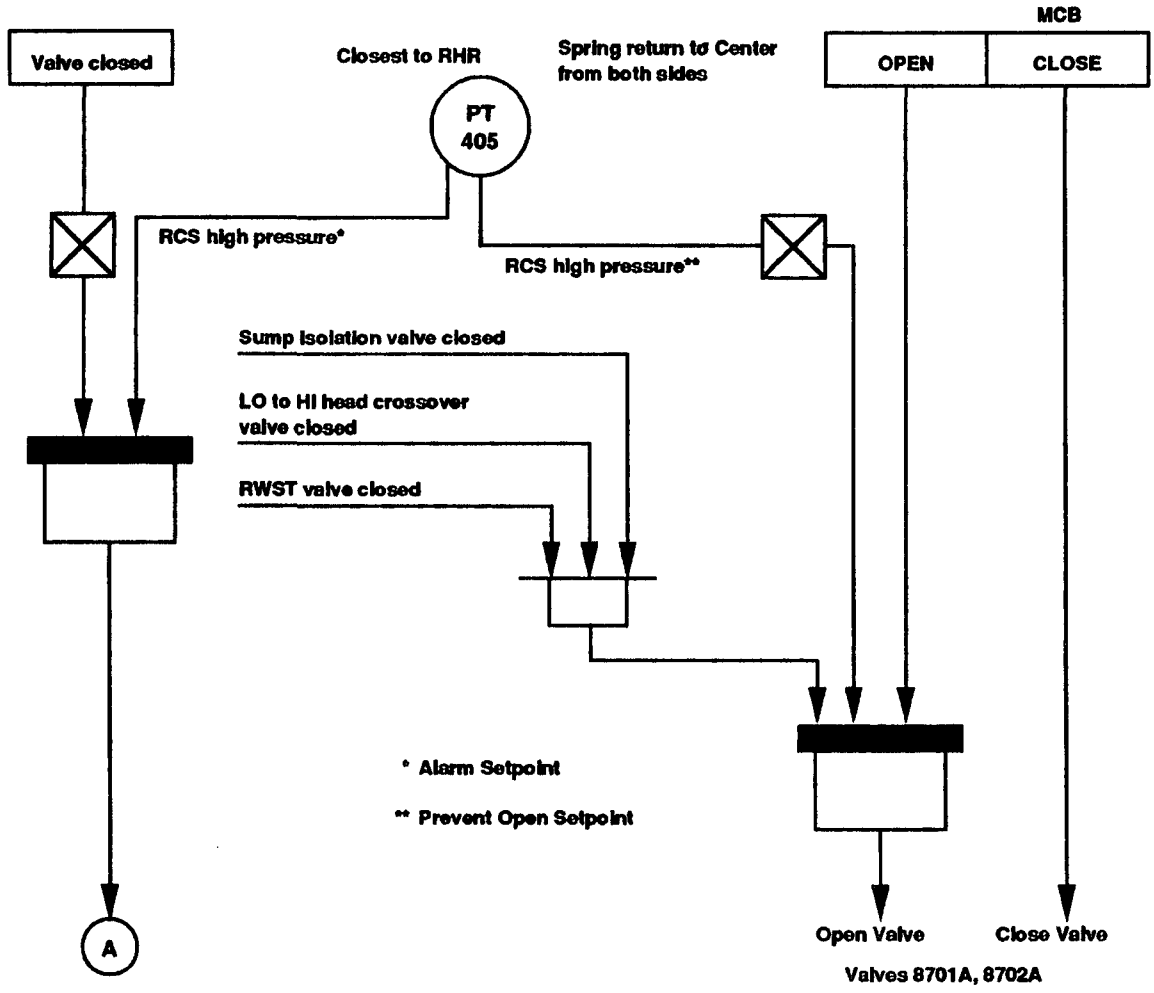

DETAIL B TYPICAL PROTECTION ACTUATION CIRCUIT BLOCKING SCHEMES
(CONTACT OPENING FOR ACTUATION)

**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

FIGURE 7.3-2

ENGINEERED SAFEGUARDS TEST CABINET—INDEX, NOTES, AND LEGEND

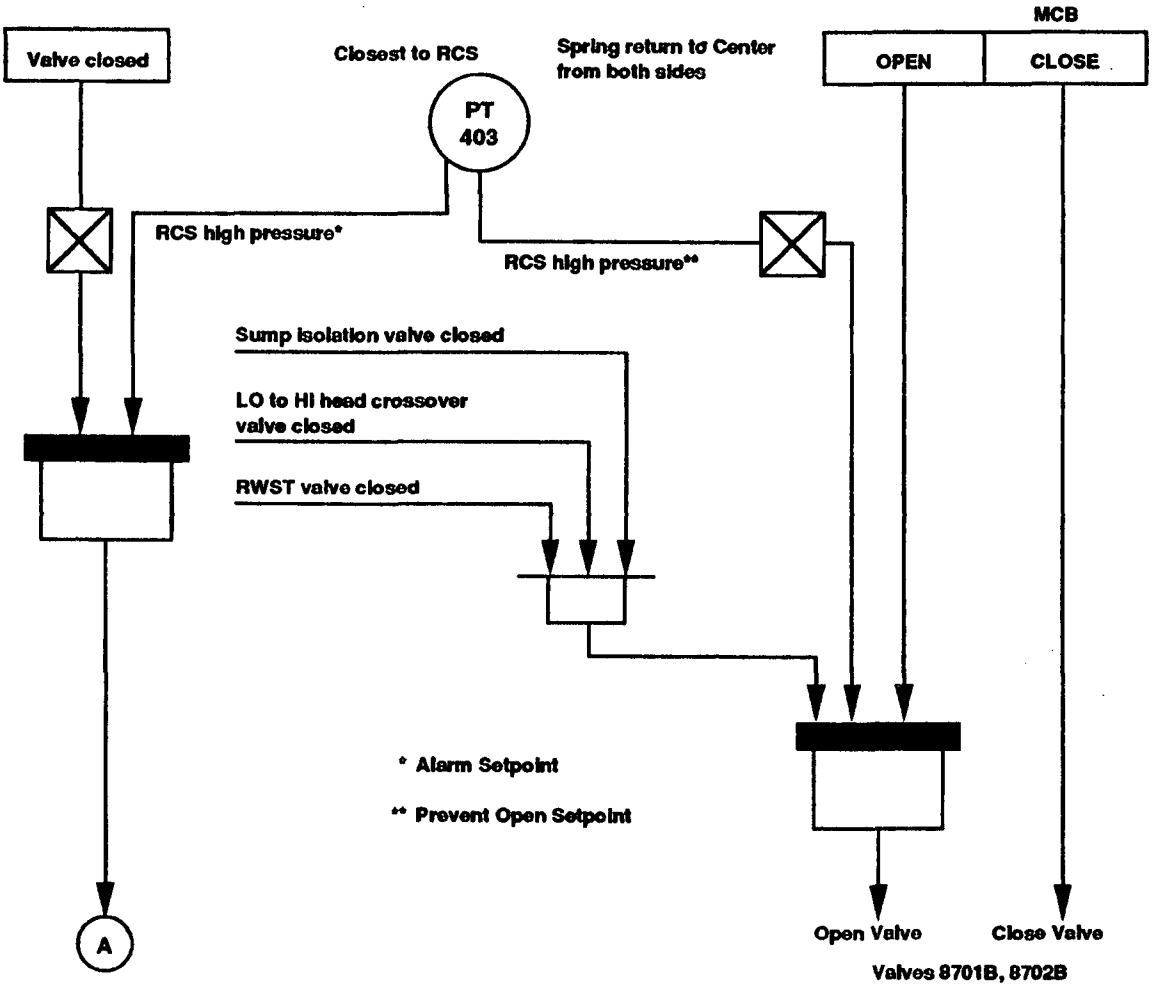
Figures 7.3-3 through 7.3-5 have been deleted intentionally.




**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

FIGURE 7.6-1

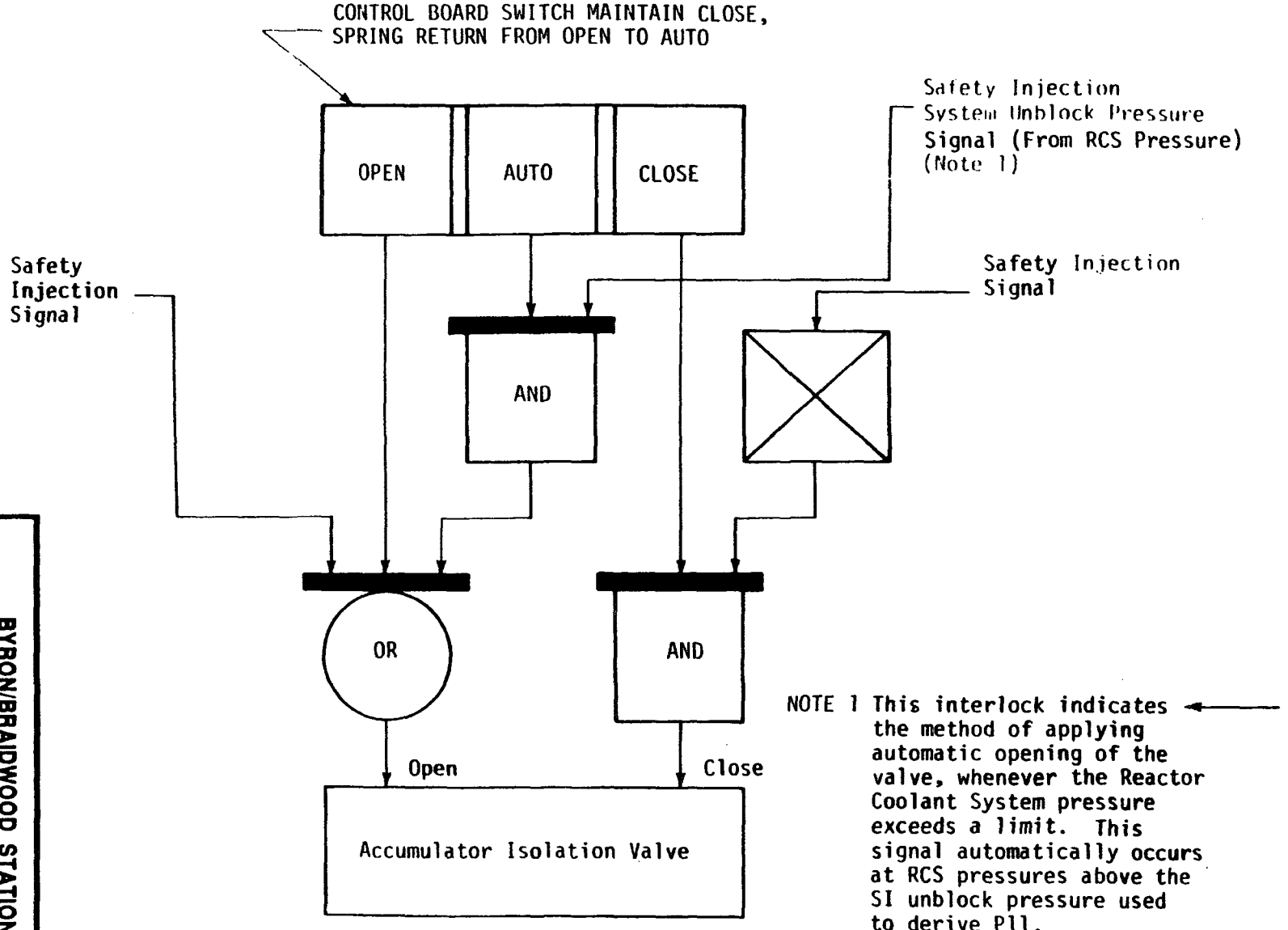
LOGIC DIAGRAM FOR OUTER
RHR ISOLATION VALVE




**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

FIGURE 7.6-2

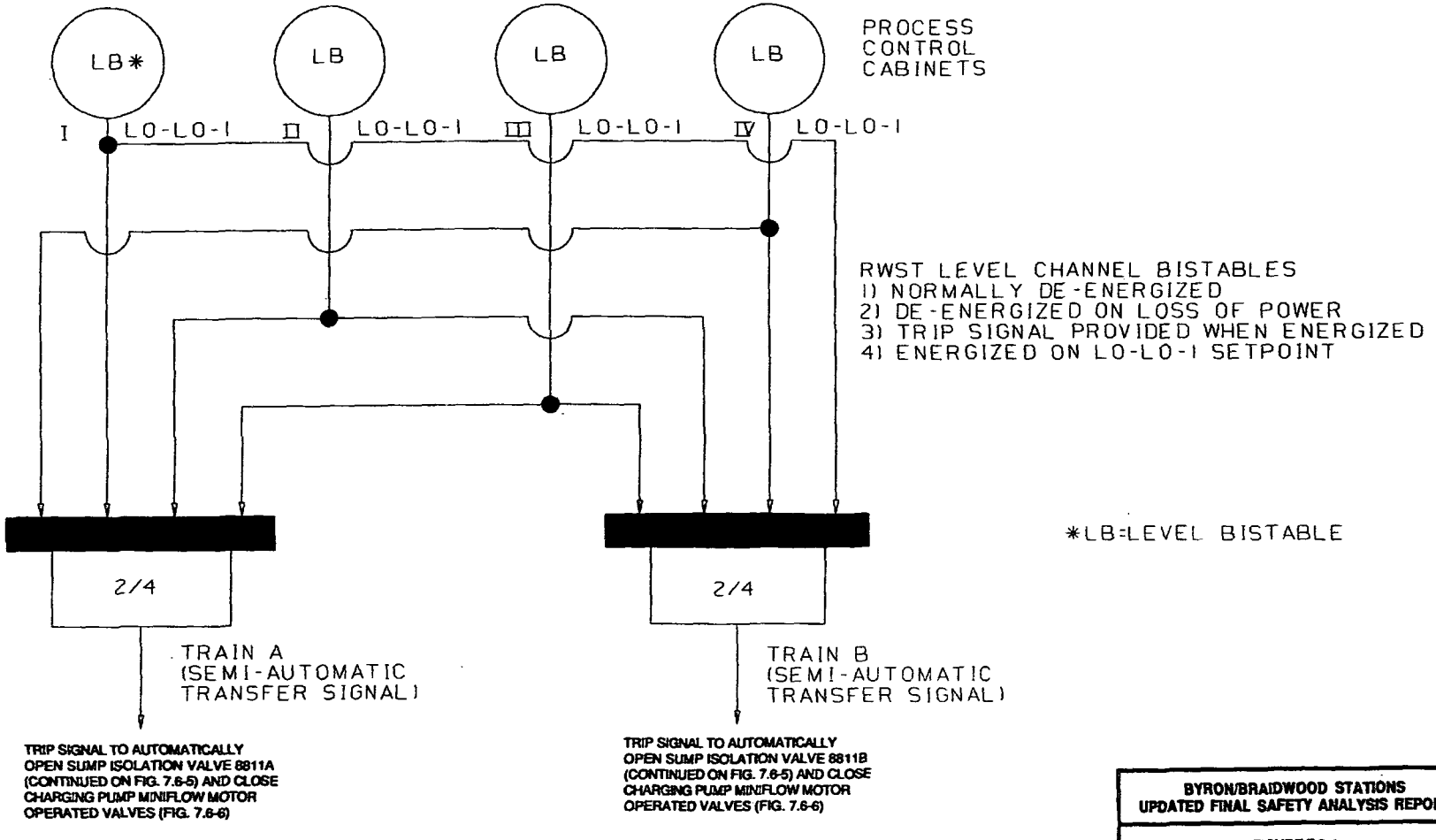
LOGIC DIAGRAM FOR INNER
RHR ISOLATION VALVE




BYRON/BRAIDWOOD STATIONS
UPDATED FINAL SAFETY ANALYSIS REPORT

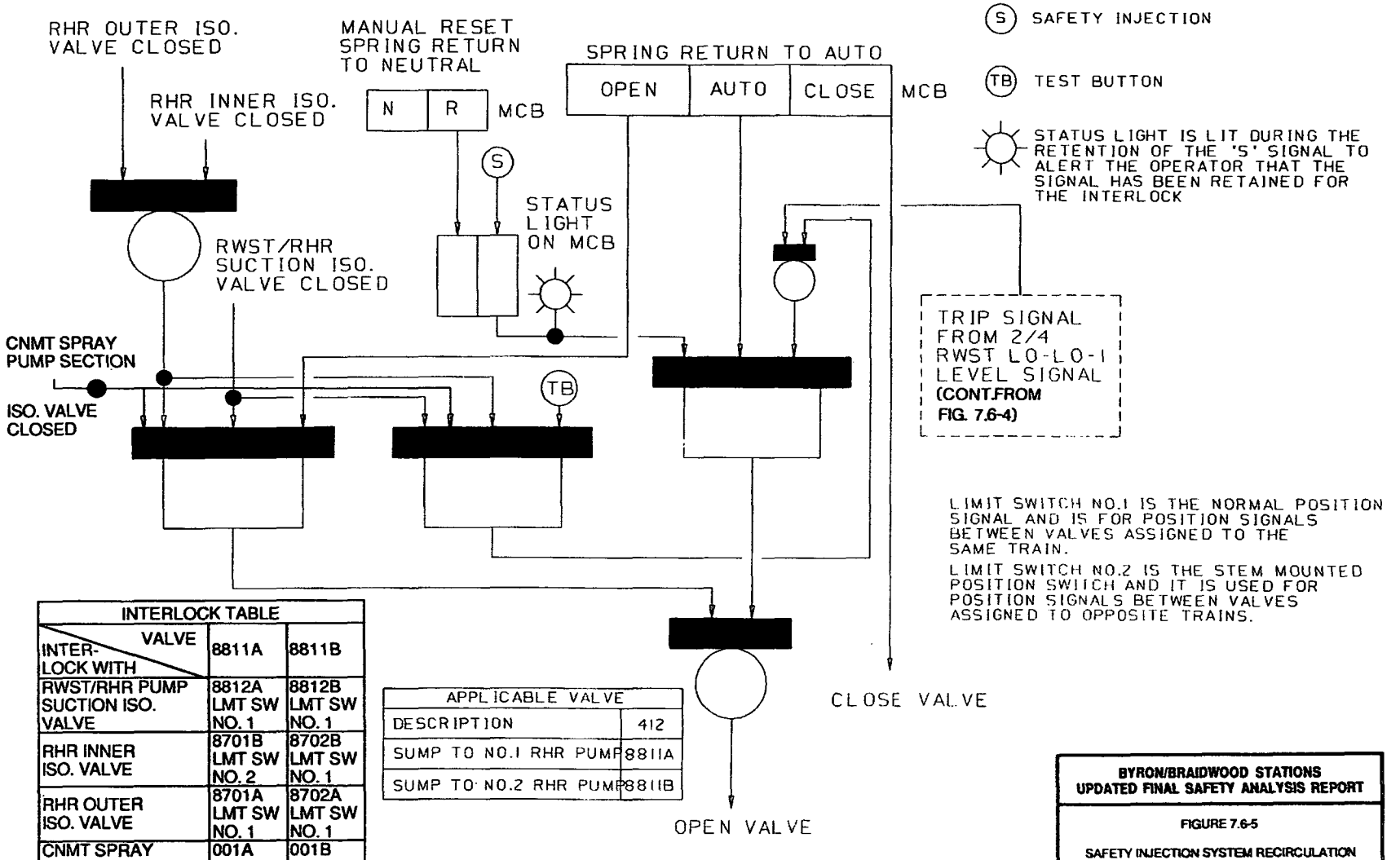
FIGURE 7.6-3

FUNCTIONAL BLOCK DIAGRAM OF
ACCUMULATOR ISOLATION VALVE




**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

FIGURE 7.6-4
TRANSFER SIGNAL FOR SI SYSTEM RECIRCULATION SUMP ISOLATION VALVES AND CHARGING PUMP MINIFLOW MOTOR OPERATED VALVE



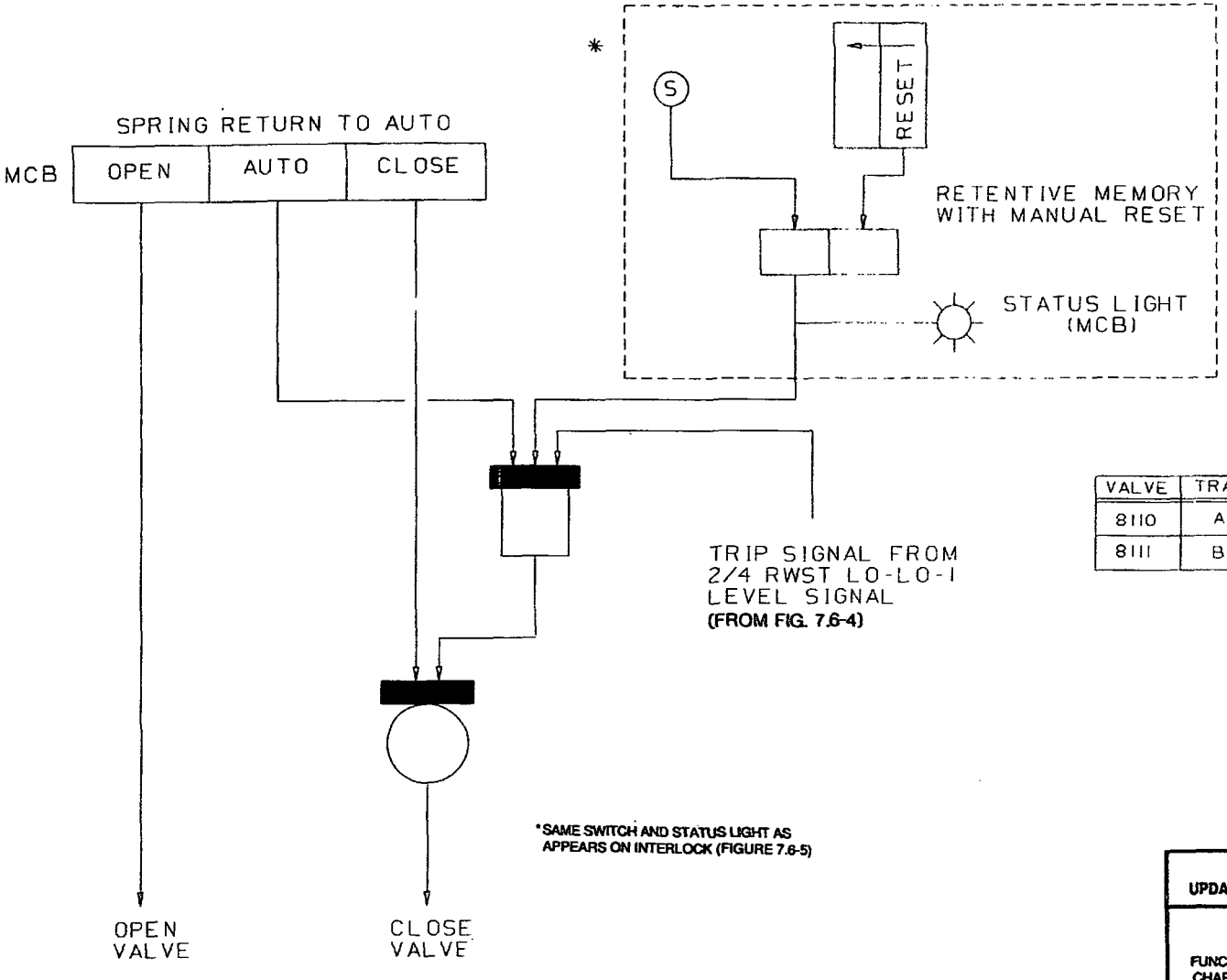

| INTERLOCK TABLE | | |
|---|---|---|
| VALVE / INTER-LOCK WITH | 8811A | 8811B |
| RWST/RHR PUMP SUCTION ISO. VALVE | 8812A LMT SW NO. 1 | 8812B LMT SW NO. 1 |
| RHR INNER ISO. VALVE | 8701B LMT SW NO. 2 | 8702B LMT SW NO. 1 |
| RHR OUTER ISO. VALVE | 8701A LMT SW NO. 1 | 8702A LMT SW NO. 1 |
| CNMT SPRAY PUMP ISO. VALVE CLOSED | 001A LMT SW NO. 1 | 001B LMT SW NO. 1 |
| TRAIN | A | B |

| APPLICABLE VALVE | |
|---|---|
| DESCRIPTION | 412 |
| SUMP TO NO.1 RHR PUMP | 8811A |
| SUMP TO NO.2 RHR PUMP | 8811B |

**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

**FIGURE 7.6-5**

**SAFETY INJECTION SYSTEM RECIRCULATION SUMP ISOLATION VALVES**



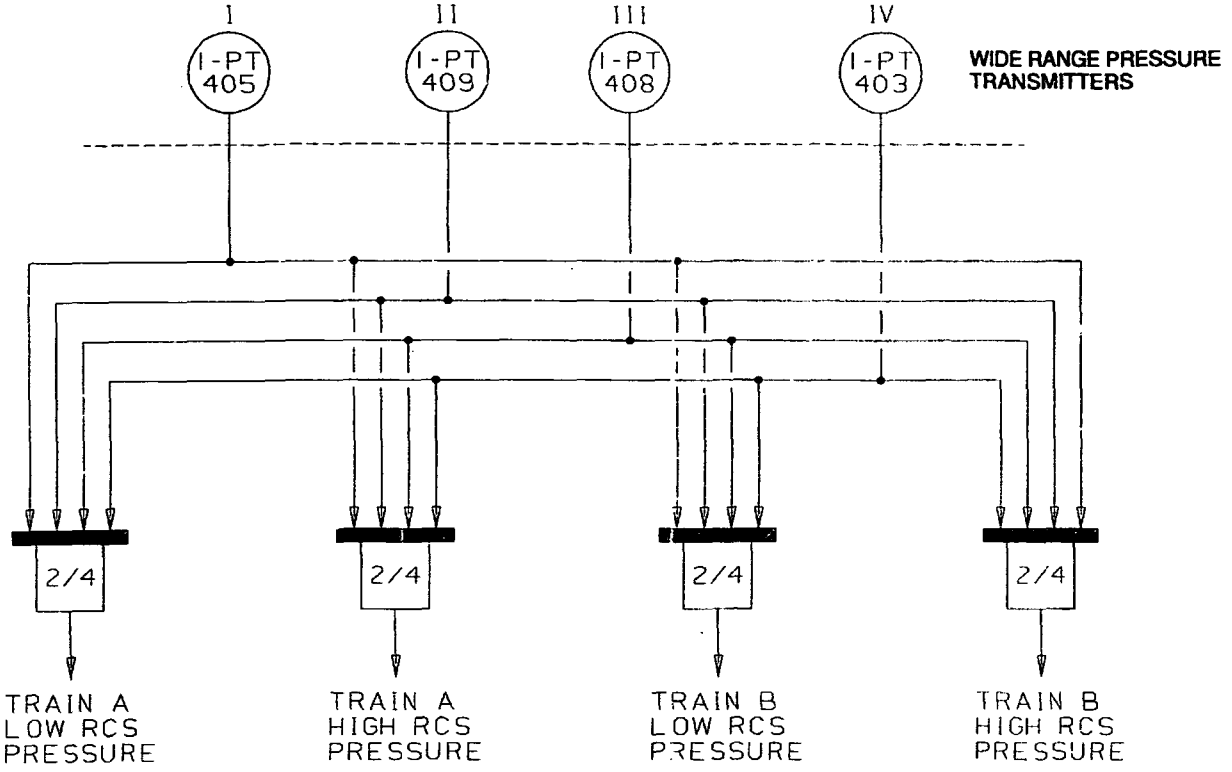

| VALVE | TRAIN |
|---|---|
| 8110 | A |
| 8111 | B |

*SAME SWITCH AND STATUS LIGHT AS APPEARS ON INTERLOCK (FIGURE 7.6-5)

**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

**FIGURE 7.6-6**

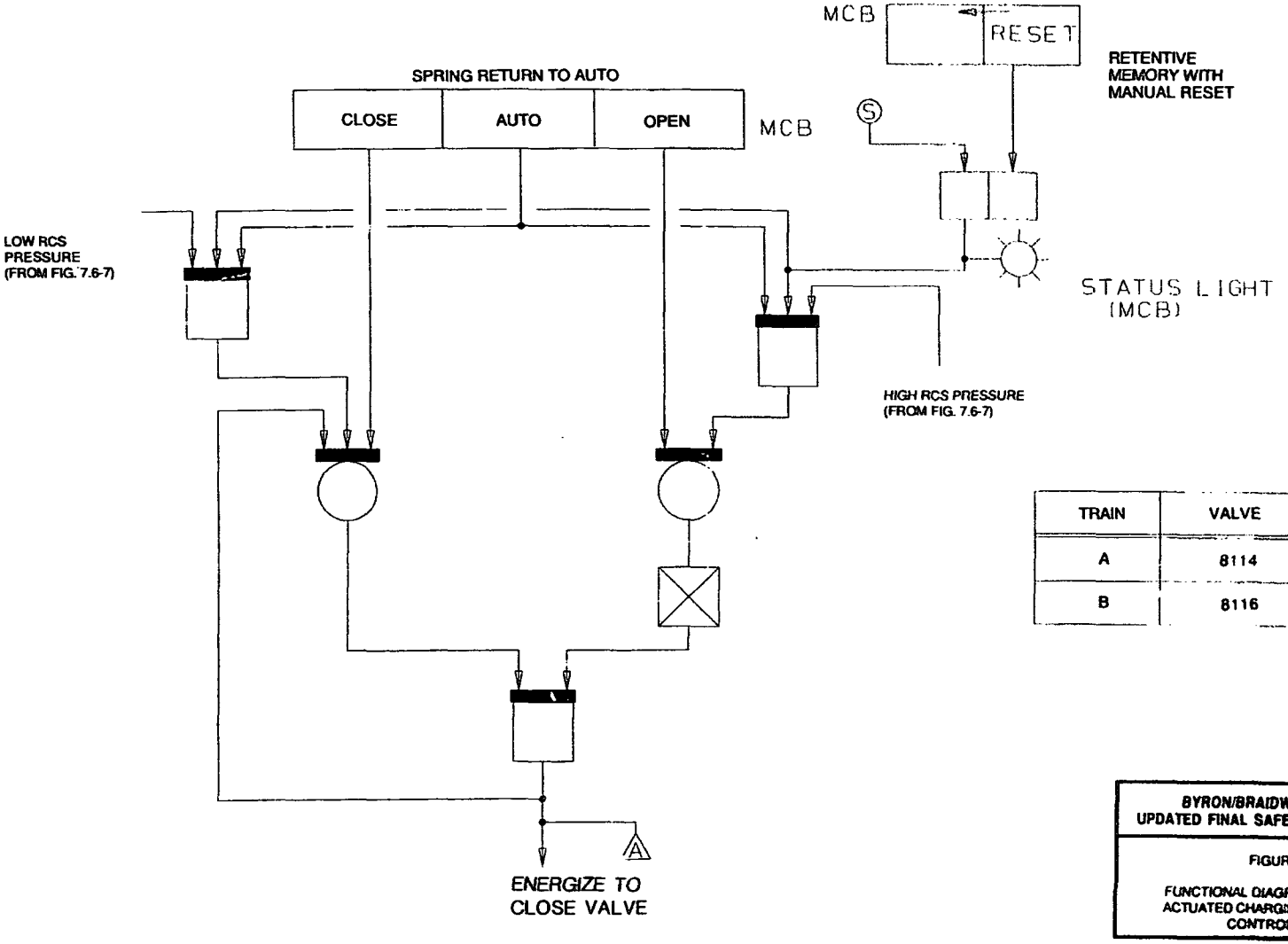
**FUNCTIONAL DIAGRAM FOR MOTOR OPERATED CHARGING PUMP MINIFLOW CONTROL VALVES**




**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

FIGURE 7.6-7

FUNCTIONAL DIAGRAM FOR WIDE RANGE PRESSURE SIGNAL FOR SOLENOID ACTUATED CHARGING PUMP MINIFLOW CONTROL VALVES

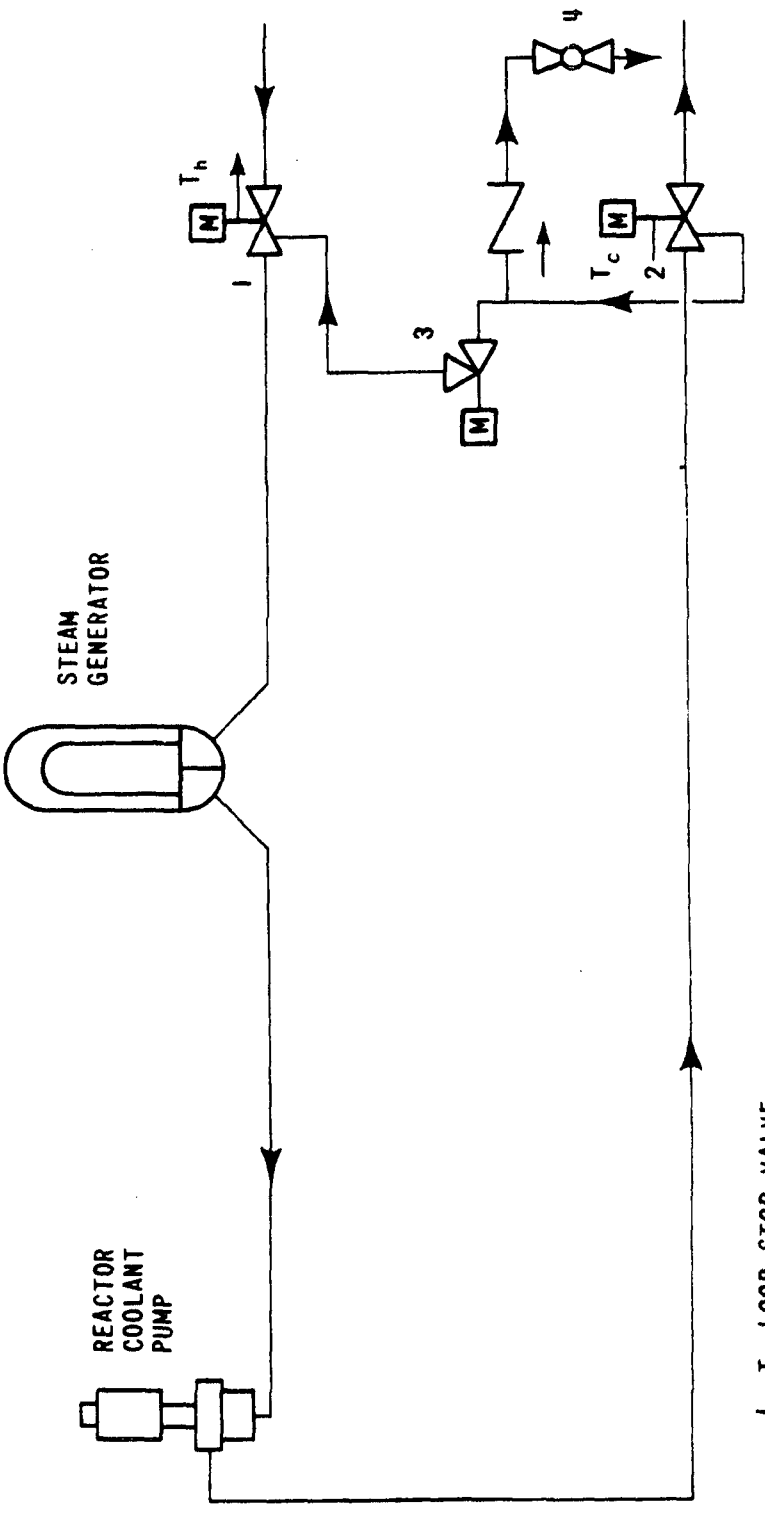



| TRAIN | VALVE |
|---|---|
| A | 8114 |
| B | 8116 |

BYRON/BRAIDWOOD STATIONS
UPDATED FINAL SAFETY ANALYSIS REPORT

FIGURE 7.6-8

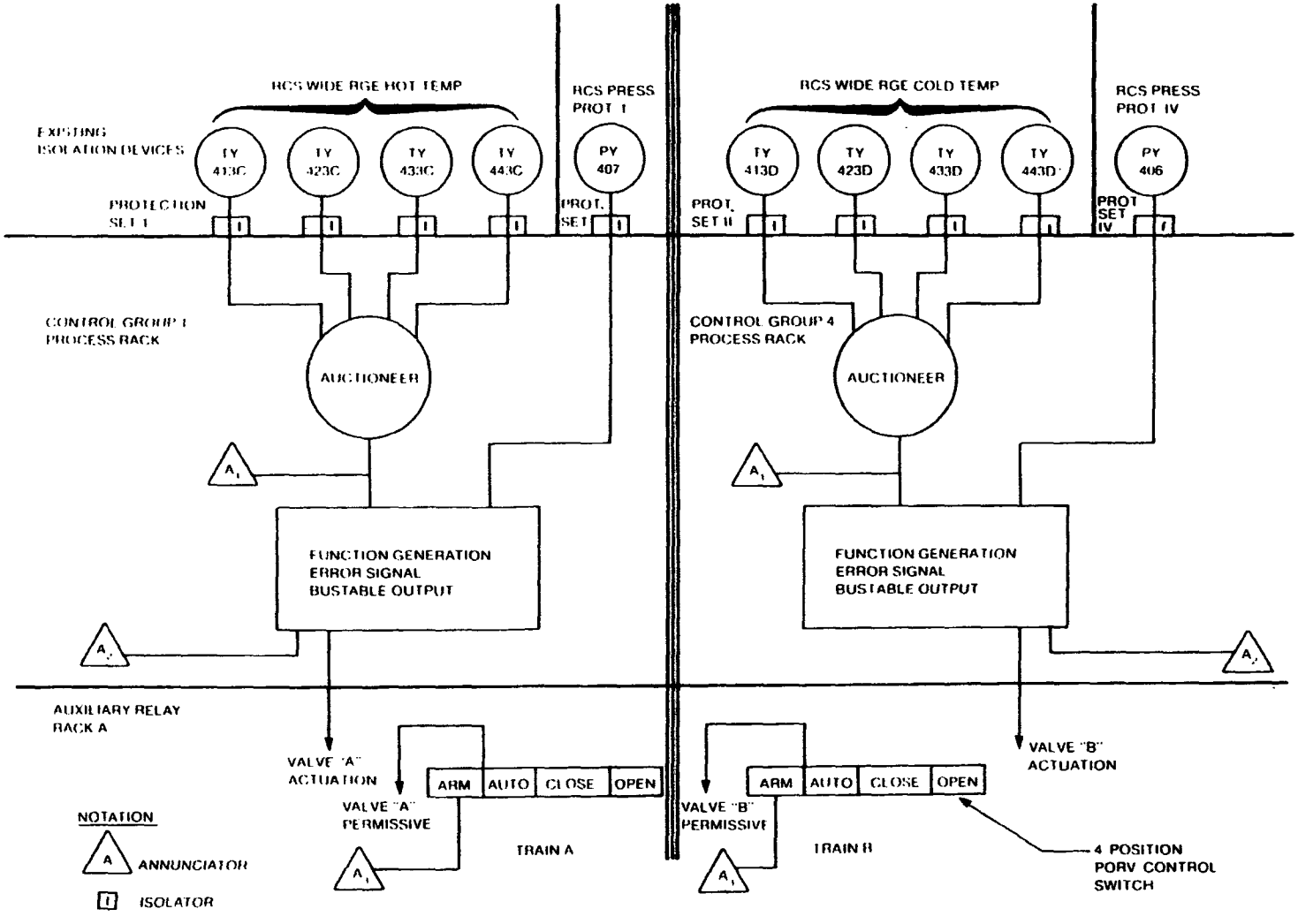
FUNCTIONAL DIAGRAM FOR SOLENOID ACTUATED CHARGING PUMP MINIFLOW CONTROL VALVES




**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

FIGURE 7.6-9

REACTOR COOLANT SYSTEM LOOP
WITH LOOP STOP VALVES

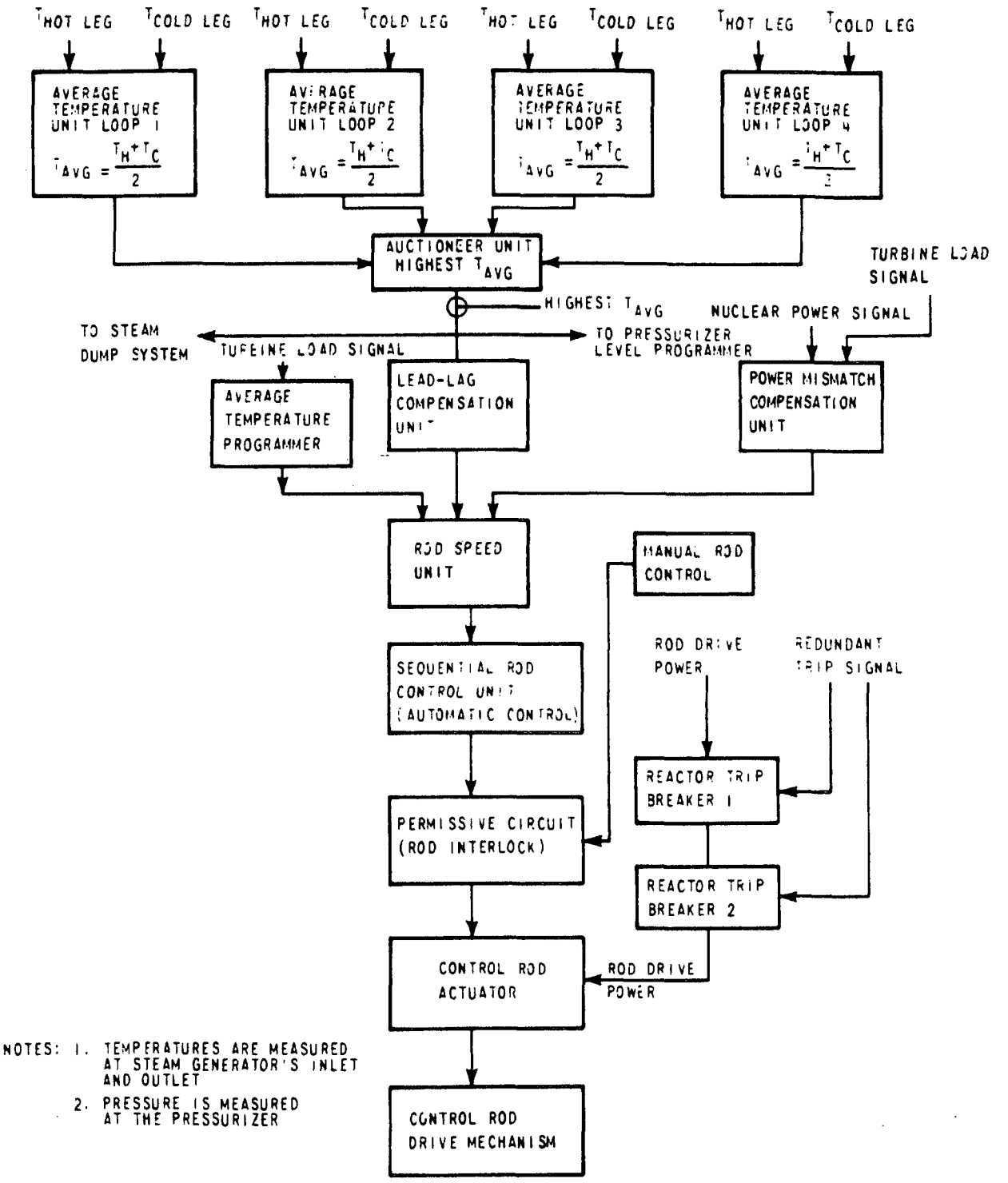



| ANNUNCIATOR | FUNCTION ARMED |
|---|---|
| $A_1$ | OPERATOR NOTIFIED TO ARM REACTOR COOLANT SYSTEM COLD OVERPRESSURE PROTECTION SYSTEM |
| $A_2$ | ACTUAL PRESSURE APPROACHES REFERENCE PRESSURE |
| $A_3$ | PORV IS ARMED WITH VALVE ACTUATION SIGNAL PRESENT |

**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

**FIGURE 7.6-10**

**DIAGRAM SHOWING GENERATING PLANT VARIABLE PROCESSING FOR LOW TEMPERATURE INTERLOCKS FOR RCS PRESSURE**



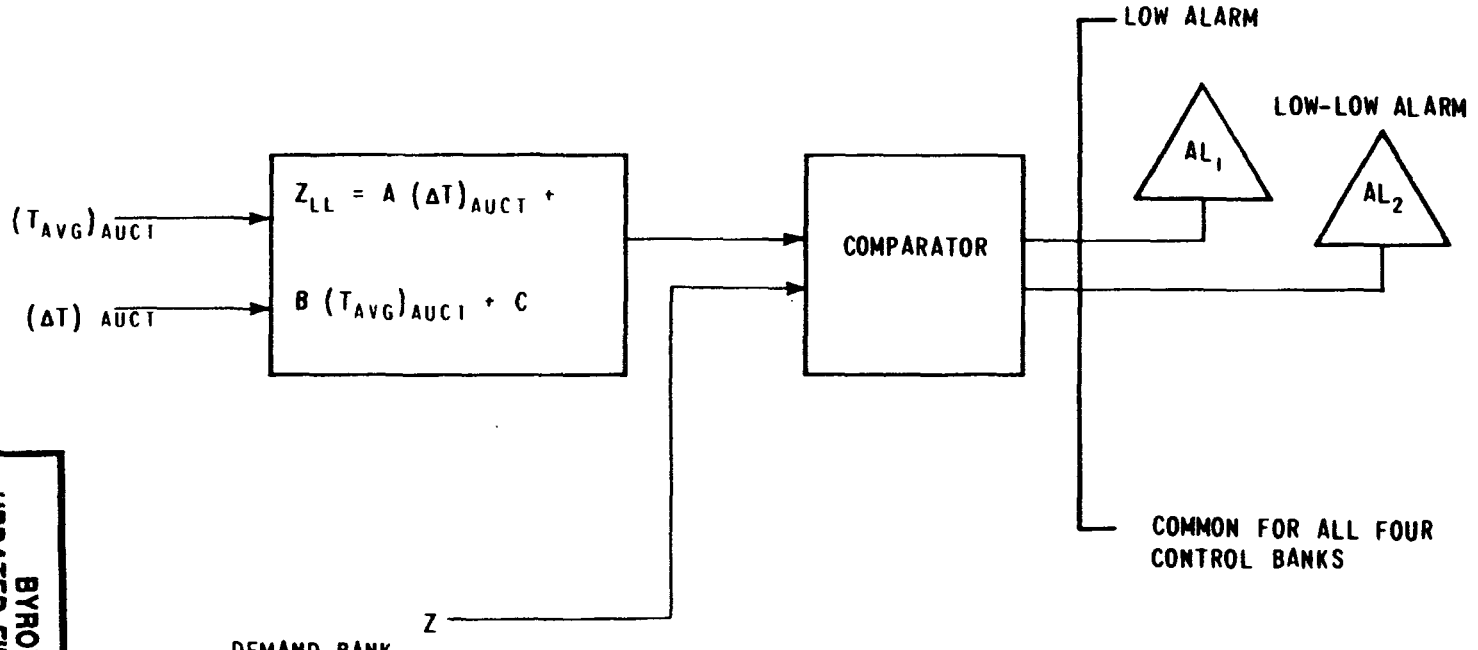

NOTES: 1. TEMPERATURES ARE MEASURED AT STEAM GENERATOR'S INLET AND OUTLET

2. PRESSURE IS MEASURED AT THE PRESSURIZER

**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

**FIGURE 7.7-1**

**SIMPLIFIED BLOCK DIAGRAM OF REACTOR CONTROL SYSTEM**



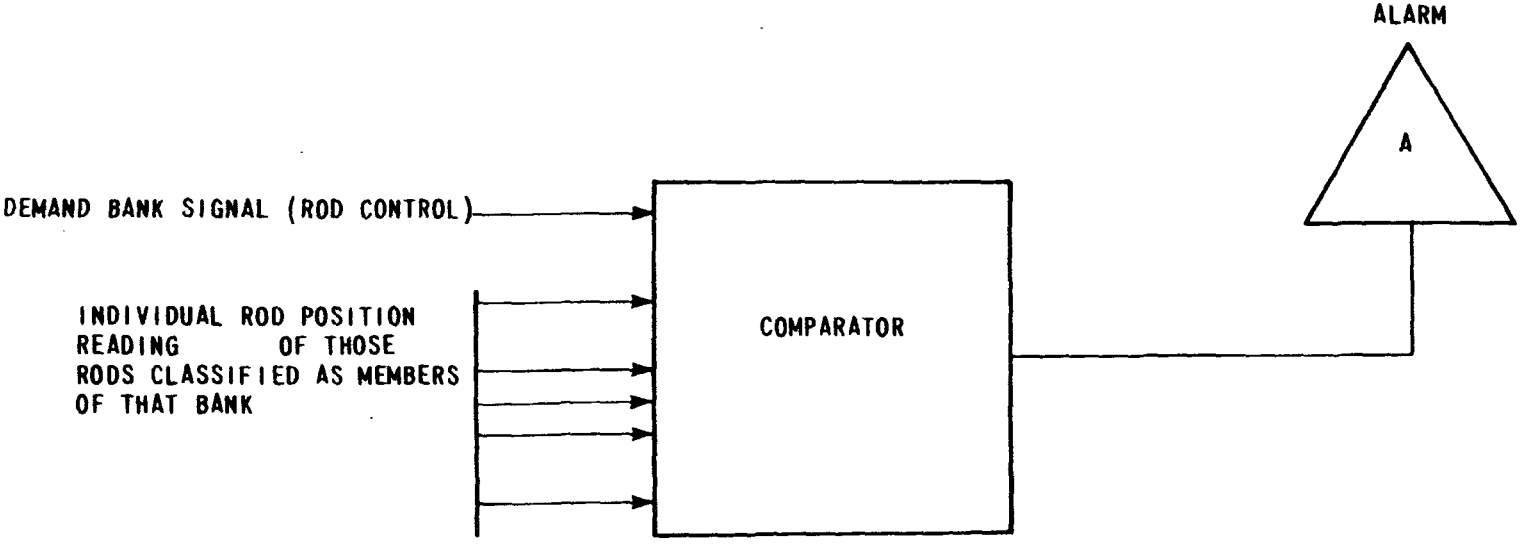

NOTE: 1. ANALOG CIRCUITRY IS USED FOR THE COMPARATOR NETWORK

2. COMPARISON IS DONE FOR ALL CONTROL BANKS

BYRON/BRAIDWOOD STATIONS
UPDATED FINAL SAFETY ANALYSIS REPORT

FIGURE 7.7-2

CONTROL BANK ROD
INSERTION MONITOR




NOTE: 1. DIGITAL OR ANALOG SIGNALS MAY BE USED FOR THE COMPARATOR INPUTS.

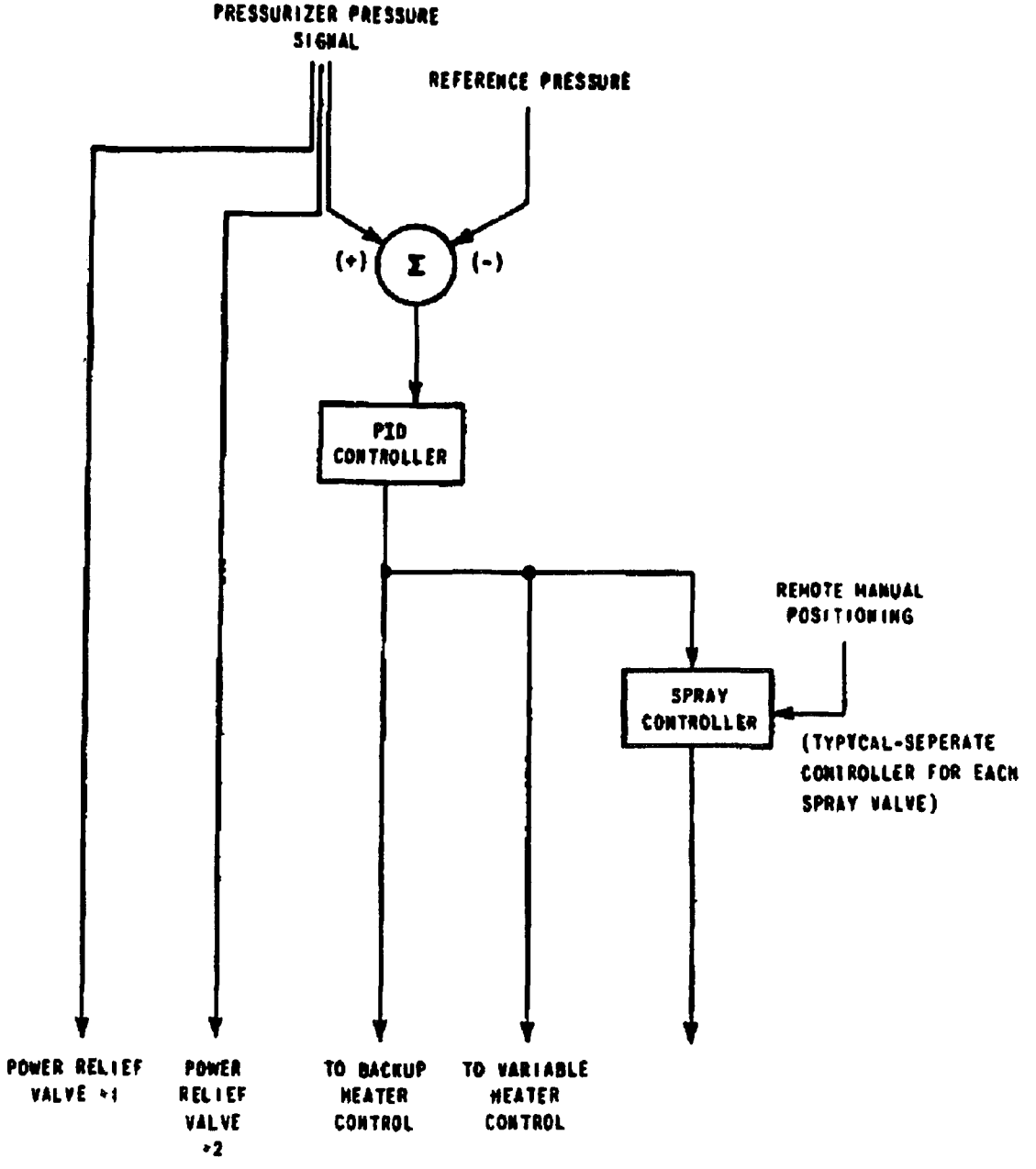
2. THE COMPARATOR WILL ENERGIZE THE ALARM IF THERE EXISTS A POSITION DIFFERENCE GREATER THAN A PRESENT LIMIT BETWEEN ANY INDIVIDUAL ROD POSITION SIGNAL DEVIATION FROM THE OTHER RODS IN THE BANK.

3. COMPARISON IS INDIVIDUALLY DONE FOR ALL CONTROL BANKS.

**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

FIGURE 7.7-3

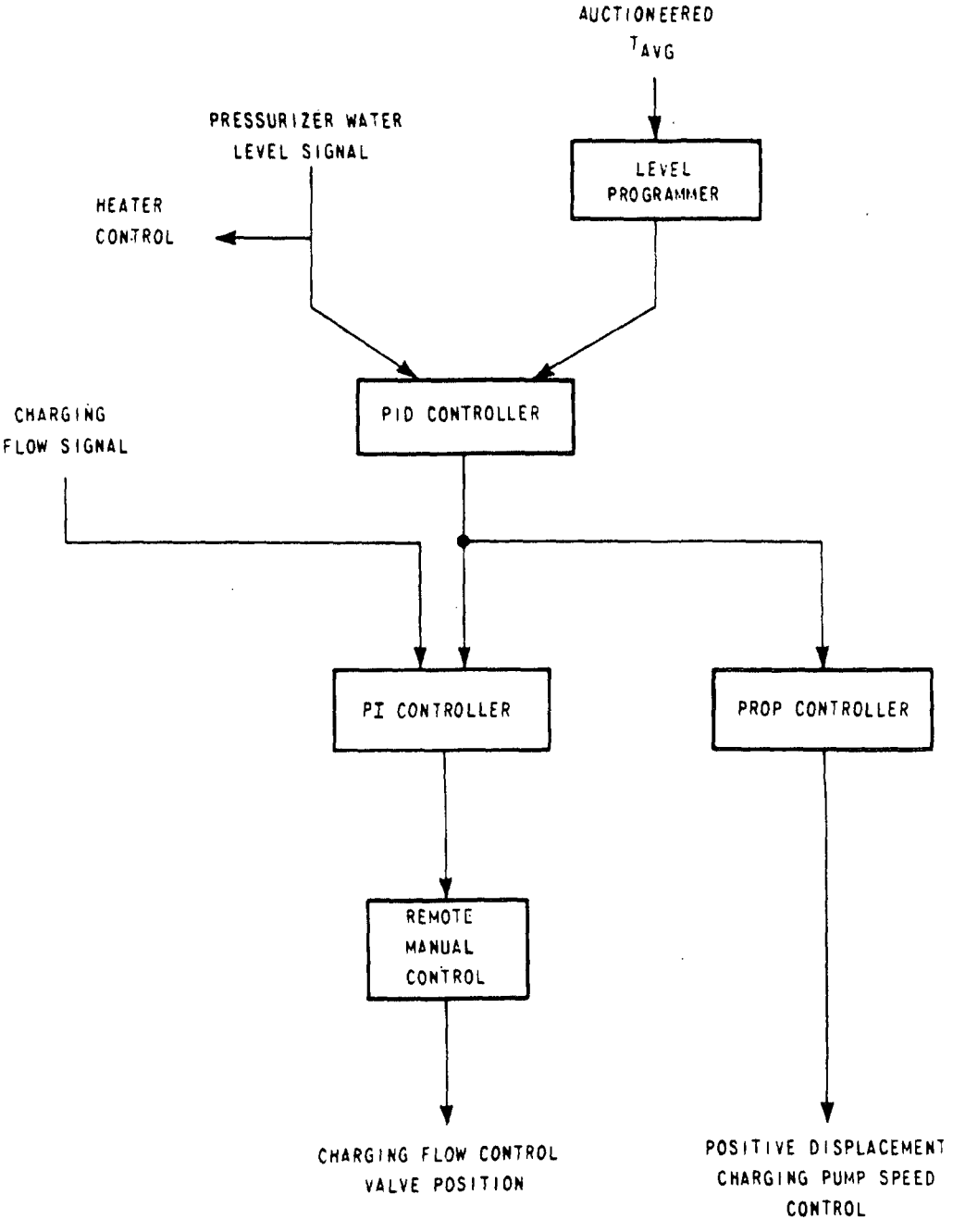
ROD DEVIATION COMPARATOR




**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

FIGURE 7.7-4

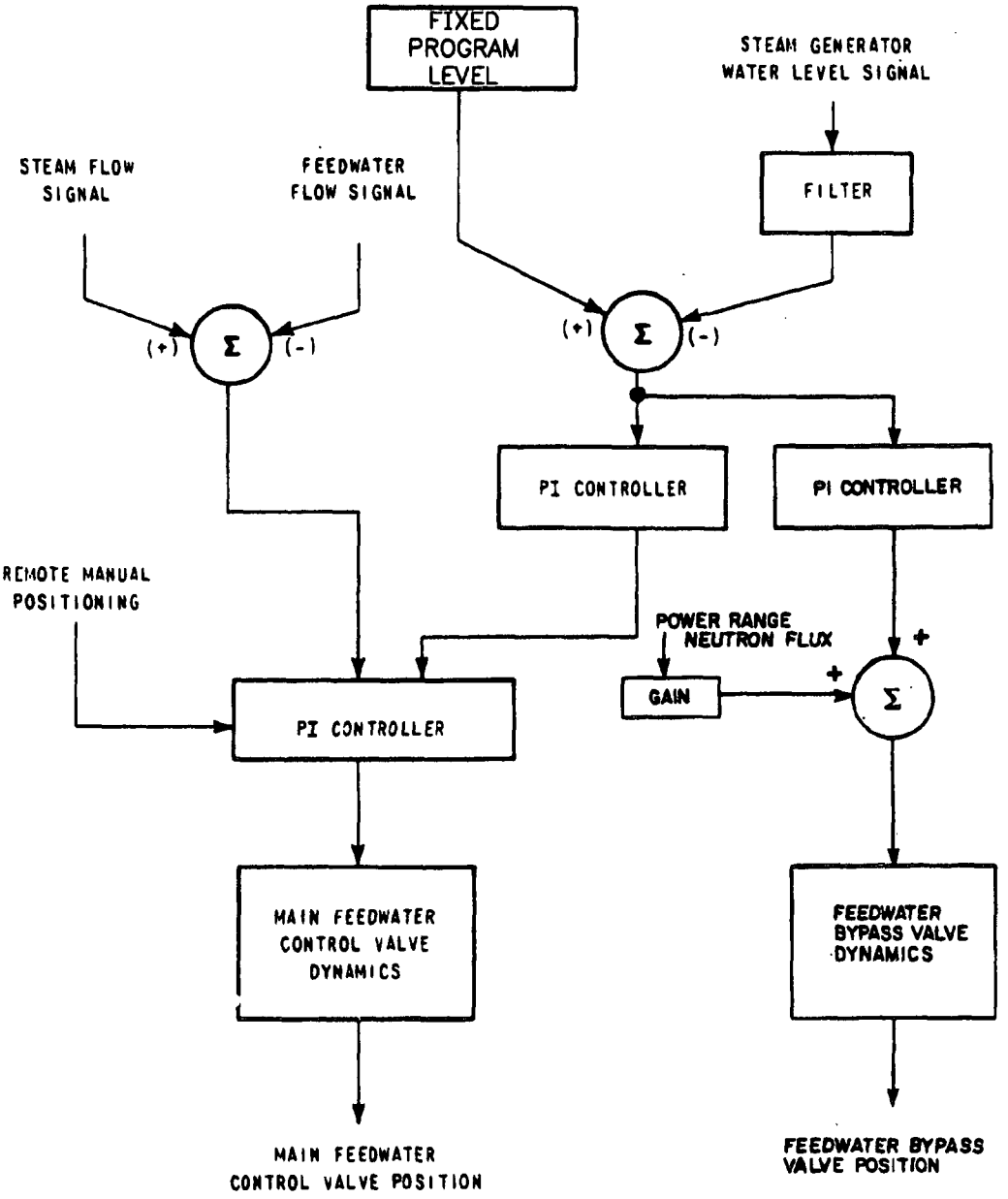
BLOCK DIAGRAM OF PRESSURIZER PRESSURE CONTROL SYSTEM




**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

FIGURE 7.7-5

BLOCK DIAGRAM OF PRESSURIZER
LEVEL CONTROL SYSTEM

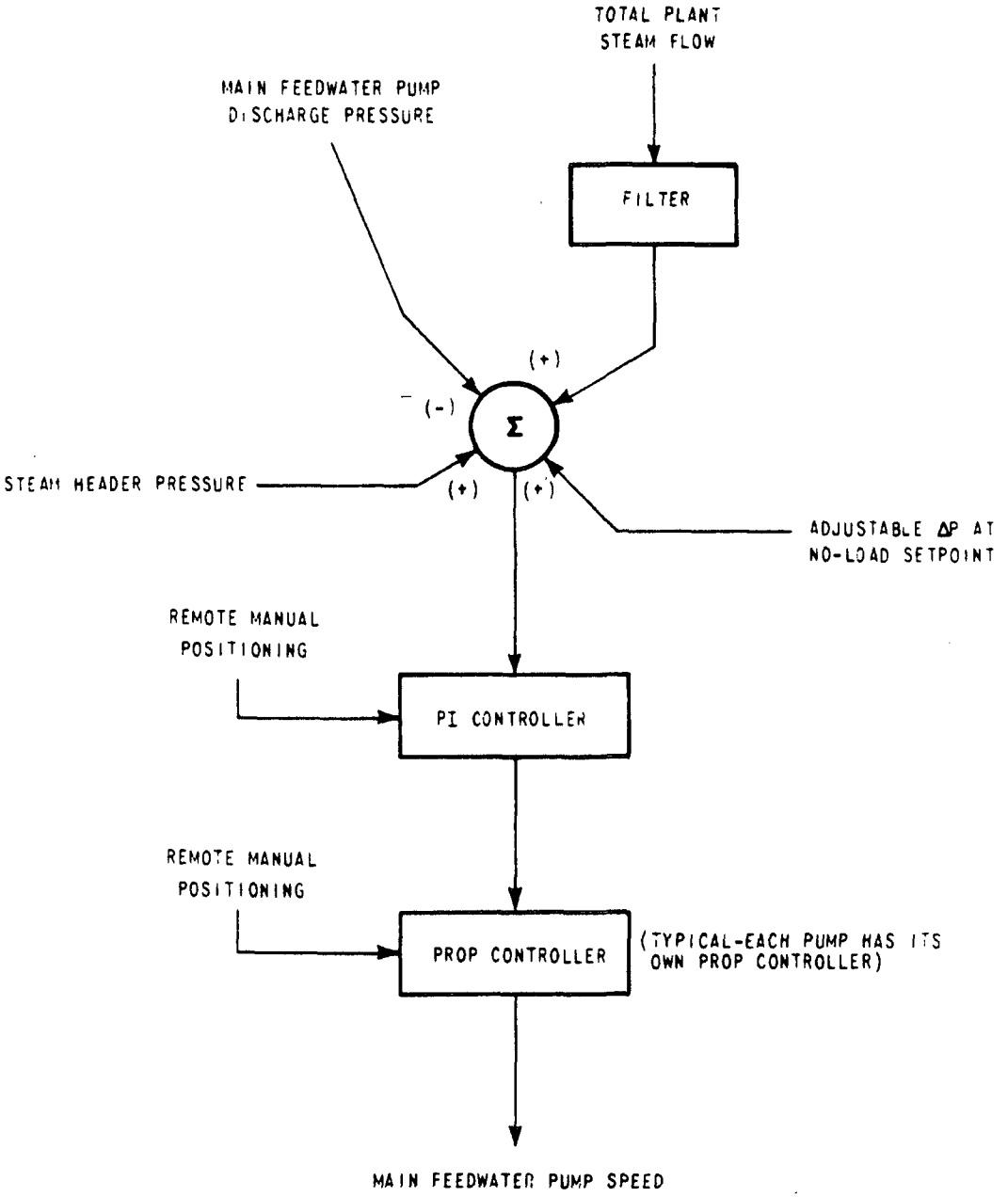



BYRON/BRAIDWOOD STATIONS

**UPDATED FINAL SAFETY ANALYSIS REPORT**

**FIGURE 7.7-6**

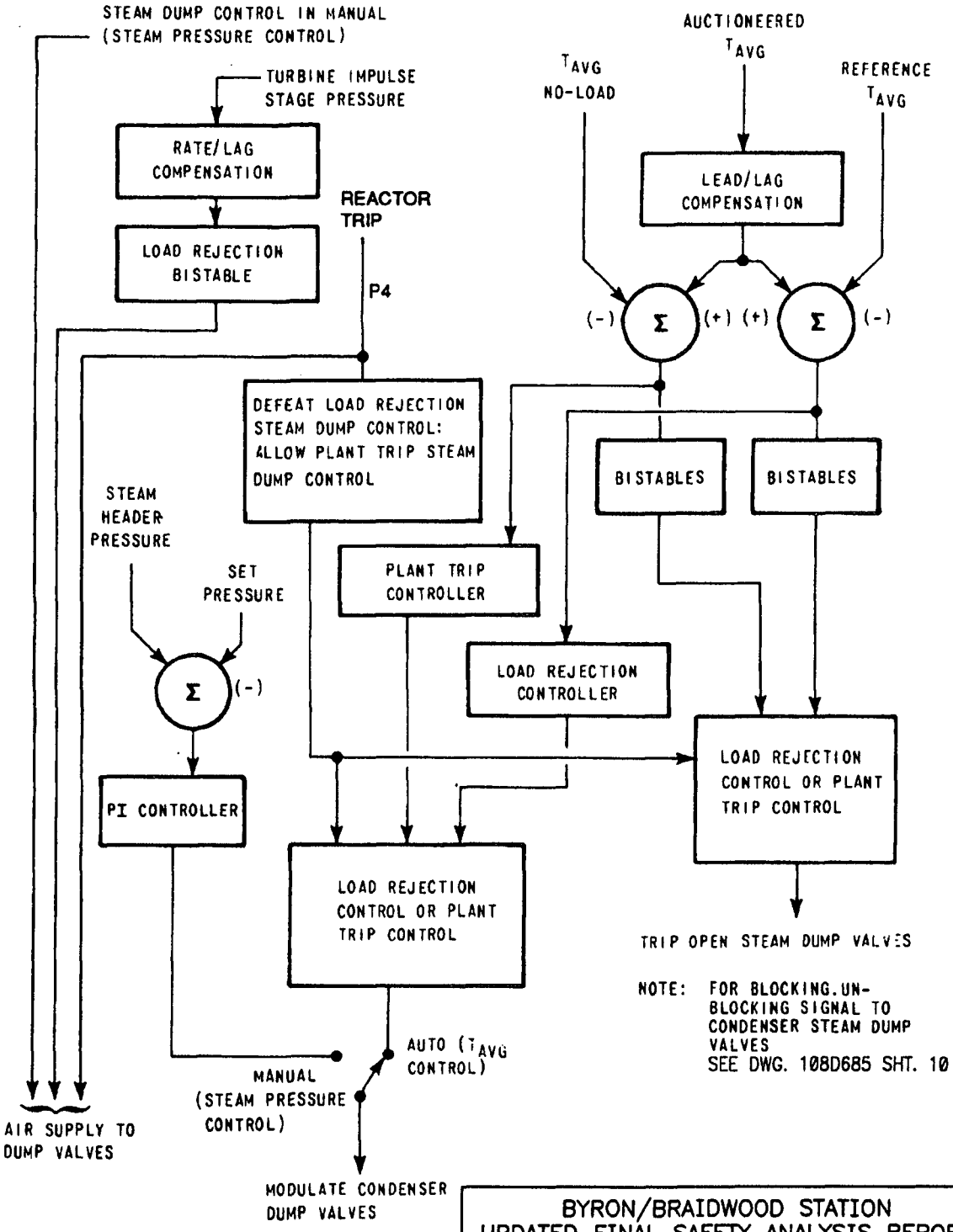
**BLOCK DIAGRAM OF STEAM GENERATOR WATER LEVEL CONTROL SYSTEM**




**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

FIGURE 7.7-7

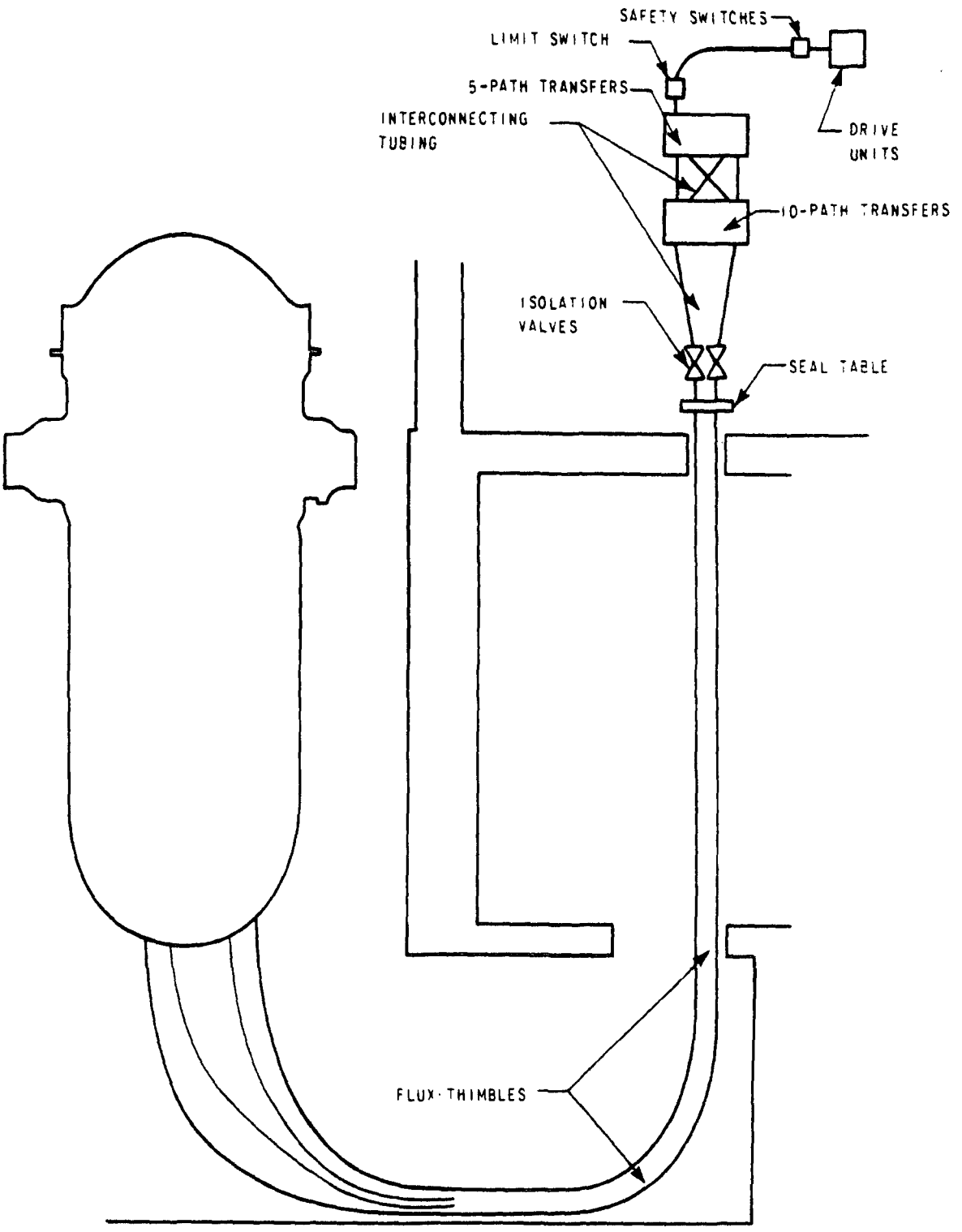
BLOCK DIAGRAM OF MAIN FEEDWATER
PUMP SPEED CONTROL SYSTEM




BYRON/BRAIDWOOD STATION
UPDATED FINAL SAFETY ANALYSIS REPORT

FIGURE 7.7–8

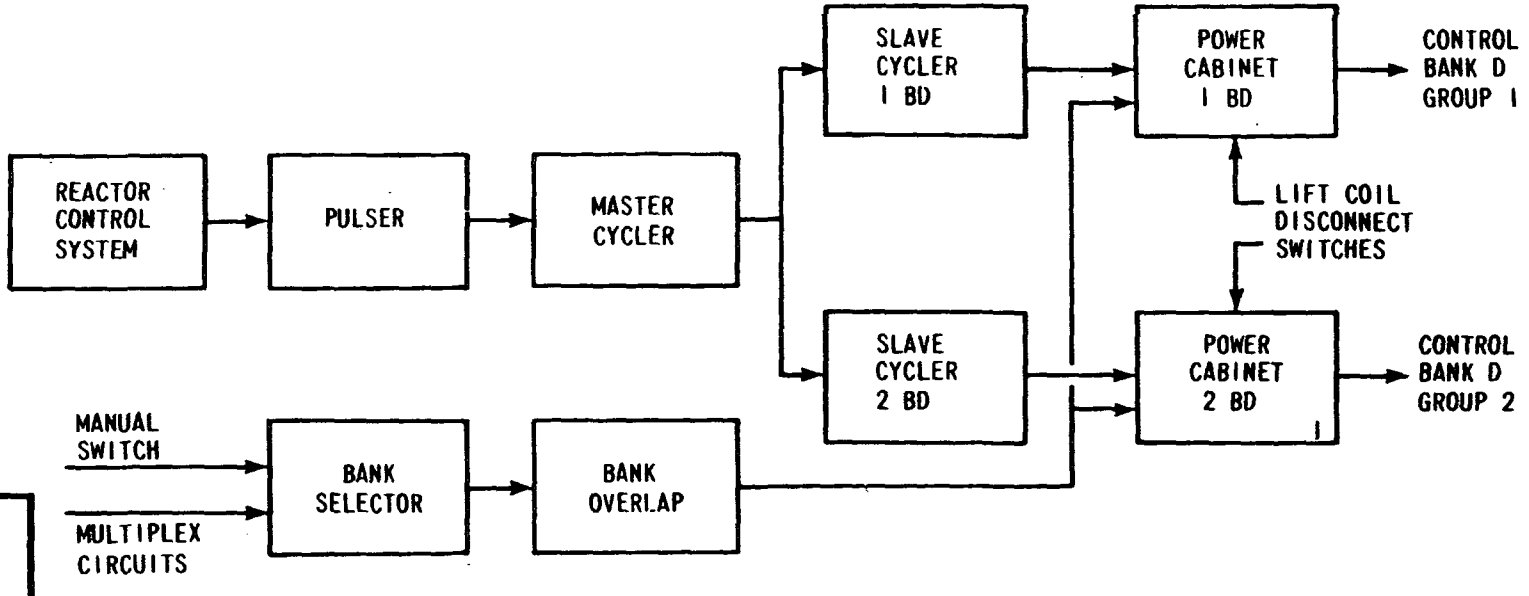
BLOCK DIAGRAM OF STEAM DUMP CONTROL SYSTEM

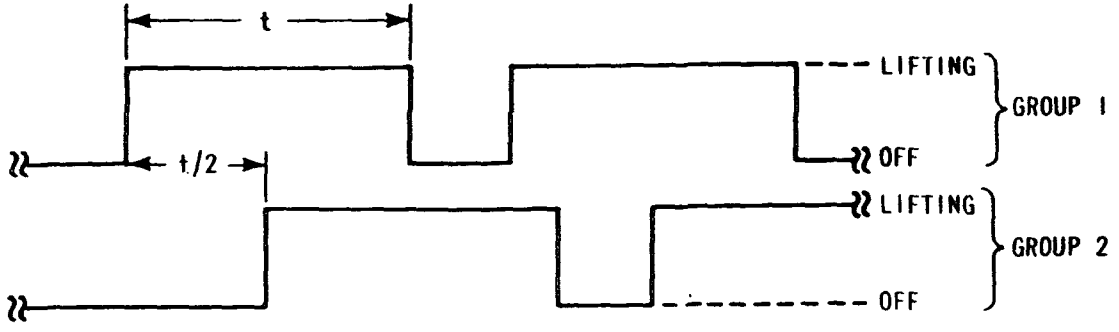



**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

FIGURE 7.7-9

BASIC FLUX—MAPPING SYSTEM

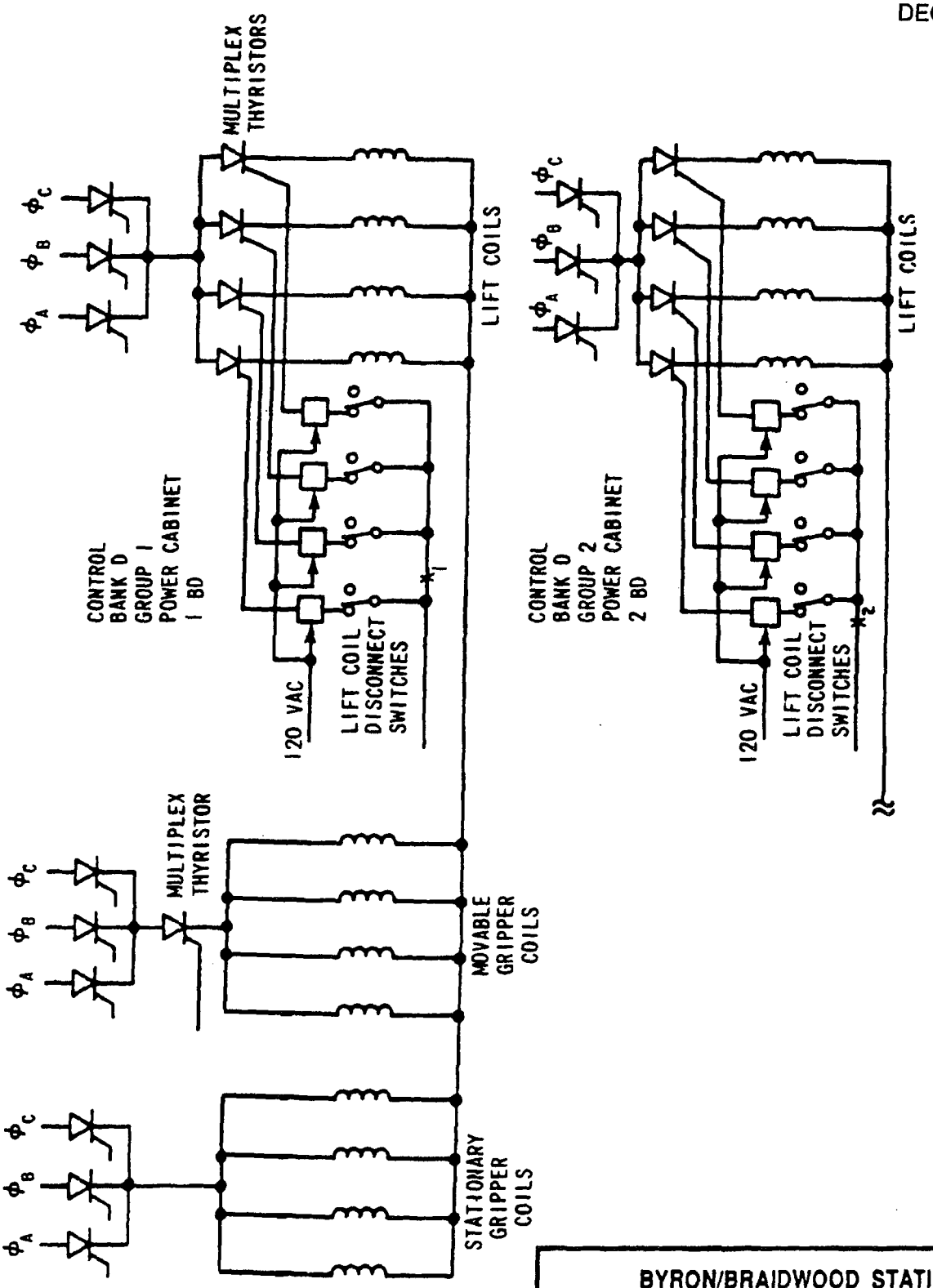



NORMAL SEQUENCING OF GROUPS WITHIN BANK

1 NOTE: ONLY CABINETS 1BD AND 2BD SHOWN. FOR MORE COMPLETE DIAGRAM INCLUDING POWER CABINETS 1AC, 2AC, AND SCD, SEE REF.1 IN SECTION 7.7.3

FIGURE 7.7-10
SIMPLIFIED BLOCK DIAGRAM
ROD CONTROL SYSTEM

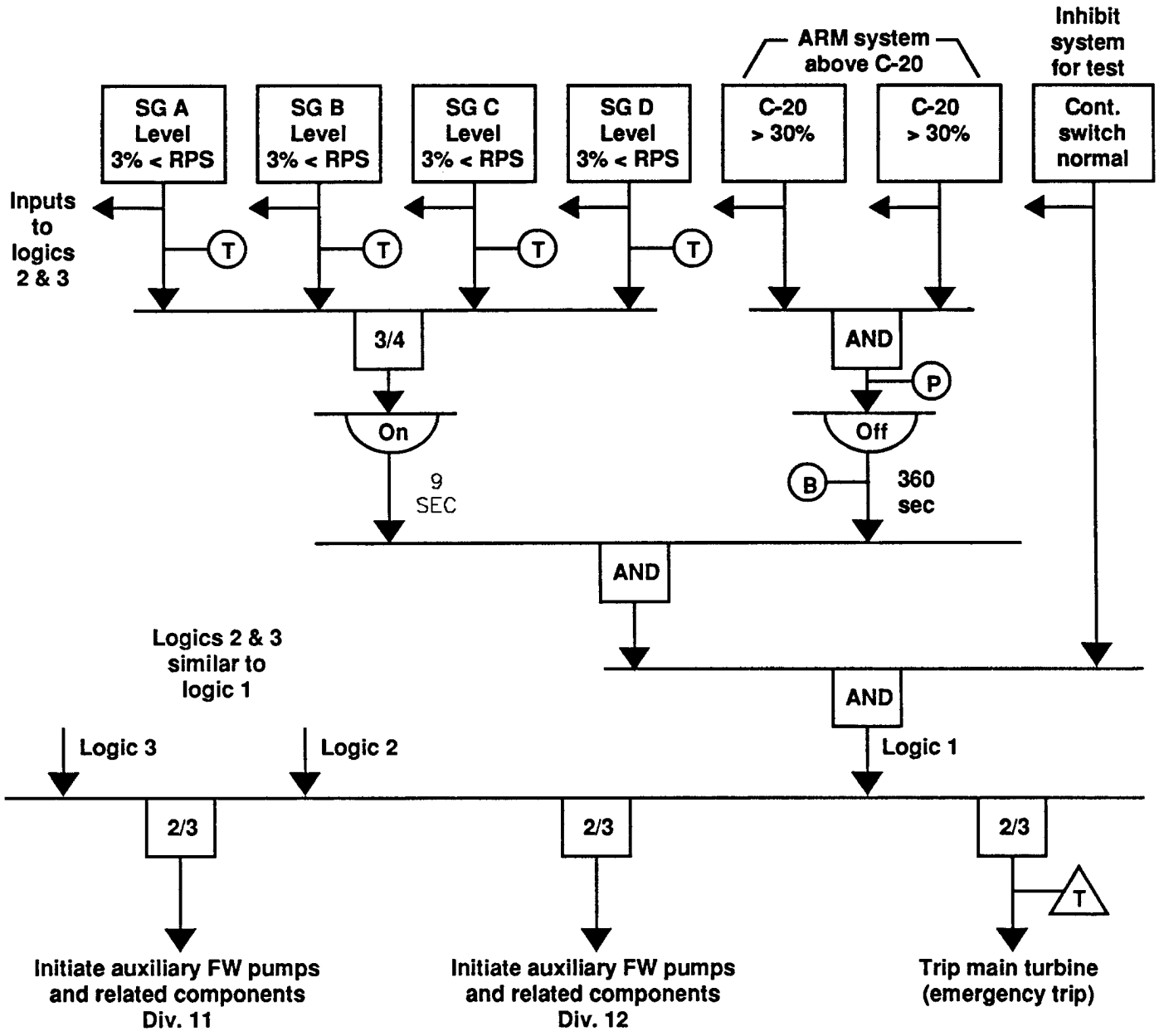



Note: Control bank D contains five control rods. Two control rods are in the group 1 power cabinet and three control rods are in the group 2 power cabinet. The remaining coil mechanisms are spares.

**BYRON/BRAIDWOOD STATIONS**
**UPDATED FINAL SAFETY ANALYSIS REPORT**

FIGURE 7.7-11

CONTROL BANK D PARTIAL SIMPLIFIED SCHEMATIC DIAGRAM POWER CABINETS 1 BD & 2 BD




BYRON/BRAIDWOOD STATIONS
UPDATED FINAL SAFETY ANALYSIS REPORT

FIGURE 7.7-12

ATWS MITIGATION SYSTEM
SIMPLIFIED LOGIC DIAGRAM

M2148.436 11-90