TABLE OF CONTENTS

Section	Title	Page
7.0	**INSTRUMENTATION AND CONTROLS**	
7.1	**INTRODUCTION**	**7.1-1**
7.1.1	Identification of Safety-Related Systems	7.1-4
7.1.1.1	Safety-Related Systems	7.1-4
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	7.1-8
7.1.2.2	Independence of Redundant Safety-Related Systems	7.1-12
7.1.2.3	Physical Identification of Safety-Related Equipment	7.1-15
7.1.2.4	Process Signal Isolation Relays	7.1-17
7.2	**REACTOR TRIP SYSTEM**	**7.2-1**
7.2.1	Description	7.2-1
7.2.1.1	System Description	7.2-1
7.2.1.2	Design Bases Information	7.2-17
7.2.1.3	Final Systems Drawings	7.2-19
7.2.2	Analyses	7.2-19
7.2.2.1	Evaluation of Design Limits	7.2-20
7.2.2.2	Evaluation of Compliance to Applicable Codes and Standards	7.2-23
7.2.2.3	Specific Control and Protection Interactions	7.2-33
7.2.2.4	Additional Postulated Accidents	7.2-36
7.2.3	Tests and Inspections	7.2-36
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
7.3.1.2	Design Bases Information	7.3-6
7.3.1.3	Final System Drawings	7.3-8
7.3.2	Analysis	7.3-8
7.3.2.1	System Reliability/Availability and Failure Mode and Effect Analyses	7.3-8
7.3.2.2	Compliance With Standards and Design Criteria	7.3-9
7.3.2.3	Further Considerations	7.3-16
7.3.2.4	Summary	7.3-17
7.4	**SYSTEMS REQUIRED FOR SAFE SHUTDOWN**	**7.4-1**
7.4.1	Description	7.4-1
7.4.1.1	Monitoring Indicators	7.4-1
7.4.1.2	Controls	7.4-2
7.4.1.3	Equipment and Systems Available for Cold Shutdown	7.4-6
7.4.2	Analysis	7.4-6

TABLE OF CONTENTS

Section	Title	Page
7.5	**INSTRUMENTATION SYSTEMS IMPORTANT TO SAFETY**	**7.5-1**
7.5.1	Post Accident Monitoring Instrumentation (PAM)	7.5-1
7.5.1.1	System Description	7.5-1
7.5.1.2	Variable Types	7.5-1
7.5.1.3	Variable Categories	7.5-2
7.5.1.4	Design Bases	7.5-3
7.5.1.5	General Requirements	7.5-6
7.5.1.6	Analysis	7.5-7
7.5.1.7	Tests and Inspections	7.5-7
7.5.2	Emergency Response Facilities Data System (ERFDS)	7.5-8
7.5.2.1	Safety Parameter Display System	7.5-8
7.5.2.2	Bypassed and Inoperable Status Indication System (BISI)	7.5-10
7.5.2.3	Technical Support Center and Nuclear Data Links	7.5-13
7.6	**ALL OTHER SYSTEMS REQUIRED FOR SAFETY**	**7.6-1**
7.6.1	120V ac and 125V dc Vital Plant Control Power System	7.6-1
7.6.2	Residual Heat Removal Isolation Valves	7.6-1
7.6.2.1	Description	7.6-1
7.6.2.2	Analysis	7.6-2
7.6.3	Refueling Interlocks	7.6-2
7.6.4	Deleted by Amendment 63.	7.6-2
7.6.5	Accumulator Motor-Operated Valves	7.6-2
7.6.6	Spurious Actuation Protection for Motor Operated Valves	7.6-3
7.6.7	Loose Part Monitoring System (LPMS) System Description	7.6-4
7.6.8	Interlocks for RCS Pressure Control During Low Temperature Operation	7.6-6
7.6.8.1	Analysis of Interlock	7.6-7
7.6.9	Switchover From Injection to Recirculation	7.6-8
7.6.9.1	Description of Instrumentation Used for Switchover	7.6-8
7.6.9.2	Initiation Circuit	7.6-9
7.6.9.3	Logic	7.6-9
7.6.9.4	Bypass	7.6-9
7.6.9.5	Interlocks	7.6-9
7.6.9.6	Sequence	7.6-10
7.6.9.7	Redundancy	7.6-10
7.6.9.8	Diversity	7.6-10
7.6.9.9	Actuated Devices	7.6-10
7.7	**CONTROL SYSTEMS**	**7.7-1**
7.7.1	Description	7.7-1
7.7.1.1	Control Rod Drive Reactor Control System	7.7-1
7.7.1.3	Plant Control Signals for Monitoring and Indicating	7.7-8
7.7.1.4	Plant Control System Interlocks	7.7-12
7.7.1.5	Pressurizer Pressure Control	7.7-13

TABLE OF CONTENTS

Section	Title	Page
7.7.1.6	Pressurizer Water Level Control	7.7-13
7.7.1.7	Steam Generator Water Level Control	7.7-14
7.7.1.8	Steam Dump Control	7.7-14
7.7.1.9	Incore Instrumentation	7.7-16
7.7.1.10	Control Board	7.7-18
7.7.1.11	Boron Concentration Measurement System	7.7-18
7.7.1.12	Anticipated Transient Without Scram Mitigation System Actuation	7.7-19
7.7.2	Analysis	7.7-20
7.7.2.1	Separation of Protection and Control System	7.7-21
7.7.2.2	Response Considerations of Reactivity	7.7-21
7.7.2.3	Step Load Changes Without Steam Dump	7.7-24
7.7.2.4	Loading and Unloading	7.7-24
7.7.2.5	Load Rejection Furnished By Steam Dump System	7.7-25
7.7.2.6	Turbine-Generator Trip With Reactor Trip	7.7-25
7.7.3	Deleted by Amendment 81	7.7-26
7A	**INSTRUMENTATION IDENTIFICATIONS AND SYMBOLS**	
7A.1	**IDENTIFICATION SYSTEM**	**7A.1-1**
7A.1.1	FUNCTIONAL IDENTIFICATION	7A.1-1
7A.1.1.1	Principal Function	7A.1-1
7A.1.1.2	Measured Variable	7A.1-2
7A.1.1.3	Readout or Passive Functions	7A.1-2
7A.1.1.4	Modifying Letters	7A.1-2
7A.1.1.5	Tagging Symbols	7A.1-2
7A.1.1.6	Special Identifying Letters	7A.1-2
7A.1.1.7	Pilot Lights	7A.1-2
7A.1.2	SYSTEM IDENTIFICATION	7A.1-3
7A.1.2.1	Identification Numbers	7A.1-3
7A.1.3	LOOP IDENTIFICATION	7A.1-3
7A.1.3.1	Instruments Common to Multiple Control Loops	7A.1-3
7A.1.3.2	Multiple Instruments with a Common Function	7A.1-3
7A.2	**SYMBOLS**	**7A.1-3**
7A.2.1	INSTRUMENT SYMBOL	7A.1-4

TABLE OF CONTENTS

Section	Title	Page

THIS PAGE INTENTIONALLY BLANK

LIST OF TABLES

Section	Title
Table 7.1-1	Watts Bar Nuclear Plant NRC Regulatory Guide Conformance
Table 7.1-2	Deleted by Amendment 8
Table 7.2-1	List of Reactor Trips
Table 7.2-2	Protection System Interlocks
Table 7.2-3	Reactor Trip System Instrumentation
Table 7.2-4	Reactor Trip Correlation
Table 7.3-1	Instrumentation Operating Condition For Engineered Safety Features
Table 7.3-2	Instrumentation Operating Condition For Isolation Functions
Table 7.3-3	Interlocks For Engineered Safety Features Actuation System
Table 7.5-1	Post Accident Monitoring Instrumentation Component Qualification Matrix (See Note)
Table 7.5-2	Regulatory Guide 1.97 Post Accident Monitoring Variables Lists Legend
Table 7.5-3	Deviations From Regulatory Guide 1.971
Table 7.7-1	Plant Control System Interlocks

LIST OF TABLES

Section **Title**

THIS PAGE INTENTIONALLY BLANK

LIST OF FIGURES

Section	Title
Figure 7.1-1	Protection System Block Diagram
Figure 7.1-2	Powerhouse-Units 1 and 2 Wiring Diagrams Control Boards Critical Wiring Braid Installation
Figure 7.1-3-SH-1	Train A and Train B Process Interlocks
Figure 7.1-3-SH-2	Train A and Train B Process Interlocks
Figure 7.1-3-SH-3	Train A and Train B Process Interlocks
Figure 7.1-3-SH-4	Train A and Train B Process Interlocks
Figure 7.2-1-SH-1	Powerhouse Unit 1 Electrical Logic Diagrams - Reactor Protection System
Figure 7.2-1-SH-2	Powerhouse Unit 1 Electrical Logic Diagrams - Reactor Protection System
Figure 7.2-1-SH-3	Powerhouse Unit 1 Electrical Logic Diagrams - Reactor Protection System
Figure 7.2-1-SH-4	powerhouse Unit 1 Electrical Logic Diagrams - Reactor Protection System
Figure 7.2-2	Setpoint Reduction Function for Overpower and Overtemperature ΔT Trips
Figure 7.3-1	ESF Test Circuits (Typical)
Figure 7.3-2	Deleted by Amendment 81
Figure 7.3-3-SH-1	Powerhouse Units 1 & 2 Electrical Logic Diagram Feedwater System
Figure 7.3-3-SH-2	Powerhouse Units 1 & 2 Auxiliary Feedwater System Logic Diagram
Figure 7.3-3-SH-3	Powerhouse Units 1 & 2 Electrical Logic Diagram for Safety Injection System
Figure 7.3-3-SH-4	Powerhouse Units 1 & 2 Logic Electrical Diagram for Containment Isolation
Figure 7.6-1	Deleted by Amendment 65
Figure 7.6-2	Deleted by Amendment 65
Figure 7.6-3	Powerhouse Unit 1 Electrical Logic Diagram for Safety Injection System
Figure 7.6-4	Powerhouse Auxiliary Building Units 1& 2 Wiring Diagrams for Safety Injection System
Figure 7.6-5	Reactor Building Unit 1 Variable Processing for Low Temperature Interlocks for RCS Pressure Control
Figure 7.6-6-SH-1	Powerhouse Unit 1 Electrical Logic Diagram for Safety Injection System
Figure 7.6-6-SH-2	Powerhouse Unit 1 Electrical Logic Diagram for Safety Injection System
Figure 7.6-6-SH-3	Powerhouse Electrical Logic Diagram Residual Heat Removal System
Figure 7.6-7-SH-1	RHR Suction Isolation Valve Interlocks
Figure 7.6-7-SH-2	RHR Bypass Valve Logic FCV-74-8 T (FCV-7 4-9)
Figure 7.7-1	Simplified Block Diagram of Reactor Control System
Figure 7.7-2	Control Bank Rod Insertion Monitor
Figure 7.7-3	Rod Deviation Comparator
Figure 7.7-4	Block Diagram of Pressurizer Pressure Control System

LIST OF FIGURES

Section	Title
Figure 7.7-5	Block Diagram of Pressurizer Level Control System
Figure 7.7-6	Block Diagram of Steam Generator Water Level Control System
Figure 7.7-7	Block Diagram of Main Feedwater Pump Speed Control System
Figure 7.7-8	Block Diagram of Steam Dump Control System
Figure 7.7-9	Basic Flux-Mapping System
Figure 7.7-10	Typical Location of Control Board Systems
Figure 7.7-11	Simplified Block Diagram Rod Control System
Figure 7.7-12	Control Bank D Partial Simplified Schematic Diagram Power Cabinets 1BD and 2BD
Figure 7A-1	Instrumentation Symbols and Tabulation from TVA DS E18.3.3
Figure 7A-2	Mechanical System Identification Numbers
Figure 7A-3	Mechanical Flow and Control Diagram Symbols
Figure 7A-4	Mechanical Basic Instrumentation and Radiation Symbols
Figure 7A-5	Mechanical Application of Basic Instrumentation Symbols
Figure 7A-6	Mechanical Digital Logic Symbols (and/or)

7.0 INSTRUMENTATION AND CONTROLS

7.1 INTRODUCTION

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

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

It is shown that the applicable criteria and codes, such as the General Design Criteria and IEEE Standards, concerned with the safe generation of nuclear power are met by these systems.

Definitions

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

Channel - An arrangement of components and modules or software as required to generate a single protective action signal when required by a plant condition. A channel loses its identity where single action signals are combined.

DNBR (Departure from Nucleate Boiling Ratio) - The ratio of the critical heat flux (defined as the transition from nucleate boiling, to film boiling) to the actual local heat flux.

Module - An 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.

Software - The entire set of programs, procedures, and related documentation associated with a system, especially a computer system.

Components - Items from which the system is assembled (e.g., resistors, capacitors, wires, connectors, transistors, tubes, switches, springs, etc.).

Single Failure - Any single event which results in a loss of protective function of a component or components of a system. Multiple failures resulting from a single event will be treated as a single failure.

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

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

Type Tests - Tests made on one or more units to verify adequacy of design.

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.

Reproducibility - This definition is taken from SAMA Standard PMC-20.1-1973. 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 SAMA Standard PMC-20.1-1973. An accuracy statement for a device falls under Note 2 of the 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," 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.

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 % 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).

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

Cold Shutdown - The reactor is in the cold shutdown condition when the reactor is subcritical by at least 1% $\Delta k/k$ and T(avg) is $\leq 200^{\circ}F$ with T(avg) defined as the average temperature across a reactor vessel as measured by the hot and cold leg temperature detectors.

Hot Shutdown Condition - When the reactor is subcritical by an amount greater than or equal to the margin to be specified in the applicable technical specification and T(avg) is greater than or equal to the temperature to be specified in the applicable technical specification.

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

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

System Response Time

Reactor Trip System Response Time: The time delays are defined as the time required for the reactor trip (i.e., the time the rods are free and begin to fall) to be initiated following a step change in the variable being monitored from at least 5% below (or above) to at least 5% above (or below) the trip setpoint.

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

Normal Operating Conditions - For this document, these conditions cover all normal process temperature and pressure changes. Also included are ambient temperature changes around the transmitters and racks.

Control Accuracy - This definition includes channel accuracy, accuracy of readout devices (isolator, controller), and rack environmental effects. Where an isolator separates control and protection signals, the isolator accuracy is added to the channel accuracy to determine control accuracy, but credit is taken for tuning beyond this point; i.e., the accuracy of these modules (excluding controllers) is included in the original channel accuracy. It is simply defined as the accuracy of the control signal in percent of the span of that signal. This will then include gain changes where the control span is different from the span of the measured variable. Where controllers are involved, the control span is the input span of the controller. No error is included for the time in which the system is in a non-steady state condition.

7.1.1 Identification of Safety-Related Systems

7.1.1.1 Safety-Related Systems

The Nuclear Steam Supply System (NSSS) instrumentation required to function to achieve the system responses assumed in the safety evaluations and those needed to shut down the plant are given in this section.

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 Section 7.1.2.1. Figure 7.1-1 is a block 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 and is 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 Section 7.1.2.1.

7.1.1.1.3 Vital Instrumentation and Control Power Supply System

Design bases for the vital control power supply system are given in Section 7.1.2.1. Further description of the system is provided in Section 8.3.

7.1.1.1.4 Auxiliary Control Air System

The auxiliary control air system supplies essential control air to safety-related equipment such as the auxiliary feedwater control valves, dampers in the auxiliary building gas treatment system and the emergency gas treatment system; and the Control Building HVAC system. Further description of the system is given in Section 9.3.1.

7.1.1.2 Safety-Related Display Instrumentation

The Post Accident Monitoring System (PAM) provides essential information required by the operator to diagnose and monitor significant accident conditions. The accident-monitoring instrumentation is designed with redundant channels so that a single failure does not prevent the operator from determining the nature of an accident, the functioning of the engineered safety features, the need for operator action, and the response of the plant to the safety measures in operation. This system is described in Section 7.5.

All other safety-related display instrumentation is discussed in Section 7.5.

The Bypassed and Inoperable Status Indication System (BISI) does not perform a safety function, nor do administrative procedures call for immediate operator action based solely on BISI indication. The BISI equipment is isolated from the associated safety-related equipment so as to preclude any abnormal or normal action of the BISI from preventing the performance of a safety function. The BISI is described in detail in Section 7.5.

7.1.1.3 Instrumentation and Control System Designers

All systems discussed in Chapter 7 have definitive functional requirements developed on the basis of the Westinghouse NSSS design. TVA is responsible for the total design of the WBN instrumentation and controls systems. The RPS, ESFAS, and SSPS are generally the instrumentation and controls systems within the scope of the Westinghouse supply. Figure 7.2-1 (Sheets 1 through 3) shows the logic for the Reactor Protection System.

7.1.1.4 Plant Comparison

System functions for all systems discussed in Chapter 7 are similar to those of Sequoyah Nuclear Plant. Detailed comparison is provided in Section 1.3.

7.1.2 Identification of Safety Criteria

Section 7.1.2.1 gives design bases for the systems given in Section 7.1.1.1, except for the auxiliary control air system which is described in Section 9.3.1 and the safety-related display instrumentation systems which are described in Section 7.5. Design bases for nonsafety-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. 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 discussed in Sections 7.2, 7.3 and 7.5.

The documents listed below were considered in the design of the systems given in Section 7.1.1. In general, the scope of these documents is given in the document itself. This determines the systems or parts of systems to which the document is applicable. A discussion of compliance with each document for systems within its scope is provided in the referenced sections.

Because some documents were issued after design and testing had been completed, the equipment documentation may not meet the format requirements of some standards. Table 7.1-1 and Notes 1 through 10 identify the degree of conformance to applicable documents and justify exceptions. The documents considered are:

(1) "General Design Criteria for Nuclear Power Plants, "Appendix A to Title 10 CFR Part 50, July 7, 1971." (See Sections 7.2, 7.3, 7.4, and 7.6).

(2) "Regulatory Guide 1.11 - Instrument Lines Penetrating Primary Reactor Containment," Regulatory Guides for Water-Cooled Nuclear Power Plants, Division of Reactor Standards, Atomic Energy Commission.

(3) "Regulatory Guide 1.22 - Periodic Testing of Protection System Actuation Functions," Regulatory Guides for Water-Cooled Nuclear Power Plants, Division of Reactor Standards, Atomic Energy Commission. (See Table 7.1-1, Note 2).

(4) Regulatory Guide 1.29 (Revision 1) - "Seismic Design Classification," Regulatory Guides for Water-Cooled Nuclear Power Plants," Directorate of Regulatory Standards, Atomic Energy Commission.

(5) The Institute of Electrical and Electronic Engineers, Inc., "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations," IEEE Standard 279-1971. (See Sections 7.2., 7.3, 7.6).

(6) The Institute of Electrical and Electronic Engineers, Inc., "IEEE Standard Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations," IEEE Standard 308-1971.

(7) The Institute of Electrical and Electronic Engineers, Inc.," IEEE Standard for Electrical Penetration Assemblies in Containment Structures for Nuclear Fueled Power Generating Stations," IEEE Standard 317-1976. (See Section 8.3.1.2.3).

(8) The Institute of Electrical and Electronic Engineers, Inc., "IEEE Trial-Use Standard: General Guide for Qualifying Class I Electric Equipment for Nuclear Power Generating Stations," IEEE Standard 323-1971. (See Table 7.1-1, Note 4).

(9) The Institute of Electrical and Electronic Engineers, Inc., "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations", IEEE Std. 323-1974.

(10) Deleted by Amendment 90.

(11) The Institute of Electrical and Electronic Engineers, Inc., "IEEE Standard Installation, Inspection, and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations," IEEE Standard 336-1971. (See Section 8.3.1.2.2).

(12) The Institute of Electrical and Electronic Engineers, Inc., "IEEE Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems," IEEE Standard 338-1971. (See Section 7.3.2.2.5 and Table 7.1-1, Note 1).

(13) IEEE-Std. 338-1987 "IEEE Standard Criteria for the Periodic Testing of Nuclear Power Generating Station Safety Systems".

(14) The Institute of Electrical and Electronic Engineers, Inc., "IEEE Trial-Use Guide for Seismic Qualification of Class I Electric Equipment for Nuclear Power Generating Stations," IEEE Standard 344-1971. (See Section 3.10).

(15) The Institute of Electrical and Electronic Engineers, Inc, "IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations," IEEE Std. 344-1975.

(16) The Institute of Electrical and Electronic Engineers, Inc, "IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations," IEEE Std. 344-1987.

(17) The Institute of Electrical and Electronic Engineers, Inc, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems," IEEE Std. 352-1975.

(18) The Institute of Electrical and Electronic Engineers, Inc., "IEEE Trial-Use Guide for the Application of the Single-Failure Criterion to Nuclear Power Generating Station Protection Systems," IEEE Standard 379-1972. (See Table 7.1-1, Note 3).

(19) The Institute of Electrical and Electronic Engineers, Inc, "IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems," IEEE Std. 379-1988.

(20) The Institute of Electrical and Electronic Engineers, Inc, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," IEEE Std. 384-1981.

(21) The Institute of Electrical and Electronic Engineers, Inc, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Std. 603-1980.

(22) "Regulatory Guide 1.53 - Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," Regulatory Guides for Water-Cooled Nuclear Power Plant Division of Reactor Standards, Atomic Energy Commission. (See Table 7.1-1, Note 3).

(23) Regulatory Guide 1.47, May 1973 "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems".

(24) Regulatory Guide 1.75, September 1978 "Physical Independence of Electrical Systems".

(25) Regulatory Guide 1.89, November 1974 "Qualification of Class 1E Equipment for Nuclear Power Plants".

(26) Regulatory Guide 1.97, December 1980 "Instrumentation for Light-Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident".

(27) Regulatory Guide 1.100, August 1977 "Seismic Qualification of Electrical Equipment for Nuclear Power Plants".

(28) Regulatory Guide 1.105, November 1976 "Instrument Setpoints".

(29) Regulatory Guide 1.118, June 1978 "Periodic Testing of Electric Power and Protection Systems".

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

- Regulatory Guide 1.153, endorses the guidance of IEEE-Std. 603-1980.

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

ANSI/IEEE-ANS-7-4.3.2-1982 - expands and amplifies the requirements of IEEE-Std. 603-1980

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

Regulatory Guide 1.152, endorses the guidance of ANSI/IEEE-7-4.3.2-1982.

7.1.2.1 Design Bases

The technical design bases for the protection systems are provided by Westinghouse equipment specifications which consider the functional requirements for these systems and applicable criteria as identified in Table 7.1-1.

7.1.2.1.1 Reactor Trip System

The reactor trip system acts to limit the consequences of Condition II events 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 analyzed in Chapter 15 are not exceeded during Condition II events and that these events can be accommodated without developing into more severe conditions.

The design requirements for the reactor trip system are derived by analyses of plant operating 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 Section 7.2.1. The design limits for this system are:

(1) Minimum DNBR shall not be below the limiting value as a result of any anticipated transient or malfunction (Condition II faults).

(2) Power density shall not exceed the rated linear power density for Condition II events. See Chapter 4 for fuel design limits.

(3) The stress limit of the RCS for the various conditions shall be as specified in Chapter 5.

(4) Release of radioactive material shall not be sufficient to interrupt or restrict public use of those areas beyond the exclusion distance or to exceed the guidelines of 10 CFR 100 as a result of any Condition III fault.

(5) For any Condition IV fault, release of radioactive material shall not result in an undue risk to public health and safety nor shall it exceed the guidelines of 10 CFR 100, "Reactor Site Criteria."

7.1.2.1.2 Engineered Safety Features Actuation System (ESFAS)

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

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

(1) Automatic Actuation Requirements

The primary functional requirement of the ESFAS is to receive input signals (information) from the various on-going processes within the reactor plant and containment and automatically provide, as output, timely and effective signals to actuate the various components and subsystems comprising the engineered safety features system. These signals must assure that the engineered safety features system will meet its performance objectives as outlined in Chapter 6.

Figure 7.3-3 (Sheets 1 through 4) shows the logic associated with the ESF actuation system.

(2) Manual Actuation Requirements

The ESFAS has provisions for manually initiating from the main control room the functions of the engineered safety features system. Manual actuation serves as backup to the automatic initiation and provides control of selective engineered safety features service features.

7.1.2.1.3 Vital Control Power Supply System

The vital 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 8.3. The design bases are given below:

(1) The inverter shall have the capacity and regulation required for the ac output for proper operation of the equipment supplied.

(2) Redundant loads shall be assigned to different distribution panels which are supplied from different inverters.

(3) 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.

(4) Each of the distribution panels shall have access to an inverter and a standby power supply.

(5) The system design details are in Section 8.3.1.2.2.

7.1.2.1.4 Standby Power

Design bases and system description for the standby power supply are provided in Chapter 8.

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 on 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 279-1971, Sections 4.11, 4.12, 4.13 and 4.14. A discussion of bypasses provided is given in Sections 7.2 and 7.3.

7.1.2.1.7 Equipment Protection

The criteria for equipment protection are given in Chapter 3. Equipment related to safe operation of the plant is designed, constructed and installed to protect it from 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 344-1971. During construction, independence and separation are achieved, as required by IEEE 279-1971, either by barriers or physical separation. 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 system. Functional diversity is discussed in WCAP 7706, "An Evaluation of Solid State Logic Reactor Protection in Anticipated Transients," Reference 1. The extent of diverse system variables has been evaluated for a wide variety of postulated accidents as discussed in WCAP 7306, "Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors," 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 nuclear flux measurements, reactor coolant loop temperature and flow measurements, pressurizer pressure and level measurements, reactor coolant pump under frequency and under voltage measurements, and steam generator water level 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.

(1) Low pressurizer pressure

(2) High containment pressure.

7.1.2.1.9 Trip Setpoints

The reactor protection system trip setpoints have been selected to ensure that core damage and loss of integrity of the reactor coolant system are prevented during anticipated operational events. These setpoints were analytically determined in accordance with the methodology described in Reference [6]. Both the nominal (trip setpoint) and limiting (allowable value) settings have been incorporated into the Technical Specifications. Nominal settings are more conservative than the limiting setpoints. This allows for measurement and calibration uncertainties and instrument

channel drift which may occur between periodic tests without exceeding the limiting setpoints.

7.1.2.2 Independence of Redundant Safety-Related Systems

The safety-related systems in Section 7.1.1.1 are designed to meet the independence and separation requirements of General Design Criteria (GDC) 22 (Appendix A to 10CFR50, 1971) and Paragraph 4.6 of IEEE 279-1971. The administrative responsibility and control provided during the design and installation is discussed in Chapter 17 which addresses the Quality Assurance programs applied by Westinghouse and TVA.

The electrical power supply instrumentation and control conductors for redundant circuits of a nuclear plant have physical separation including PAM Category I and protection set I, II, III and IV instrumentation and control. Their cables are run in separate raceways to preserve divisional integrity and to ensure that no single credible event will prevent operation of the associated function due to electrical conductor damage. Detailed information pertaining to electrical cable for safety-related systems is given in Section 8.3.1.4. Critical circuits and functions include: power, control, and process protection channels associated with the operations of the reactor trip system or engineered safety features actuation system. Failure events are evaluated for credibility and credible events shall include, but not be limited to, the effects of short circuits, pipe rupture, missiles, etc., and are considered in the basic plant design. Control board details are given in Section 7.7.1.10. In the control board, separation of redundant circuits is maintained as described in Section 7.1.2.2.2.

Instrument sensing lines (including capillary systems) which serve safety-related systems identified in Section 7.1.1.1 are designed to meet the independence requirements of criterion 22 of the 1971 General Design Criteria and IEEE 279-1971 Section 4.6. The requirements consider the following events: (1) normal activities in the area (e.g., maintenance); (2) high and moderate energy jet streams, missiles, and pipe whip; and (3) possible damage caused by falling loads from the plant lifting systems (e.g., cranes, monorails). Exceptions to these requirements shall be evaluated for technical adequacy and documented in Design Basis Documents.

7.1.2.2.1 General

(1) Cables of redundant circuits shall be run in separate cable trays, conduits, ducts, penetrations, etc.

(2) Circuits for nonredundant functions should be run in cable trays or conduit separated from those used for redundant circuits. Where this can not be accomplished, nonredundant circuits may be run in a cable tray, conduit, etc., assigned to a redundant function. When so routed, it must remain with that particular redundant circuit routing and shall not cross over to other redundant groups.

(3) Horizontal and vertical separation shall be maintained between cable trays associated with redundant circuits.

(4) Where it is impractical for reasons of equipment arrangement to provide separate cable trays, cables of redundant circuits shall be isolated by approved barriers or proven safe by test or analysis.

(5) Power and control cables rated at 600V or below shall not be placed in cable trays with cables rated above 600V.

(6) Low-level type signal cables shall not be routed in cable trays containing power cables. Higher level protection instrumentation analog and signal cables (above 100 mV) may be routed in the same tray with control cables if a tray barrier is provided between cables.

7.1.2.2.2 Specific Systems

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. Each redundant channel is energized from a separate ac power feed.

Within the process protection system there are four separate protection channel sets. Redundant protection channels are separated by locating the processing electronics of the redundant channels in different protection channel rack sets. Separation of redundant channels begins at the sensors and is maintained in the field wiring, containment penetrations, and process protection channel racks. Thus any single failure within a channel will not prevent initiation of a required protection system action.

In the nuclear instrumentation system and the solid state protection system racks where redundant channels of protection 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.

Independence of the logic trains is discussed in Sections 7.2 and 7.3. 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 control rod drive mechanisms, permitting the rods to free fall into the core.

(1) Reactor Trip System

(a) Separate routing is maintained between the four reactor trip system process protection channels, including the sensor signals, comparator signals, and associated power supplies.

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

spatial separation, by an approved barrier, or by separate cable trays or wireways) from the four protection instrumentation channels.

(2) Engineered Safety Features Actuation System

(a) Separate routing is maintained for the four redundant sets of ESF actuation system process protection channels, comparator output signals and power supplies for such systems. The separation of these four redundant and independent protection channel sets is maintained from sensors through process protection racks to logic system cabinets.

(b) Separate routing of the ESF actuation signals from the two redundant logic system cabinets is maintained. The ESF actuation signals are also separated from the four process protection channels.

(c) Separate routing of redundant 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.

(3) Vital Control Power Supply System

The separation criteria presented above 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.

(4) Control Board

Control board switches and associated lights are generally furnished in modules. Modules provide a degree of physical protection for the switches, associated lights and wiring. Teflon wire is used within the module and between the module and the first termination point.

Modular train column wiring is formed into wire bundles and carried to metal wireways (gutters). Gutters are run into metal vertical wireways (risers). The risers are the interface between field wiring and control board wiring. Risers are arranged to maintain the separated routing of the field cable trays.

Wiring within control boards has been designed and installed to maintain physical independence. Design features include enclosed modular switches, metal wireways, use of metallic woven braid over approved insulation of critical wires. PVC type tubing (Tygon) has been used in some installations to insulate up to approximately 6 inches of the drain wire where signal cable is broken out to terminate the cable at termination points.

Figure 7.1-2 shows the details of the control boards critical wiring braid installation. Wiring for each train is routed from the field to separate vertical risers, separated horizontally in enclosed horizontal wireways, and then routed from the wireway to the enclosed switch module in metallic braid.

Maximum air space between cables of different trains has been maintained and in no case do cables from different trains touch nor can they migrate with time to touch.

In order to maintain separation between wiring associated with different logic 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.

Safety-related indicators, e.g., post accident monitoring indicators are separated by metallic barrier plates and/or air separation. Teflon insulated wire is used between the indicators and the first termination point. The wire routing method is similar to that used for the modules.

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

7.1.2.2.3 Fire Protection

Details of fire protection are provided in Section 9.5.1.

7.1.2.3 Physical Identification of Safety-Related Equipment

There are four separate sets of process protection channel racks identifiable with equipment associated with the reactor trip system and with the engineered safety features actuation system. A process protection channel set may consist of more than one instrumentation rack. The color coding of each instrumentation rack nameplate coincides with the color code established for the protection instrumentation channel of which it is a part. Redundant channels are separated by locating them in different protection channel racks. Separation of redundant channels begins at the process sensors and is maintained in the field wiring, containment penetrations, and process protection racks to the redundant trains in the logic racks. The solid state protection system input cabinets are divided into four isolated compartments, each serving one of the four redundant process protection channels. Horizontal 1/8-inch thick solid steel barriers, coated with fire-retardant paint, separate the compartments. Four solid steel wireways coated with fire-retardant paint enter the input cabinets vertically. The wireway for a particular compartment is open into that compartment so that flame could not propagate to affect other channels. At the logic racks the protection set color coding for redundant channels is clearly maintained until the channel loses its identity in the redundant logic trains. The color-coded nameplates described below provide identification of equipment associated with protective functions and their channel set association.

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

Post accident monitoring and train-oriented modules are identified as follows:

	Color
Train A	Orange and white
Train B	Brown and White
Special[1]	Gold and Black
Postaccident Monitoring Channel 1	Purple and White
Postaccident Monitoring Channel 2	Green and Black
Nondivisional (Nonsafety-related)	White and Black
Normal Offsite PWR Supply	White and Black
Alternate Offsite PWR Supply	White and Black

All nonrack-mounted protective equipment and components are provided with an identification tag or nameplate. Small electrical components such as relays

[1]The circuits requiring special separations are suffix S and described in Section 8.3.1.4.3.

have nameplates on the enclosure which houses them. All cables are numbered with identification tags. In congested areas, such as under or over the control boards, instrument racks, etc., cable trays and conduits containing redundant circuits are identified using permanent markings. The purpose of such markings, discussed in detail in Section 8.3.1.4, is to facilitate cable routing identification for future modifications or additions. Positive permanent identification of field routed cables is provided by nameplates on the input panels of the solid state logic protection system.

7.1.2.4 Process Signal Isolation Relays

Criteria for Process Signal Isolation Relays

The following criteria are to be used in providing isolation between process signals and safety circuits:

(1) A safety signal derived from the Solid-State Protection System (SSPS) shall override the process signal.

(2) The isolation relays shall have a coil to contact rating equal to or greater than the maximum credible ac or dc potential that could be applied to the non-1E circuit at its end points or intermediate routing.

(3) The isolation relays and racks designated as Train A or Train B shall be seismically qualified.

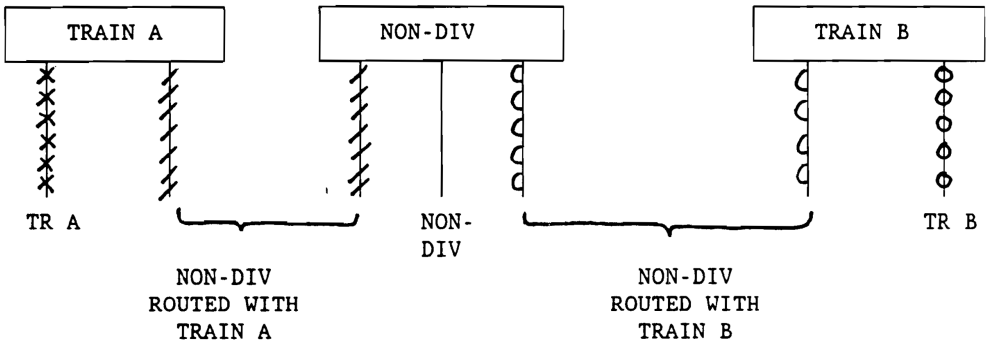
Implementation of Criteria

(1) The following is a listing of the Auxiliary Relay Racks (ARR) and the cable routing scheme utilized

AUXILIARY RELAY RACKS

LOCATION	TRAIN A	NON-DIV	TRAIN B
AUXILIARY CONTROL	1-L-11A	1-L-10	1-L-11B
B0P AUX INST ROOM	1-R-73,74	1-R-71,72,75,76,80	1-R-77,78
NSSS AUX INST ROOM	1-R-54	1-R-58	1-R-55
	(ARI)	(AR3)	(AR2)

ROUTING SCHEME-AUXILIARY RELAY RACKS



(2) Figure 7.1-3 (Sheets 1-4) illustrates the various isolation configurations used in the design of Watts Bar.

REFERENCES

(1) W. C. Gangloff and W. D. Luftus, "An Evaluation of Solid State Logic Reactor Protection in Anticipated Transients," WCAP-7706-L, July 1971, (Westinghouse NES Proprietary), and WCAP-7706, July 1971.

(2) T. W. T. Burnett, "Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors." WCAP-7306, April 1969.

(3) Deleted by Amendment 81.

(4) W. C. Gangloff, "An Evaluation of Anticipated Operational Transient in Westinghouse Pressurized Water Reactors." WCAP-7486-L, December 1970, (Westinghouse NES Proprietary), and WCAP-7486, May 1971.

(5) Erin, L. E., "Topical Report Eagle 21 Microprocessor-Based Process Protection System," WCAP-12374, Rev. 1, December 1991 (Westinghouse Proprietary Class 2); WCAP-12375, Rev. 1, December 1991 (Westinghouse Proprietary Class 3).

(6) Reagan, J. R., "Westinghouse Setpoint Methodology for Protection Systems, Watts Bar Units 1 and 2, Eagle 21 Version, "WCAP-12096, Rev. 5 (Westinghouse Proprietary Class 2).

(7) "Westinghouse Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrument System, WCAP-10271, Supp. 1 and WCAP 10271-P-A, Supp. 2."

Table 7.1-1 Watts Bar Nuclear Plant NRC Regulatory Guide Conformance (Page 1 of 7)

The extent to which the recommendations of the applicable NRC regulatory guides and IEEE standards are followed for the Class 1E instrumentation and control systems is shown below. The symbol (F) indicates full compliance. Those which are not fully implemented are discussed in the referenced sections of the FSAR and in the footnotes as indicated.

Regulatory Guide 1.11, "Instrument Lines Penetrating Primary Containment" (F).

Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions" (F, see note 2).

Regulatory Guide 1.29, "Seismic Design Classification" (F).

Regulatory Guide 1.30, "Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment." (See Section 7.1 for compliance.)

Regulatory Guide 1.40, "Qualification Tests of Continuous Duty Motors Installed Inside the Containment of Water-Cooled Nuclear Power Plants" (F).

Regulatory Guide 1.45, "Reactor Coolant Pressure Boundary Leakage Detection systems" (F, See Note 7).

Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems" (F see note 5).

Regulatory Guide 1.53, "Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems" (F see note 3).

Regulatory Guide 1.62, "Manual Initiation of Protective Actions" (F).

Regulatory Guide 1.63, "Electrical Penetration Assemblies in Containment Structures for Water-Cooled Nuclear Power Plants" (See Section 8.1 for compliance).

Regulatory Guide 1.68, "Preoperational and Initial Startup Test Program for Water-Cooled Power Reactors" (See Table 14.2-3).

Table 7.1-1 Watts Bar Nuclear Plant NRC Regulatory Guide Conformance (Page 2 of 7)

Regulatory Guide 1.73, "Qualification Tests for Electric Valve Operators Installed Inside the Containment of Nuclear Power Plants" (F).
Regulatory Guide 1.75, "Physical Independence of Electric Systems" (See Sections 7.1.2.2, 7.1.2.3, 8.3.1.4, 8.3.2.4, and 8.3.2.5 for compliance).
Regulatory Guide 1.79, (ECCS Testing) See Section 6.3.4.
Regulatory Guide 1.80, "Preoperational Testing of Instrument Air Systems" (F).
Regulatory Guide 1.89, "Environmental Qualification of Certain Electrical Equipment Important to Safety for Nuclear Power Plants" (See note 4).
Regulatory Guide 1.97, December 1980 "Instrumentation for Light-Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident" (See Section 7.5).
Regulatory Guide 1.100, August 1977 "Seismic Qualification of Electrical Equipment for Nuclear Power Plants" (See Note 8).
Regulatory Guide 1.105, November 1976 "Instrument Setpoints" (See Note 8).
Regulatory Guide 1.118, June 1978 "Periodic Testing of Electric Power and Protection Systems" (See Notes 8 and 11), (See Section 8.1.5.3, Note 8, for electric power systems).
Regulatory Guide 1.153, December 1985 "Criteria For Power, Instrumentation and Control Portions of Safety Systems" (See Notes 8 and 9).
ANSI/IEEE-ANS-7-4.3.2-1982 "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations" (See Notes 8 and 10).
Regulatory Guide 1.152, "Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants" (P) (See note 6).

Table 7.1-1 Watts Bar Nuclear Plant NRC Regulatory Guide Conformance (Page 3 of 7)

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

IEEE Standard 308-1971, "Class 1E Power Systems for Nuclear Power Generating Stations" (F).

IEEE Std. 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," (See Note 8).

IEEE Standard 338-1971, "Periodic Testing of Nuclear Power Generating Station Safety Systems" (See note 1 and Section 7.3.2.2.5 for compliance).

IEEE Standard 338-1977, "IEEE Standard Criteria for the Periodic Testing of Nuclear Power Generating Station Safety Systems" (See Note 11).

IEEE-Std, 338-1987, "IEEE Standard Criteria for the Periodic Testing of Nuclear Power Generating Station Safety Systems," (See Note 8).

IEEE Standard 344-1971, "Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations" (F) (For clarification of conformance to

IEEE Standard 344-1975, See Section 3.10.1).

IEEE Std. 344-1987, "IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations," (See Note 8).

IEEE Std. 352-1975, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems," (See Note 8).

IEEE Std. 379-1988, "IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems," (See Note 8).

IEEE Std. 384-1981, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," (See Note 8).

Table 7.1-1 Watts Bar Nuclear Plant NRC Regulatory Guide Conformance (Page 4 of 7)

IEEE Std. 603-1980, IEEE Standard Criteria For Safety Systems for Nuclear Power Generating Stations," (See Note 8).

Note 1 Conformance to IEEE 338-1971

The periodic testing of the reactor protection systems conforms to the requirements of IEEE Standard 338-1971 with the following comments:

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

Protection systems response times from the sensor through the actuated device, as identified in the Watts Bar Technical Requirements Manual, will be verified. Technical Specifications require periodic testing on at least 18-month intervals. 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 all channels are tested at least once every (N times 18) months, where N is the total number of redundant channels in a specific protection function.

The measurement of response time at the specified frequencies 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.

2.The reliability goals specified in Paragraph 4.2 of IEEE Standard 338 are being developed, and adequacy of test frequencies are demonstrated in WCAP 10271 Supp. 1 and 2.

3.The periodic test frequency discussed in Paragraph 4.3 of IEEE Standard 338 and specified in the plant Technical Specifications is conservatively selected to assure that equipment associated with protection functions has not drifted beyond its minimum performance requirements. If any protection channel appears to be marginal or requires more frequent adjustments due to plant condition changes, the test frequency is accelerated to accommodate the situation until the marginal performance is resolved.

4.The test interval discussed in Paragraph 5.2, IEEE Standard 388, is developed primarily on past operating experience and modified if necessary to assure that system and subsystem protection is reliably provided. Analytic methods for determining reliability are not used to determine test interval.

Table 7.1-1 Watts Bar Nuclear Plant NRC Regulatory Guide Conformance (Page 5 of 7)

Note 2 Conformance to Regulatory Guide 1.22

Periodic testing of the reactor trip and engineered safety features actuation systems, as described in Sections 7.2.2 and 7.3.2, complies with NRC Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions." Under the present design, there are functions which are not tested at power because to do so would render the plant in a less safe condition. These are as follows:

1.Turbine trip equipment that causes a reactor trip; the trip of turbine from this same turbine trip equipment also is taken credit for on a safety injection or reactor trip;

2.Generation of a reactor trip by use of the manual trip switch;

3Generation of a reactor trip by use of the manual safety injection switch;

4.Closing the main steam line stop valves;

5.Closing the feedwater control valves;

6.Closing the feedwater isolation valves;

7.Reactor coolant pump component cooling water isolation valves (close);

8.Reactor coolant pump seal water return valves (close).

The actuation logic for the functions listed is tested as described in Sections 7.2 and 7.3. As required by Regulatory Guide 1.22, where actuated equipment is not tested during reactor operation it has been determined that:

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

Table 7.1-1 Watts Bar Nuclear Plant NRC Regulatory Guide Conformance (Page 6 of 7)

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

3.The equipment will be routinely tested when the reactor is shutdown as defined in the Technical Specification.

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

Note 3 Conformance to IEEE 379-1972 and 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 requirements of Regulatory Guide 1.53. The formal analyses required by the standard have not been documented exactly as outlined although parts of such analyses are published in various documents (e.g. Reference 4). Westinghouse has gone beyond the required analyses and has performed a fault-tree analysis Reference [1].

The referenced Topical Reports provide 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-379 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.

Note 4 Conformance to Regulatory Guide 1.89

Watts Bar Nuclear Power Plant 1E equipment within the scope of 10 CFR 50.49 is qualified in accordance with IEEE 323-1971 or IEEE 323-1974. (See Reference [1] of Section 3.11). Reference [5] provides additional information for the Eagle 21 process protection system.

Table 7.1-1 Watts Bar Nuclear Plant NRC Regulatory Guide Conformance (Page 7 of 7)

Note 5 Conformance to Regulatory Guide 1.47

Watts Bar Nuclear Plant will be in full compliance with the intent of Regulatory Guide 1.47 (BISI) Revision 0, as described in Section 7.5.2.2.

Note 6 Conformance to Regulatory Guide 1.152

Watts Bar Nuclear Plant process protection racks are qualified by procedures and testing to Westinghouse's interpretation of Regulatory Guide 1.152 (WCAP-13191, Watts Bar Nuclear Plant Eagle 21 Process Protection System Replacement Hardware Verification and Validation Report, April 1992). Regulatory Guide 1.152 endorses the guidance of ANSI/IEEE-ANSI-7-4.3.2-1982.

Note 7 Conformance to Regulatory Guide 1.45

Compliance to Regulatory Guide 1.45 is as identified in Section 5.2.7.3.

Note 8These Rules, Regulations and standards are applicable to the design of the Eagle 21 process protection system cabinets. Unless stated otherwise, the revision in effect on December 1, 1983 is applicable to the design.

Note 9Regulatory Guide 1.153 endorses the guidance of IEEE Std. 603-1980.

Note 10ANSI/IEEE-ANS-7-4.3.2-1982 - expands and amplifies the requirements of IEEE Std. 603-1980.

Note 11 Conformance to Regulatory Guide 1.118

The design of the Eagle 21 process protection system cabinets complies with the requirements of Regulatory Guide 1.118 R2 except as follows:

Position C.6(a) - Where feasible, test switches or other necessary equipment will be installed permanently to minimize the use of temporary jumpers in testing in accordance with the requirements in IEEE Standard 338-1977.

Table 7.1-2 Deleted by Amendment 8

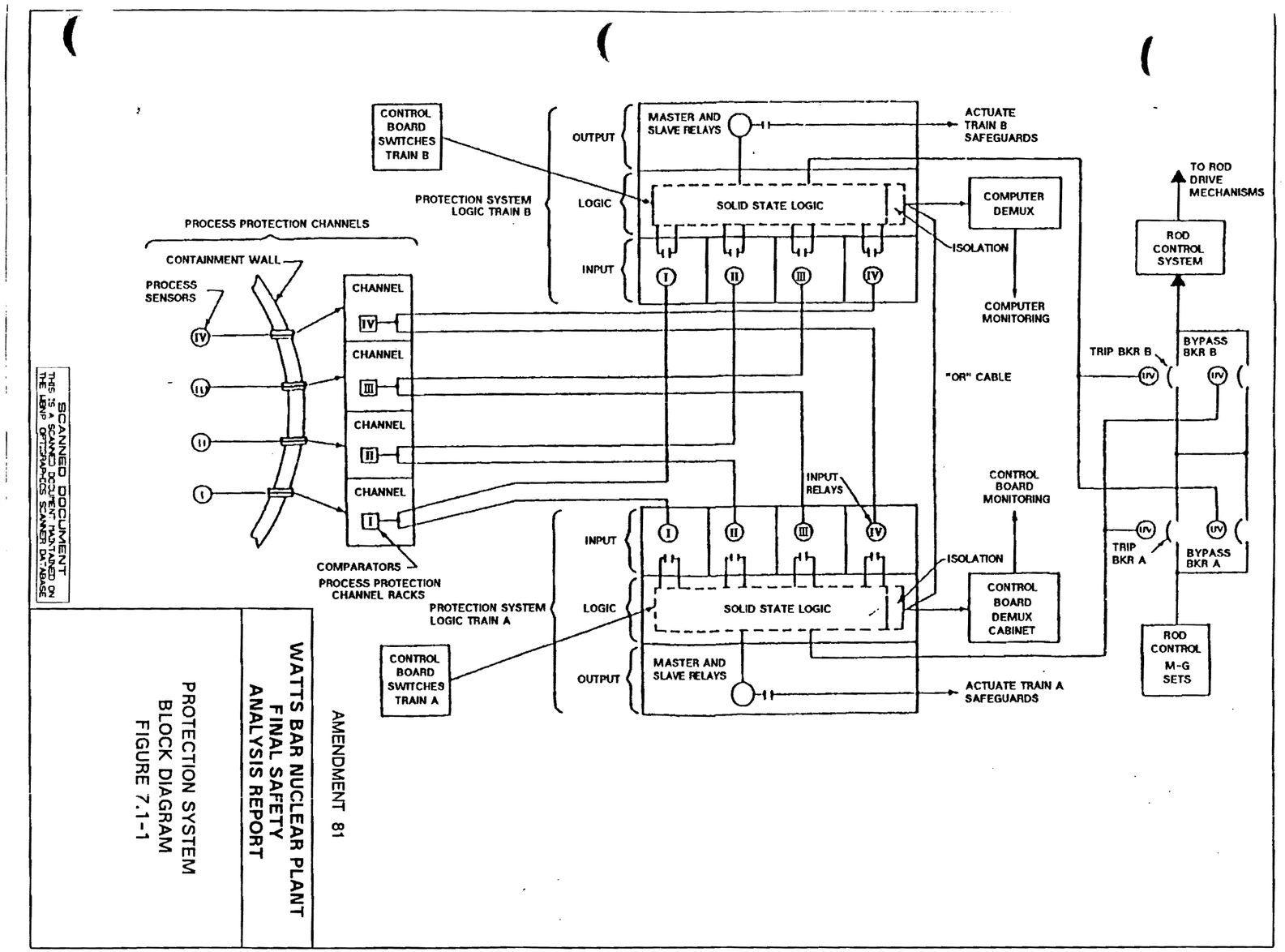
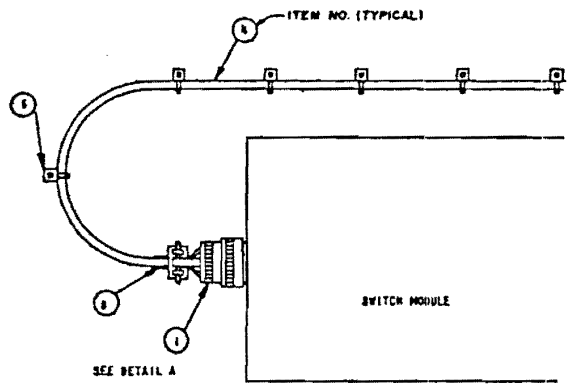
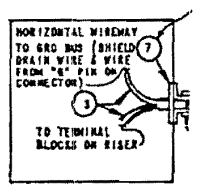


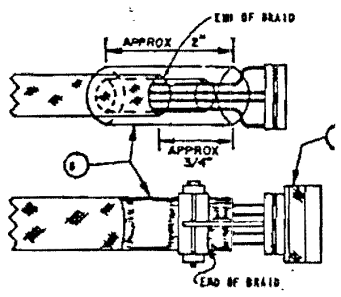
Figure 7.1-1 Protection System Block Diagram

SECTION 1. CONTROL BOARD CRITICAL WIRING

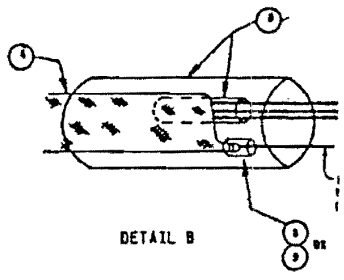




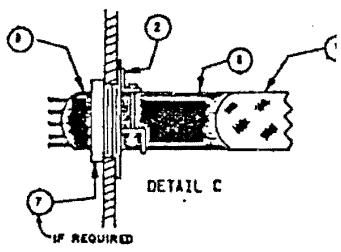
BRAID INSTALLATION FOR CONTROL BOARD
(SIDE VIEW)



DETAIL A



DETAIL B



DETAIL C

1.0 FOR CONTROL BOARDS WHICH CONTAIN MORE THAN ONE TRAIN OF CRITICAL WIRING ALL TRAI TRAIN B WIRING SHALL BE ENCLOSED IN METAL BRAID FROM THE DEVICE CONNECTOR OR TER TO THE HORIZONTAL WIRING DUCTS. ALL TRAIN A OR TRAIN B CABLES THAT TERMINATE A DEVICE (NOT RUN THROUGH THE RISER) SHALL BE ENCLOSED IN METAL BRAID INSIDE THE B

1.0.7 IN PANEL 1-M-13, CABLE/WIRING DESIGNATED "D", "E", "F" AND "G" SHALL BE SEPA FROM EACH OTHER AND SHALL BE ROUTED WITH ANY OTHER SUFFIX CABLE/WIRING. NON-DIVISIONAL CABLE/WIRING WITHIN THE PANEL MUST BE ROUTED SEPARATE FRO SUFFIX.

1.0.8 "J" DESIGNATED CABLE/WIRING MAY BE ROUTED WITH "A" DESIGNATED CABLE/WIR "K" DESIGNATED CABLE/WIRING MAY BE ROUTED WITH "B" DESIGNATED CABLE/WIR "J" DESIGNATED CABLE/WIRING SHALL BE SEPARARED FROM "K" DESIGNATED CABLE

A) CALIBRATION LAB ACCEPTANCE CRITERIA

ON A WEEKLY BASIS, BURNDY TOOL TYPE # MRND WITH DIE SET #MRT-24 MUST HAVE A SAMPLE CRIMP VERIFIED BY THE CALIBRATION LAB.

TWO CRITERIA MUST BE MET TO HAVE THE TOOL ACCEPTED:

1) UL-486-A PULL TEST - A PULL TEST IN ACCORDANCE WITH UL-486-A SHALL BE PERFORMED WITH A MINIMUM OF 30# FORCE FOR ONE MINUTE.
2) DIMENSION CHECK - A DIMENSION OF .053" TO .060" (HEIGHT OF CROSS - SECTION OF CRIMPED SAMPLE) MUST BE VERIFIED PER BURNDY DRAWING SC66423 R2. ATTACHED SH. 2.

B) FIELD INSPECTION ACCEPTANCE CRITERIA

1) ASSURE WIRE IS NOT LOOSE IN CONNECTOR BARREL BY PULLING ON PIN OR SOCKET.
2) ASSURE THE PIN OR SOCKET HAS NO OBVIOUS DAMAGE. THE CRIMPED CONTACT SHALL EXHIBIT NO EVIDENCE OF FRACTURING, CHIPPING, FLAKING, OR PROTRUDING SHARP EDGES.
3) NO CONDUCTOR INSULATION SHALL BE ALLOWED UNDER THE BARREL OF THE CONNECTOR.
4) CONDUCTOR MUST BE VISIBLE THROUGH INSPECTION HOLE TO ASSURE PROPER SEATING.
5) WIRE INSULATION MUST BE CLOSE TO THE BARREL; NO MORE THAN .030" +.006 -.000 OF CONDUCTOR SHALL BE VISIBLE AT THE END OF BARREL. (STRIP BACK LENGTH IS 1/4" ± 1/64").
6) ASSURE ALL CONDUCTOR STRANDS HAVE BEEN CAPTURED BY THE BARREL.
7) CONTACTS SHALL BE CLEAN, FREE OF BURRS, OXIDES, OR FILMS.

SECTION 3. BURNDY PIN ACCEPTANCE CRITERIA

3.1 CALIBRATION LAB ACCEPTANCE CRITERIA

B.1 ON A MONTHLY BASIS, BURNDY TOOL TYPE # MRND WITH DIE SET #MRT-21 MUST BE VERIFIED BY THE CALIBRATION LAB.

THE CRITERIA TO HAVE THE TOOL ACCEPTED IS AS FOLLOWS:

1) DIMENSION CHECK - A DIMENSION OF .016" TO .024" (HEIGHT OF SPACE BETWEEN CRIMPING JAWS WHILE IN FULLY CLOSED POSITION) MUST BE VERIFIED PER BRUNDY DRAWING SC61661 R2. (ATTACH SH. 3).

B.2 FIELD INSPECTION ACCEPTANCE CRITERIA

1) ASSURE WIRE IS NOT LOOSE IN CONNECTOR BARREL BY PULLING ON PIN OR SOCKET.
2) ASSURE THE PIN OR SOCKET HAS NO OBVIOUS DAMAGE. THE CRIMPED CONTACT SHALL EXHIBIT NO EVIDENCE OF FRACTURING, CHIPPING, FLAKING, OR PROTRUDING SHARP EDGES.
3) NO CONDUCTOR INSULATION SHALL BE ALLOWED UNDER THE BARREL OF THE CONNECTOR.
4) CONDUCTOR MUST BE VISIBLE THROUGH INSPECTION HOLE TO ASSURE PROPER SEATING.
5) WIRE INSULATION MUST BE CLOSE TO THE BARREL; NO MORE THAN .030" +.006 -.000 OF CONDUCTOR SHALL BE VISIBLE AT THE END OF BARREL. (STRIP BACK LENGTH IS 1/4" ± 1/64").
6) ASSURE ALL CONDUCTOR STRANDS HAVE BEEN CAPTURED BY THE BARREL.
7) CONTACTS SHALL BE CLEAN, FREE OF BURRS, OXIDES, OR FILMS.

REFERENCES:

1. MAIN CONTROL BOARD E-SPEC 952367 FOR WATTS BAR CONTRACT NO. 71C62-54114.
DESIGN CRITERIA FOR SEPARATION OF ELECTRIC EQUIPMENT AND WIRING WB-DC-30-4
WATTS BAR FSAR SECTION 7.1.2.2.2
2. 1040885 - CONCEPT OF BRAID INSTALLATION OVER CRITICAL WIRING.

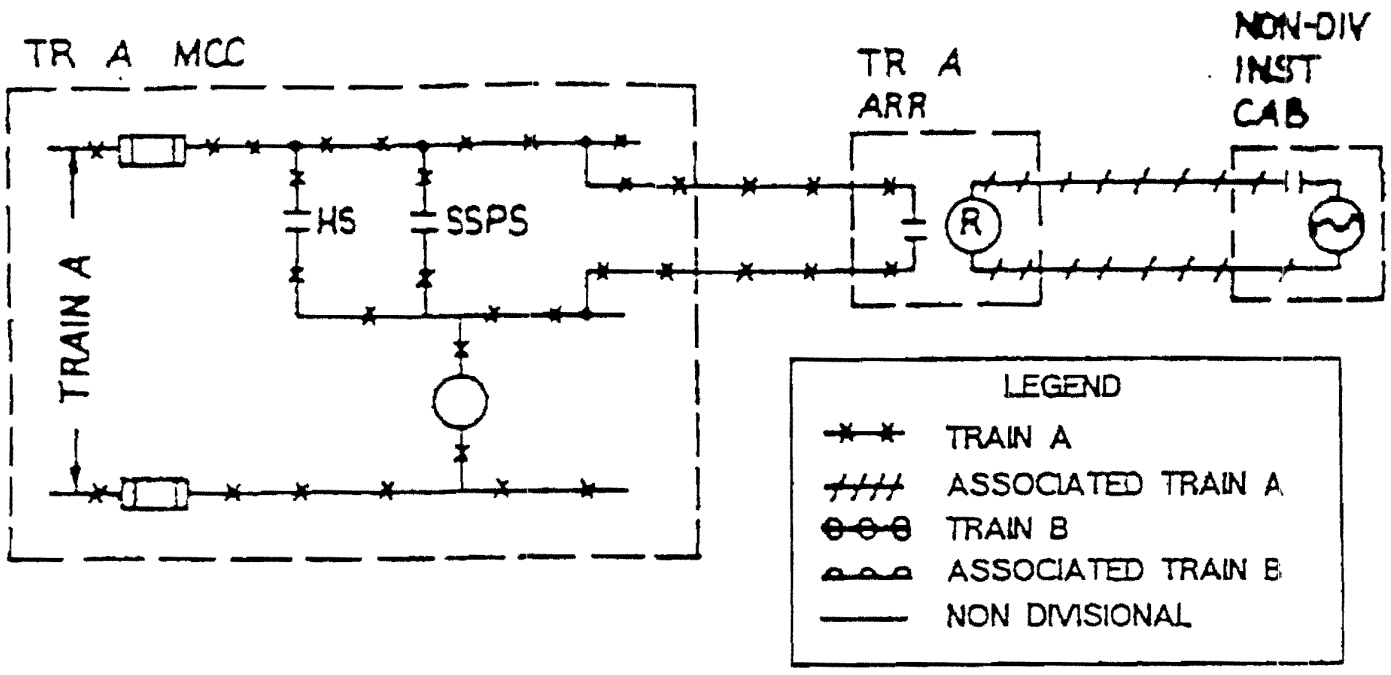
AMENDMENT 81

WATTS BAR
FINAL SAFETY
ANALYSIS REPORT

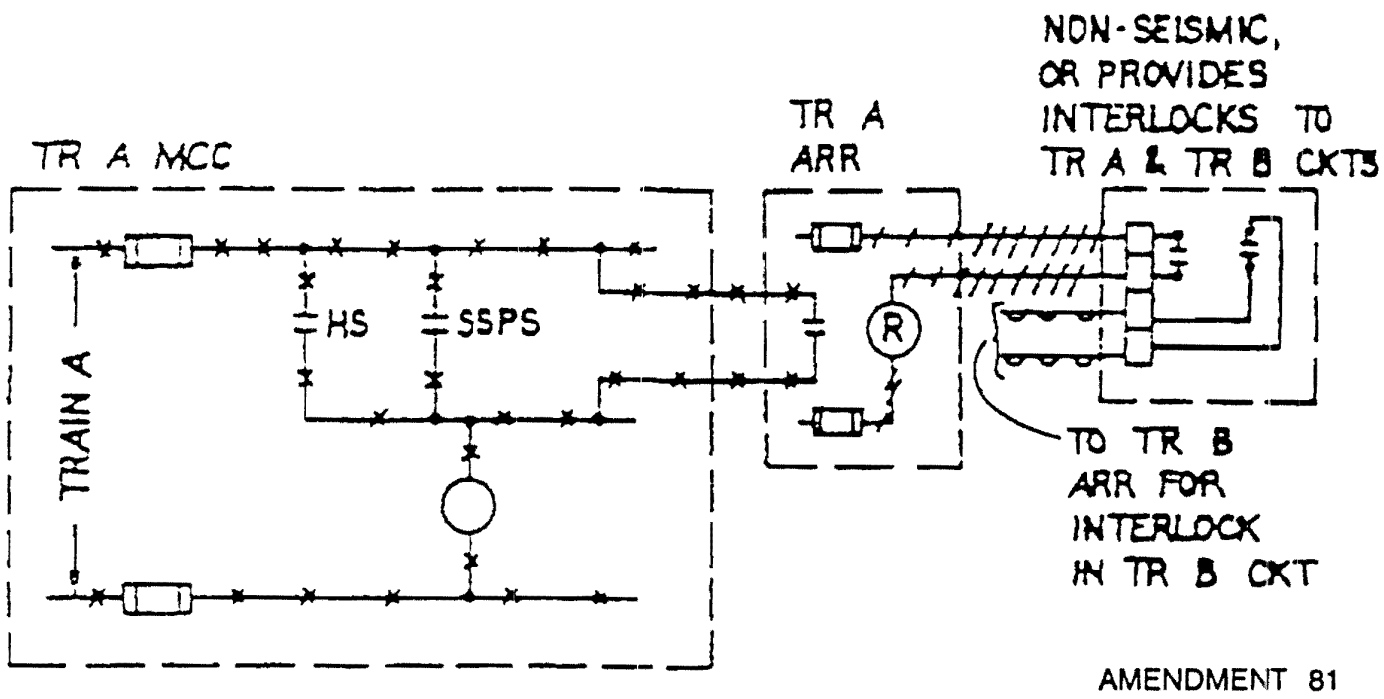
POWERHOUSE
UNITS 1 & 2
WIRING DIAGRAMS
CONTROL BOARDS CRITICAL WIRING
BRAID INSTALLATION
TVA DRAWING 45W1640 REV. E
FIGURE 7.1-2

Figure 7.1-2 Powerhouse-Units 1 and 2 Wiring Diagrams Control Boards Critical Wiring Braid Installation

1 TRAIN A CIRCUIT WITH PROCESS INTERLOCK DERIVED FROM NON-DIVISIONAL INSTRUMENTATION CABINET WHICH HAS A 120 V AC OUTPUT (SIMILAR FOR TRAIN B CKTS)



2. TRAIN A CIRCUIT WITH PROCESS INTERLOCK DERIVED FROM A NON-SEISMIC DEVICE OR A PANEL WHICH HAS INTERLOCKS IN BOTH TRAIN A AND TRAIN B CIRCUITS.



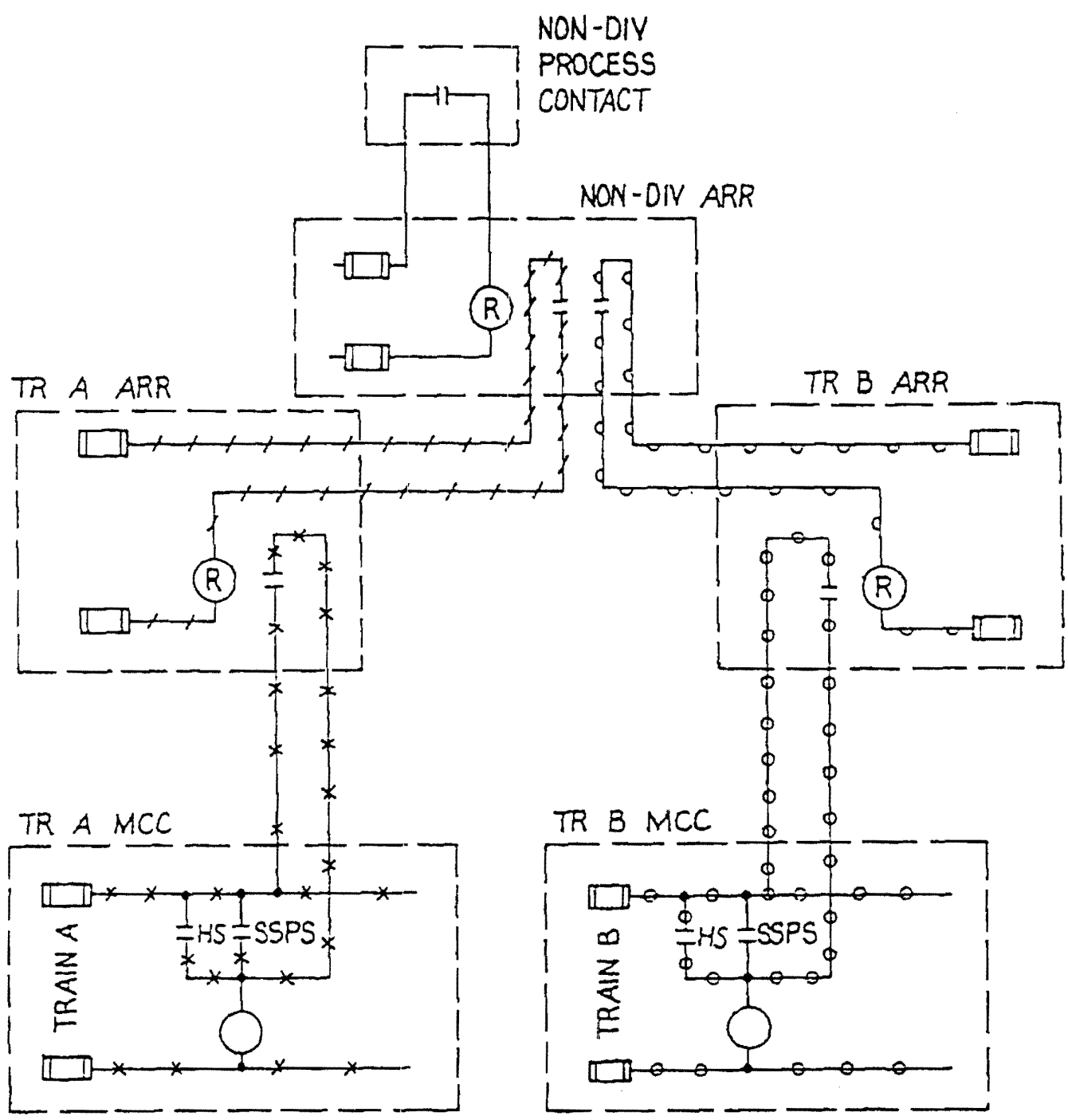
AMENDMENT 81

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

TRAIN A AND TRAIN B
PROCESS INTERLOCKS
FIGURE 7.1-3 (SHEET 1)

SCANNED DOCUMENT
THIS IS A SCANNED DOCUMENT MAINTAINED ON THE WBNP OPTIGRAPHICS SCANNER DATABASE

Figure 7.1-3-SH-1 Train A and Train B Process Interlocks



AMENDMENT 81

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

TRAIN A AND TRAIN B
PROCESS INTERLOCKS
FIGURE 7.1-3 (SHEET 2)

SCANNED DOCUMENT
THIS IS A SCANNED DOCUMENT MAINTAINED ON
THE WBNP OPTIGRAPHICS SCANNER DATABASE

Figure 7.1-3-SH-2 Train A and Train B Process Interlocks

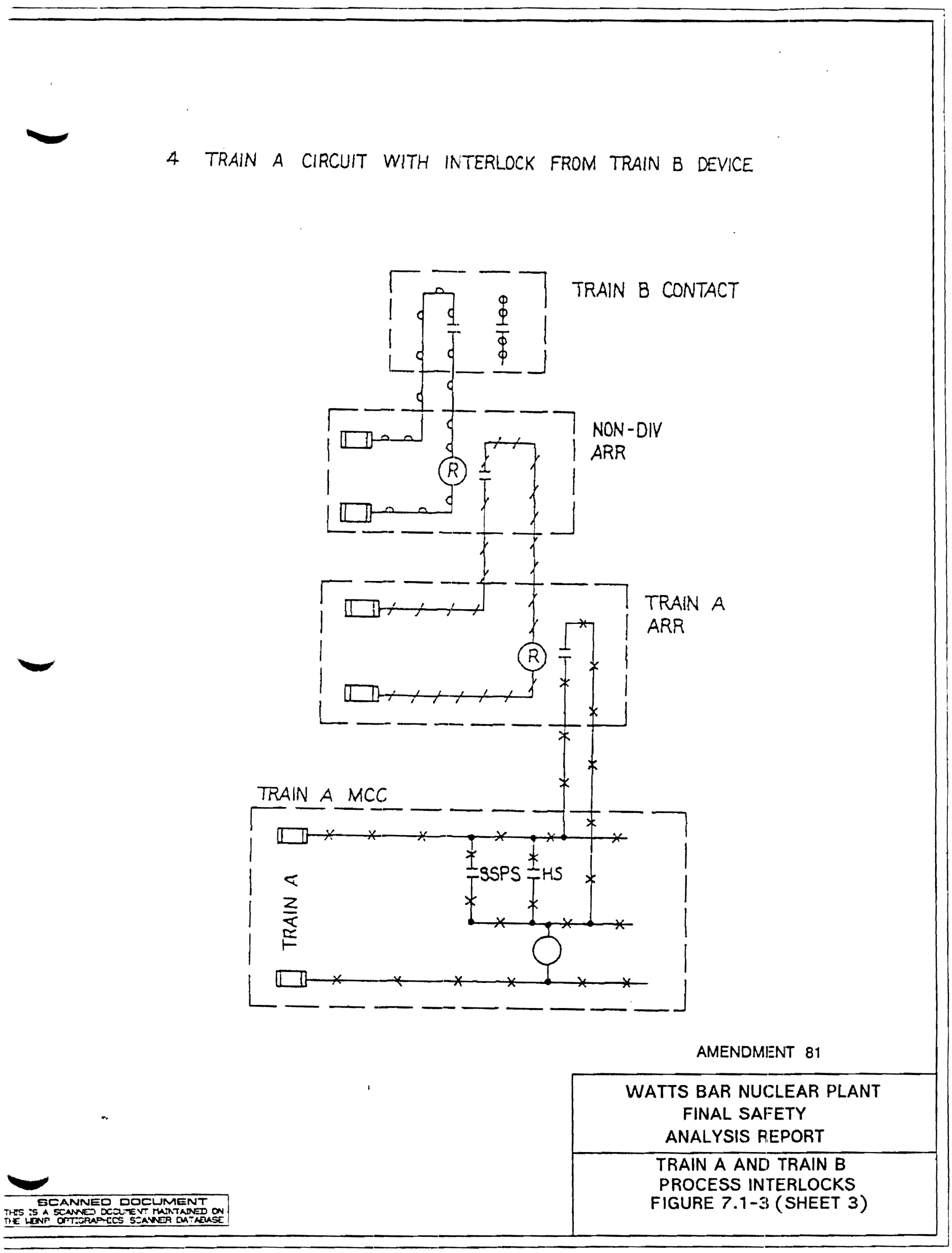
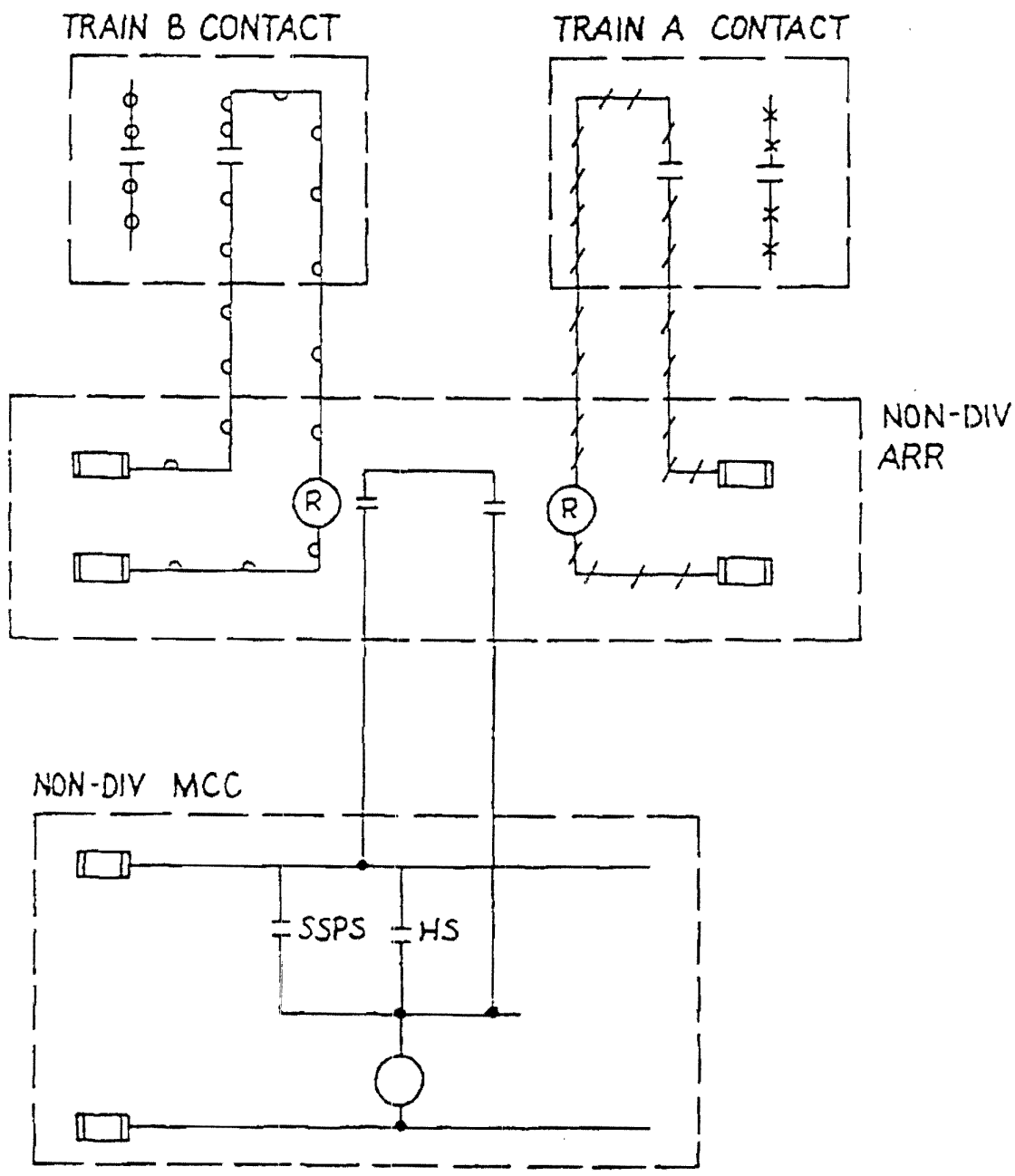


Figure 7.1-3-SH-3 Train A and Train B Process Interlocks

5 NON-DIVISIONAL CIRCUIT REQUIRING INTERLOCKS FROM BOTH TRAIN A AND B



AMENDMENT 81

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

TRAIN A AND TRAIN B
PROCESS INTERLOCKS
FIGURE 7.1-3 (SHEET 4)

SCANNED DOCUMENT
THIS IS A SCANNED DOCUMENT MAINTAINED ON THE WBNP OPTIGRAPHICS SCANNER DATABASE

Figure 7.1-3-SH-4 Train A and Train B Process Interlocks

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 exceeding the specified fuel design limit, gross damage to fuel cladding or loss of system integrity which could lead to release of radioactive fission products into the containment.

The following systems make up the reactor trip system:

(1) Process Protection and Control System [1] and [11]
(2) Nuclear Instrumentation System [2] and [15]
(3) Solid State Logic Protection System [3]
(4) Reactor Trip Switchgear
(5) Manual Actuation Circuit

The reactor trip system consists of two to four redundant sensors and associated process protection channels, which monitor various plant variables, and two redundant logic trains, which receive input protection actuation signals from the process protection channels to complete the logical decisions 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 ac power from the rod drive motor generator sets to the rod drive power cabinets, as shown on Figure 7.2-1, Sheet 1. Normally both the dc undervoltage trip coil and the shunt trip relay for each breaker are kept energized allowing power to be available at the rod control power supply cabinets. For reactor trip, a loss of dc voltage to the undervoltage coil releases the trip plunger and trips open the breaker and the shunt relay drops out causing the shunt trip coil to energize and also trip the breaker. When either of the trip breakers opens, power is interrupted to the rod drive power supply, and the control rods fall, by gravity, into the core. The rods cannot be withdrawn until the trip breakers are manually reset. The trip breakers cannot be reset until the abnormal condition which initiated the trip is corrected or no longer requires a

reactor trip. Bypass breakers BYA and BYB are provided to permit testing of the trip breakers, as discussed in Section 7.2.2.2.

7.2.1.1.1 Functional Performance Requirements

The reactor trip system automatically initiates reactor trip:

(1) Whenever necessary to prevent fuel damage for an anticipated operational transient (Condition II),

(2) To limit core damage for infrequent faults (Condition III),

(3) So that the energy generated in the core is compatible with the design provisions to protect the reactor coolant pressure boundary for limiting fault conditions (Condition IV).

The reactor trip system initiates a turbine trip signal whenever reactor trip is initiated to prevent the reactivity insertion that would otherwise result from excessive reactor system cooldown and to avoid unnecessary actuation of the engineered safety features actuation system.

The reactor trip system provides for manual initiation of reactor trip by operator action.

7.2.1.1.2 Reactor Trips

The various reactor trip circuits automatically open the reactor trip breakers whenever a condition monitored by the reactor trip system reaches a preset level. To ensure a reliable system, high quality design, components, manufacturing, quality control and testing are used. In addition to redundant channels and trains, the design approach provides a reactor trip system which monitors numerous system variables, therefore providing protection system functional diversity. The extent of this diversity has been evaluated for a wide variety of postulated accidents and is detailed in References [4] and [5].

Table 7.2-1 provides a list of reactor trips which are described below. Protection system interlocks are described in Table 7.2-2. The functional logic for reactor trips is shown on Figure 7.2-1.

(1) Nuclear Overpower Trips

The specific trip functions generated are as follows:

(a) Power range high neutron flux trip

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

There are two independent bistables, 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.

(b) Intermediate range high neutron flux trip

The intermediate range high neutron flux trip circuit trips the reactor when one out of the two intermediate range channels exceeds 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.

(c) Source range high neutron flux trip

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

(d) Power range high positive neutron flux rate trip

This circuit trips the reactor when a sudden abnormal increase in nuclear power occurs in two out of four power range channels. This trip provides DNB protection against rod ejection accidents of low worth from midpower and is always active.

(e) Power range high negative neutron flux rate trip

This circuit trips the reactor when a sudden abnormal decrease in nuclear power occurs in two out of four power range channels. This trip provides protection against two or more dropped rods and is always active. Protection against one dropped rod is not required to prevent occurrence of DNB per Section 15.2.3.

Figure 7.2-1, Sheet 2, shows the logic for all of the nuclear overpower and rate trips. Detailed functional descriptions of the equipment associated with these functions are given in References [2] and [15].

(2) Core Thermal Overpower Trips

The specific trip functions generated are as follows:

(a) Overtemperature ΔT trip

This trip protects the core against low DNBR and trips the reactor on two out of four coincidence with one set of temperature measurements per loop. The setpoint for this trip is continuously calculated by the Eagle-21 process protection circuitry for each loop by solving the following equation:

$$\text{OT}\Delta\text{T Stepoint}_i = \Delta T_i^{\circ}\left[K_1 - K_2\left(\frac{1+\tau_1 S}{1+\tau_2 S}\right)(T_{avg_i} - T^{\circ}_{avg_i}) + K_3(P - P^{\circ}) - f_1(\Delta I)\right]$$

An overtemperature ΔT reactor trip occurs when

$$\Delta T_i\left(\frac{1+\tau_4 S}{1+\tau_5 S}\right) > \text{OT}\Delta\text{T Stepoint}_i$$

where:

ΔT°_i = Indicated ΔT at Rated Thermal Power in loop i
(i = 1 to 4)

$K_1 \leq 1.0952$

$K_2 = 0.0133/°F$

τ_1, τ_2 = Time constants utilized in the lead-lag compensator for T_{avg}, τ_1 = 33 secs; τ_2 = 4 secs

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

T_{avgi} = Average Temperature of loop i (i = 1 to 4), °F

$T°_{avgi}$ = Nominal T_{avg} at Rated Thermal Power (Calibration temperature for ΔT instrumentation, ≤ 588.2°F)

$K_3 = 0.000647/psig$

P = Pressurizer Pressure, psig

P° = 2235 psig (Nominal RCS operating pressure)

$f_1(\Delta I)$ = is a function of the indicated difference between the top and bottom detectors of the power range neutron ion chambers. Gains are selected based on measured instrument response during plant startup tests such that:

(i) for $I_t - I_b$ between -32% and +10% $f_1(\Delta I) = 0$ (where I_t and I_b are % RATED THERMAL POWER in the top and bottom halves of the cores respectively and $I_t - I_b$ is the total THERMAL POWER in % of RATED THERMAL POWER)

(ii) for each % that the magnitude of $(I_t - I_b)$ is less than -32%, the ΔT trip setpoint is automatically reduced by 1.34% of its value at RATED THERMAL POWER

(iii) for each % that the magnitude of $(I_t - I_b)$ exceeds +10%, the ΔT trip setpoint is automatically reduced by 1.22% of its value at RATED THERMAL POWER

ΔT_i = Temperature delta between hot leg and cold leg in loop i (i = 1 to 4)

τ_4, τ_5 = Time constants utilized in the lead-lag compensator for measured ΔT.
τ_4 = 12 seconds
τ_5 = 3 seconds

Note: Additional information on associated tau values (τ_6 and τ_7) are provided in Section 7.2.1.1.4.

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

Increases in ΔI beyond a predefined deadband result in a decrease in trip setpoint. Refer to Figure 7.2-2.

The required one pressurizer pressure parameter per loop is obtained from separate sensors connected to three pressure taps at the top of the pressurizer. Four pressurizer pressure signals are obtained from the three taps by connecting one of the taps to two pressure transmitters. Refer to Section 7.1.2.2 for a discussion of independence of redundant sense lines.

The logic for this function is shown on Figure 7.2-1, Sheet 3. A detailed functional description of the process equipment associated with this function is contained in Reference [11].

(b) Overpower ΔT trip

This trip protects against excessive power (fuel rod rating protection) and trips the reactor on two out of four coincidence with one set of temperature measurements per loop. The setpoint for each channel is continuously calculated by the process protection circuitry using the following equation:

$$\text{OP}\Delta\text{T Stepoint}_i = \Delta T^\circ_i \left[K_4 - K_5 \left(\frac{\tau_3 S}{1 + \tau_3 S} \right) (T_{avg_i}) - K_6 (T_{avg_i} - T^\circ_{avg_i}) - f_2(\Delta I) \right]$$

An overpower ΔT reactor trip occurs when:

$$\Delta T_i \left[\frac{1 + \tau_4 S}{1 + \tau_5 S} \right] > \text{OP}\Delta\text{T Setpoint}_i$$

where: The following parameters have been defined in Section 7.2.1.1.2(2)(a) Overtemperature ΔT trip: ΔT°_i, T_{avg_i}, T°_i, ΔT_i, τ_4, τ_5, S

$K_4 \leq 1.091$

K_5 = 0.02/°F for increasing average temperature (T_{avg^i}) and 0 for decreasing average temperature (T_{avg^i})

K_6 = 0.00126/°F for $T_{avg^i} > T^\circ_{avg^i}$ and 0 for $T_{avg^i} \leq T^\circ_{avg\ i}$

τ_3 = Time constant used in lag compensator for T_{avg}, τ_3 = 5 sec

f_2 (ΔI) = 0 for all ΔI

Note: Additional information on associated tau values (τ_6 and τ_7) are provided in Section 7.2.1.1.4.

The source of temperature and flux information is identical to that of the overtemperature ΔT trip and the resultant overpower ΔT setpoint is compared to the same ΔT. The trip logic for this function is shown on Figure 7.2-1, Sheet 3. A detailed functional description of the process equipment associated with this function is contained in Reference [11].

(3) Reactor Coolant System Pressurizer Pressure and Water Level Trips

The specific trip functions generated are as follows:

(a) Pressurizer low pressure trip

The purpose of this trip is to protect against low pressure which could lead to DNB. The parameter being sensed is reactor coolant pressure as measured in the pressurizer. Above P-7 the reactor is tripped when two out of four pressurizer pressure measurements (compensated for rate of change) fall below preset limits. This trip is blocked below P-7 to permit startup. The trip logic and interlocks are given in Table 7.2-1.

The trip logic is shown on Figure 7.2-1, Sheet 2. A detailed functional description of the process equipment associated with the function is contained in References [5] and [11].

(b) Pressurizer High Pressure Trip

The purpose of this trip is to protect the reactor coolant system against system overpressure. The same sensors and transmitters used for the pressurizer low pressure trip are used for the high pressure trip except that separate comparators are used for trip. These comparators trip the reactor when two out of four uncompensated pressurizer pressure signals exceed preset limits 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 Figure 7.2-1, Sheet 2. The detailed functional description of the process equipment associated with this trip is provided in References [5] and [11].

(c) Pressurizer High Water Level Trip

This trip is provided as a backup to the high pressurizer pressure trip and serves to prevent water relief through the pressurizer safety valves. Above P-7, the reactor is tripped when two out of three pressurizer water level measurements exceed preset limits. 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 on Figure 7.2-1, Sheet 2. A detailed description of the process equipment associated with this function is contained in References [5] and [11].

(4) Reactor Coolant System Low Flow Trips

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

(a) Low Reactor Coolant Flow

The parameter sensed is reactor coolant flow. Four elbow taps in each coolant loop are used as flow devices that indicate the status of reactor coolant flow. The basic function of this device is to provide information as to whether or not a reduction in flow has occurred. An output signal from two out of the three comparators in a loop would indicate a low flow in that loop. Above P-8, low flow in one loop will trip the reactor. Between P-7 and P-8, low flow in two out of four loops will result in a reactor trip. This trip is blocked below P-7 to permit startup.

The coincidence logic and interlocks are given in Table 7.2-1. The logic for this trip is shown on Figure 7.2-1, Sheet 3. A detailed functional description of the process equipment associated with the trip function is contained in References [5] and [11].

(b) Reactor Coolant Pump Undervoltage Trip

This trip is required in order to protect against low flow which can result from loss of voltage to more than one reactor coolant pump motor (e.g., from plant loss of voltage or reactor coolant pump breakers opening). This trip is blocked below P-7 to permit startup.

There is one undervoltage sensing relay for each pump motor connected at the load side of each reactor coolant pump breaker. These relays provide an output signal when the pump voltage goes below approximately 70% of rated voltage. Signals from these relays are time delayed to prevent spurious trips

caused by short term voltage perturbations. The coincidence logic and interlocks are given in Table 7.2-1. The trip logic is shown on Figure 7.2-1, Sheet 3.

(c) Reactor Coolant Pump Underfrequency Trip

This trip provides protection against low reactor coolant flow resulting from bus underfrequency (e.g., power grid frequency transients). Above the P-7 interlock setpoint, an underfrequency condition on two out of four reactor coolant pump (RCP) motors will trip the reactor and open all of the RCP circuit breakers.

There is one underfrequency sensing relay connected to the load side of each RCP breaker with a setpoint of approximately 57 Hz. The signals from these relays are time delayed to prevent spurious trips caused by short-term frequency perturbations. The coincidence logic and interlocks are given in Table 7.2-1. The trip logic is shown on Figure 7.2-1, Sheet 3.

Westinghouse analysis of loss of flow accidents caused by power system frequency transients [Reference 6] has shown that the reactor is adequately protected by the underfrequency reactor trip for frequency of decay rates less than 6.8 Hz/sec without taking credit for the RCP breaker trip. A grid analysis of the TVA power system determined the maximum system frequency decay rate to be less than 5 Hz/sec. Consequently, the RCP breaker trip on underfrequency is not included in the protection system.

(5) Low-Low Steam Generator Water Level Trip (including Trip Time Delay)

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

The signals to actuate the reactor trip and start auxiliary feedwater pumps are delayed through the use of a Trip Time Delay (TTD) system for reactor power levels below 50% of RTP. Low-Low water level in any steam generator will generate a signal which starts an elapsed time trip delay timer. The allowable trip time delay is based upon the prevailing power level at the time the low-low level trip setpoint is reached and the number of steam generators that are affected. If power level rises after the trip time delay setpoints have been determined, the trip time delay is re-determined (i.e., decreased) according to the increase in power level.

At this point the timer will continue timing from the original timer initiation. However, the trip time delay setpoints are not increased if the power level

decreases after the TTD timer has started. The use of this delay allows added time for natural steam generator level stabilization or operator intervention to avoid an undesirable inadvertent protection system actuation.

There are no interlocks or permissives associated with this trip function. The logic for this protective function is shown on Figure 7.2-1, Sheet 4. A detailed functional description of the process equipment associated with this function is contained in References [11] and [14].

(6) Reactor Trip on a Turbine Trip

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

The reactor trip on turbine trip provides additional protection and conservatism beyond that required for the health and safety of the public. This trip is included as part of good engineering practice and prudent design. No credit is taken in any of the accident analyses (Chapter 15) for this trip.

Separate routing is maintained for the four turbine trip channel sets. Each of three sets includes the signal from low autostop oil pressure and the signal from closing of the steam stop valve. The fourth set consists of the signal from closing of the steam stop valve. The separation of these four channel sets is maintained from the sensors to the reactor protection system logic input cabinets. These channel routings meet the redundance and separation requirements identical to those for Class 1E circuits. Mounting and location is in non-seismic Category I structures.

The turbine provides anticipatory trips to the reactor protection system from contacts which change position when the turbine stop valves close or when the turbine autostop oil 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 closed 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 to cause reactor trip.

This design functions in a de-energize-to-trip fashion to cause a reactor 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 considerations 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.). The anticipatory trips thus meet the intent of

IEEE-279-1971, including redundancy, separation, single failure, etc. Seismic qualification of the contacts sensors is not required.

The logic for this trip is shown on Figure 7.2-1, Sheet 3.

(7) 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 heat sink.

Figure 7.2-1, Sheet 1, shows the logic for this trip. A detailed functional description of the process equipment associated with this trip function is provided in References [5] and [11].

(8) Manual Trip

The manual trip consists of two switches with two outputs on each switch. One output is used to actuate the train A reactor trip breaker, the other output actuates the train B reactor trip breaker. Operating a manual trip switch removes the voltage from the undervoltage trip coil and energizes the shunt trip coil.

There are no interlocks which can block this trip. Figure 7.2-1, Sheet 2, shows the manual trip logic.

7.2.1.1.3 Reactor Trip System Interlocks

(1) Power Escalation Permissives

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

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

The intermediate range 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 permissive P-10, thus ensuring automatic activation to more restrictive trip protection.

The development of permissives P-6 and P-10 is shown on Figure 7.2-1, Sheet 2. All of the permissives are digital; they are derived from analog signals in the nuclear power range and intermediate range channels.

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

(2) Blocks of Reactor Trips at Low Power

Interlock P-7 blocks a reactor trip below approximately 10% of full power on a low reactor coolant flow in more than one loop, reactor coolant pump undervoltage, reactor coolant pump underfrequency, pressurizer low pressure, or pressurizer high water level. See Figure 7.2-1, Sheets 2 and 3, for permissive applications. The low power signal is derived from three out of four power range neutron flux signals below the setpoint in coincidence with two out of two turbine impulse chamber pressure signals below the setpoint (low plant load). See Figure 7.2-1, Sheet 2, for the derivation of P-7.

The P-8 interlock blocks a reactor trip when the plant is below approximately 48% of full power, on a low reactor coolant flow in any one loop. The block action (absence of the P-8 interlock signal) occurs when three out of four neutron flux power range signals are below the setpoint. Thus, below the P-8 setpoint, the reactor will be allowed to operate with one inactive loop and trip will not occur until two loops are indicating low flow. See Figure 7.2-1, Sheet 3, for derivation of P-8 and applicable logic.

The P-9 interlock blocks a reactor trip on a turbine trip when the plant is below approximately 50% of full power. The block action (absence of the P-9 interlock signal) occurs when three out of four neutron flux power range signals are below the setpoint. Thus, below the P-9 setpoint, the reactor will not trip directly from a turbine-tripped signal but will allow the reactor control system, utilizing steam dump to the condenser as an artificial load, to bring the reactor to zero power. See Figure 7.2-1, Sheet 2, for derivation of P-9, and Sheet 3 for logic applications.

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

7.2.1.1.4 Reactor Coolant Temperature Sensor Arrangement and Calculational Methodology

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

The cold leg temperature measurement on each loop is accomplished with two narrow range RTDs mounted in thermowells. The cold leg sensors are inherently redundant in that either sensor can adequately represent the cold leg temperature measurement.

The hot leg temperature measurement on each loop is accomplished with three narrow range RTDs mounted in thermowells spaced 120 degrees apart around the circumference of the reactor coolant pipe for spatial variations.

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

The two cold leg temperature signals are subjected to range and consistency checks and then averaged to provide a group value for T cold.

A consistency check is performed on the T_{cold} input signals. If these signals agree within an acceptance interval (DELTAC), the group quality is set to GOOD. If the signals do not agree within the acceptance tolerance DELTAC, the group quality is set to BAD and the individual signal qualities are set to POOR. The average of the two signals is used to represent the group in either case. If an input signal is manually disabled or subject to a diagnosed hardware failure, the group is represented by the active signal. DELTAC is a fixed input parameter based on operating experience. One DELTAC value is required for each loop/protection set.

The following parameters are used in conjunction with the Overtemperature ΔT and Overpower ΔT reactor trips:

$T_{c_{ji}}$ = jth narrow range T_{cold} input signal from loop i

$T^f_{c_{ji}}$ = Filtered T_{cold} signal for the jth RTD; = $T_{cji}(1/(1 + \tau_7 s))$

where:

j = 1, 2 and i = 1 to 4

τ_7 = Time constant utilized in the lag compensator for T_{cold}. Typically set to 0.0 sec.

$T^f_{c_{ave_i}}$ = Group average of the valid input signals

= $(T^f_{c_{(j-1)_i}} + T^f_{c_{ji}})/2$ for two valid input signals (j=2)

= $T^f_{c_{ji}}$ for one valid input signal (j=l)

where:

i = 1 to 4

S is defined in Section 7.2.1.1.2

Each of the three hot leg temperature signals is subjected to a range check, and utilized to calculate an estimated average hot leg temperature which is consistency checked against the other two estimates for average hot leg temperature.

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

If the signal values do not all agree within ±DELTAH of the average, the algorithm will delete the signal value which is furthest from the average. The quality of this signal will be set to POOR and a consistency check will then be performed on the remaining GOOD signals. If these signals pass the consistency check, the group value will be taken as the average of these GOOD signals and the group quality will be set to POOR. However, if these signals again fail the consistency check (within ±DELTAH), then the group value will be set to the average of these two signals; but the group quality will be set to BAD. All of the individual signals will have their quality set to POOR. If one or two input signals is manually disabled or subject to a diagnosed hardware failure, the group value is based on the unaffected signal(s). DELTAH is a fixed input parameter based on temperature distribution tests with the hot leg and operating experience. One DELTAH value is required for each loop/protection set.

The following parameters are used in conjunction with the Overtemperature ΔT and Overpower ΔT reactor trips:

T_{hji} = jth narrow range T_{hot} input signal from loop i

T^f_{hji} = Filtered T_{hot} signal for the jth RTD; = $T_{hji}\ (1/(1 + \tau_6 s))$

where:

j = 1 to 3 and i = 1 to 4

τ_6 = Time constant utilized in the lag compensator for T_{hot}. Typically set to 0.0 sec

$T^f_{h\ ave\ i}$ = Group average of the valid input signals

= $(T^f_{h(j-2)i} + T^f_{h(j-1)i} + T^f_{hji})/3$ for three valid input signals (j=3)

= $(T^f_{h(j-1)i} + T^f_{hji})/2$ for two valid input signals (j=2)

= T^f_{hji} for one valid input signal (j=1)

where: i = 1 to 4

The estimated average hot leg temperature is derived from each T hot input signal as follows:

$\bar{T}_{h_{ji}} = T^{f}_{h_{ji}} - P_{B_1} S^{\circ}_{ji}$ = estimated T_{hot} average

where:

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

$$P_{B_i} = \left(\frac{T^{f}_{h_{ave_i}} - T^{f}_{c_{ave_i}}}{\Delta T^{\circ}_{i}} \right)$$

ΔT°_{i} is defined in the equation for Overtemperature Delta-T trip in Section 7.2.1.1.2, subsections 2 and 3.

S°_{ji} = manually input bias which corrects the individual T hot RTD value to the loop average.

ΔT and T_{avg} are calculated as follows:

$$\Delta T_i = T^{f}_{h_{ave_i}} - T^{f}_{c_{ave_i}}$$

$$T_{avg_i} = \frac{(T^{f}_{h_{ave_i}} + T^{f}_{c_{ave_i}})}{2.0}$$

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

7.2.1.1.5 Pressurizer Water Level Reference Leg Arrangement

The design of the pressurizer water level instrumentation includes a slight modification of the usual tank level arrangement using differential pressure between an upper and a lower tap. The modification consists of the use of a sealed reference leg instead of the conventional open column of water. Refer to Section 7.2.2.3.4 for an analysis of this arrangement.

7.2.1.1.6 Process Protection System

The process protection instrumentation system is described in References [1] and [11]. The nuclear instrument system is described in References [2] and [15]. Reference [2] is applicable to the power range only.

7.2.1.1.7 Solid State Logic Protection System

The solid state logic protection system takes binary inputs from the process protection and nuclear instrument channels and other plant equipment corresponding to conditions (normal/abnormal) of plant parameters. The system combines these signals in the required logic combination and generates a trip signal (no voltage) to the undervoltage coils and the shunt trip relays (which energize the shunt trip coils) of the reactor trip circuit breakers when the necessary combination of signals occurs. The system also provides annunciator, status light and computer input signals which indicate the condition of comparator 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. A detailed description of this system is given in Reference [3].

7.2.1.1.8 Isolation Devices

In certain applications, control signals and other non-protective functions are derived from individual protection channels through isolation devices contained in the protection channel, as permitted by IEEE Standard 279-1971. The isolation devices are part of the protection system and are located in the process protection racks. By definition, non-protective functions include those signals used for control, remote process indication, and computer monitoring.

Isolation device qualification type tests are described in References [7], [8], and [11].

7.2.1.1.9 Energy Supply and Environmental Variations

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

As documented in Reference [7], testing was performed on the Eagle 21 Process Protection System to demonstrate that the Eagle 21 system remained operational before, during and after applied noise, fault, surge withstand, electro-magnetic interference (EMI) and Radio Frequency Interference (RFI) operating conditions. Objectives accomplished by the test demonstrated that the physical independence of

the non-class 1E and Class 1E circuitry was maintained and that the system was designed to withstand worst-case noise environment conditions.

7.2.1.1.10 Setpoints

The setpoints that require trip action are given in the Technical Specifications.

7.2.1.1.11 Seismic Design

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

7.2.1.2 Design Bases Information

The information given below presents the design bases information requested by Section 3 of IEEE Standard 279-1971, Reference [9]. The reactor trip logic is presented in Figure 7.2-1, Sheets 1 through 4.

7.2.1.2.1 Generating Station Conditions

The following are the generating station conditions requiring reactor trip.

(1) DNBR approaching the limiting value.

(2) Power density (kilowatts per foot) approaching rated value for Condition II events (See Chapter 4 for fuel design limits).

(3) Reactor coolant system overpressure creating stresses approaching the limits specified in Chapter 5.

7.2.1.2.2 Generating Station Variables

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

(1) Neutron flux

(2) Reactor coolant temperature

(3) Reactor coolant system pressure (pressurizer pressure)

(4) Pressurizer water level

(5) Reactor coolant flow

(6) Reactor coolant pump bus voltage and frequency

(7) Steam generator water level

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

7.2.1.2.3 Spatially Dependent Variables

Reactor coolant temperature is a spatially dependent variable. See Section 7.3.1.2.3 for a discussion.

7.2.1.2.4 Limits, Margins and Levels

The parameter values that will require reactor trip are given in the Technical Specifications and in Chapter 15, Accident Analyses. Chapter 15 demonstrates 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 clad damage and loss of integrity of the reactor coolant system as a result of any ANS Condition II incident. As such, during any ANS Condition II incident, the reactor trip system limits the following parameters to:

(1) Minimum DNBR - limiting value.

(2) Maximum system pressure = 2750 psia

(3) Fuel rod maximum linear power - maximum rated power

The accident analyses described in Section 15.2 demonstrate that the functional requirements as specified for the reactor trip system are adequate to meet the above considerations, even assuming, for conservatism, adverse combinations of instrument errors (Refer to Table 15.1-3). A discussion of the safety limits associated with the reactor core and reactor coolant system, plus the limiting safety system setpoints, are presented in the Technical Specifications. The Technical Specifications incorporate both nominal and limiting setpoints. Nominal settings of the setpoints are more conservative than the limiting settings. This allows for calibration uncertainty and instrument channel drift without violating the limiting setpoint. Automatic initiation of protective functions occurs at the nominal setpoints (plus or minus the allowed tolerances). The methodology used to derive the setpoints is documented in Reference [13] and [16]. A further discussion on trip setpoints is given in Section 7.2.2.1.1.

7.2.1.2.5 Abnormal Events

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

(1) Earthquakes (see Sections 2.5 and 3.7).

(2) Fire (see Section 9.5)

(3) Explosion (hydrogen buildup inside containment) (see Section 6.2).

(4) Missiles (see Section 3.5).

(5) Flood (see Sections 2.4 and 3.4).

(6) 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 provides protection against destruction of the system from fires, explosions, floods, wind, and tornadoes (see each item above). The discussions in Section 7.1.2.1.7 and this section adequately address or reference the Safety Analysis Report coverage of the effects of abnormal events on the reactor trip system in conformance with applicable General Design Criteria.

7.2.1.2.6 Minimum Performance Requirements

(1) Reactor Trip System Response Time

Reactor trip system response time is defined in Section 7.1. The maximum allowable time delays in generating the reactor trip signal are provided in the Technical Requirements Manual. These values are verified in accordance with the Technical Specifications and are consistent with the safety analyses. See Table 7.1-1 Note 1 for a discussion of periodic response time verification capabilities.

(2) Reactor Trip Accuracies

Accuracy is defined in Section 7.1. Reactor trip accuracies are given in Reference [13].

(3) Protection System Ranges

Typical Protection System ranges are tabulated in Table 7.2-3.

7.2.1.3 Final Systems Drawings

Functional block diagrams, electrical elementaries and other drawings required to assure electrical separation and perform a safety review are provided in Table 1.7-1.

7.2.2 Analyses

A reliability study for the reactor trip and engineered safety features function of the Eagle 21 process protection system hardware has been performed. The basis for this study was to compare the availability of the Eagle 21 digital system with the existing implementation of the same function using analog hardware. Availability is defined as the probability that a system will perform its intended function (e.g., actuate a partial trip) at a randomly selected instant in time. Results of the availability study determined that the Eagle 21 digital system is commensurate with an equivalent analog process protection system availability although no credit was given to the Eagle 21 process protection features of automatic surveillance testing, self calibration and self diagnostics when the study was performed. It is expected that if credit were given to the Eagle 21 self diagnostic features (EPSOM checksums, RAM checks, Math Co-Processor checks and Loop Cycle Time checks), automatic surveillance testing and self calibration capabilities, system availability would be improved. Therefore, the

impact on the system operation due to channel drift being corrected by the Eagle 21 self-calibration feature and the impact on system downtime because of the automatic surveillance/self-diagnostic features, will be minimized. Additionally, with the MMI test unit provided with the Eagle 21 system, the amount of technician and engineering time required for maintenance and troubleshooting will be minimized. Thus, large quantities of engineering time required for the review of the quarterly functional tests, prior to restoring the channel to an operable condition, is eliminated because of the user-friendly printout provided from the MMI. In total, interface with the Eagle 21 process protection system will be reduced, resulting in a decreased potential for technician induced error which results in improved system reliability and availability.

In the Eagle 21 process protection system design, there are failure modes which could result in the failure of an entire protection rack. During these conditions, the rack will fail to the preferred failure mode (tripped/not tripped condition) providing maximum protection for the plant. The failure of a single rack is considered to be bounded by the loss of an entire protection set, which is the existing licensing basis. This failure has been shown not to adversely impact plant safety due to the existence of redundancy, functional diversity and defense-in-depth design measures employed in the design of the process protection system. Use of these design measures ensures that in the event of a single failure, the remaining protection system channels would be available for plant protection if required. Additional discussion of the defense-in-depth, redundancy and functional diversity design measures used in the design of the Eagle 21 process protection system can be found in References [5] and [14].

A failure mode and effects analysis (FMEA) of the logic portion of the reactor trip system has been performed. The basis of the FMEA is that the reactor protection system is designed to sense abnormal plant conditions and to initiate action necessary to assure that acceptable fuel design limits are not exceeded for anticipated operational occurrences. Results of this study and a fault tree analysis are presented in Reference [4]. The results of the study show that the probability of protection system failure in anticipated transients is sufficiently low that no provision need be made in plant design to accommodate such hypothetical failure.

7.2.2.1 Evaluation of Design Limits

While most setpoints used in the reactor protection system are fixed, there are variable setpoints, most notably the overtemperature ΔT and overpower ΔT. All setpoints in the reactor trip system have been selected on the basis of engineering design or safety studies. The capability of the reactor trip system to prevent loss of integrity of the fuel cladding and/or reactor coolant system pressure boundary during Condition II and III transients is demonstrated in Chapter 15. These accident analyses are carried out using those setpoints determined from results of the engineering design studies. Setpoint limits are presented in the Technical Specifications. A discussion of the intent for each of the various reactor trips and the accident analyses (where appropriate) which utilize this trip is presented below. The selection of trip setpoints provides for margin before protection action is actually required to allow for uncertainties and instrument errors (Reference 13). The design meets the requirements of Criteria 10, 15, 20, and 29 of the 1971 GDC.

7.2.2.1.1 Trip Setpoint Discussion

It has been pointed out previously that below the limiting value of DNBR there is likely to be significant local fuel cladding failure. The DNBR existing at any point in the core for a given core design can be determined as a function of the core inlet temperature, power output, reactor coolant operating pressure and flow. Consequently, core safety limits in terms of the limiting value of DNBR for the hot channel can be developed as a function of core ΔT, T_{avg}, and pressure for a specified flow as illustrated by the dashed lines in Figure 15.1-1. Shown as solid lines in Figure 15.1-1 are the loci of conditions equivalent to 118% of power as a function of ΔT and T_{avg} representing the overpower (KW/ft) limit on the fuel. The solid lines indicate the maximum permissible setpoints (ΔT) as a function of T_{avg} and pressure for the overtemperature and overpower reactor trips. Actual setpoint constants in the equation representing the solid lines are as given in the Technical Specifications. These values are conservative to allow for instrument errors. The design meets the requirements of Criteria 10, 15, 20 and 29 of the 1971 GDC.

DNBR is not a directly measurable quantity; however, the process variables that determine DNBR are sensed and evaluated. Small isolated changes in various process variables may not individually result in violation of a core safety limit, whereas the combined variations, over sufficient time, may cause the overpower or 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 ΔT trips provide sufficient protection for slow transients as opposed to such trips as low flow or high flux which will trip the reactor for rapid changes in flow or flux, respectively, that would result in fuel damage before actuation of the slower responding ΔT trips could be effected.

Therefore, the reactor trip system has been designed to provide protection for fuel cladding and reactor coolant system pressure boundary integrity where: 1) a rapid change in a single variable or factor which will quickly result in exceeding a core or a system safety limit, and 2) a slow change in one or more variables will have an integrated effect which will cause safety limits to be exceeded. Overall, the reactor trip system offers diverse and comprehensive protection against fuel cladding failure and/or loss of reactor coolant system integrity for Condition II and III accidents. This is demonstrated by Table 7.2-4 which lists the various trips of the reactor trip system, the corresponding technical specification on safety limits and safety system settings and the appropriate accident discussed in the safety analyses in which the trip could be utilized.

The plant is prohibited by Technical Specifications from operating with an inactive loop for extended periods of time, and administrative procedures require that the unit be brought to a load of less than 25% of full power prior to starting the pump in the inactive

loop in order to bring the inactive loop hot leg temperature closer to the core inlet temperature.

However, it should be noted that the reactor trip system automatically provides core protection during this non-standard operating configuration, i.e., no protection system setpoints need to be reset. This is because the nominal value of the power (P-8) interlock setpoint restricts the power levels such that DNB ratios below the design basis limit will not be realized during any Condition II transients occurring during this mode of operation. This restricted power level is considerably below the boundary of permissible values for 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.

The reactor trip system design was evaluated in detail with respect to common mode failure and is presented in References [4] and [5]. 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 confirmation of the system design.

Analyses of the results of Condition II, III and IV events, including considerations of instrumentation installed to mitigate their consequences, are presented in Chapter 15. The instrumentation installed to mitigate the consequences of load rejection and turbine trip is given in Section 7.4.

7.2.2.1.2 Reactor Coolant Flow Measurement

The elbow taps used on each loop in the primary coolant system are instrument devices that are used to indicate reactor coolant flow. The basic function of this measurement is to ensure that thermal design flow is achieved. The correlation between flow and elbow tap signal is given by the following equation:

$$\frac{\Delta P}{\Delta P_0} = \left(\frac{w}{w_0}\right)^2,$$

where ΔP_O is the pressure differential at the reference flow w_o, and ΔP is the pressure differential at the corresponding flow, w. The full flow reference point is established during initial plant startup. The low flow trip point is then established by extrapolating along the correlation curve. The expected absolute accuracy of the channel is within $\pm$10% of full flow and field results have shown the repeatability of the trip point to be within $\pm$1%.

7.2.2.2 Evaluation of Compliance to Applicable Codes and Standards

The reactor trip system meets the requirements of the General Design Criteria as indicated. The reactor trip system meets the requirements of Section 4 of IEEE Standard 279-1971[9] as indicated below.

(1) General Functional Requirement

The protection system automatically initiates appropriate protective action whenever a condition monitored by the system reaches a preset value. Functional performance requirements are given in Section 7.2.1.1.1. Section 7.2.1.2.4 presents a discussion of limits, margins and setpoints; Section 7.2.1.2.5 discusses unusual (abnormal) events; and Section 7.2.1.2.6 presents minimum performance requirements.

(2) Single Failure Criterion

The protection system is designed to provide two, three, or four redundant process protection 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 system action 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 Criteria 21, 22 and 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] and [5]. The design meets the requirements of Criteria 21 and 22 of the 1971 GDC.

(3) Quality of Components and Modules

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

(4) Equipment Qualification

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

(5) Channel Integrity

Protection system channels required to operate in accident conditions maintain necessary functional capability under extremes of conditions relating to environment, energy supply, malfunctions, and accidents. The energy supply for the reactor trip system is described in Chapter 8. The

environmental variations, throughout which the system will perform is given in Section 3.11. The design meets the requirements of Criteria 21 and 22 of the 1971 GDC.

(6) Independence

Channel independence is carried throughout the system, extending from the sensor through 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 protection channels are separated by locating the processing electronics of the redundant channels in different protection rack sets. Each redundant protection channel set is energized from a separate AC power feed. This design meets the requirements of Criteria 21 and 22 of the 1971 GDC.

Independence of the logic trains is discussed in Reference[3]. 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 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. The extent of this diversity has been evaluated for a wide variety of postulated accidents and is discussed in Reference [5]. Generally, two or more diverse protection functions would terminate an accident before intolerable consequences could occur. This design meets the requirements of Criterion 22 of the 1971 GDC.

(7) Control and Protection System Interaction

The protection system is designed to be independent of the control system. In certain applications the control signals and other non-protective functions are derived from individual protective channels through isolation devices. The isolation devices are classified as part of the protection system and are located in the process protection racks. Non-protective functions include those signals used for control, remote process indication, and computer monitoring. The isolation devices are designed such that a short circuit, open circuit, or the application of credible fault voltages on the isolated output portion of the circuit (i.e., the non-protective side of the circuit) will not affect the input (protective) side of the circuit. The signals obtained through the isolation devices are never returned to the process protection racks. This design meets the requirements of Criterion 24 of the 1971 GDC and paragraph 4.7 of IEEE Standard 279-1971[9].

Specific control and protection system interactions are discussed in Section 7.2.2.3.

A detailed discussion of the design and testing of the protection system isolation devices is given in References [7], [8], and [11]. These reports include the results of applying various malfunction conditions on the output portion of the isolation devices. The results show that no significant disturbance to the isolation devices' input signal occurred.

Where failure of a protection system component can cause a process excursion which requires protective action, the protection system can withstand another, independent failure without loss of protective action. This is normally achieved by means of two-out-of-four (2/4) trip logic for each of the protective functions except Steam Generator Protection. The Steam Generator Low Water Level protective function relies upon two-out-of-three (2/3) trip logic and a control system Median Signal Selector (MSS). The use of a control system MSS prevents any protection system failure from causing a control system reaction resulting in a need for subsequent protective action. This meets the requirements of Criterion 24 of the 1971 GDC. A detailed discussion of the function of the MSS relative to control and protection system interaction is contained in References [12] and [14].

(8) Derivation of System Inputs

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

(9) Capability for Sensor Checks

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

(10) Capability for Testing

The reactor trip system is capable of being tested during power operation. Where only parts of the system are tested at any one time, the testing sequence provides the necessary overlap between the parts to assure complete system operation. The testing capabilities are in conformance with Regulatory Guide 1.22 as discussed in Table 7.1-1.

The protection system is designed to permit periodic testing of the signal processing portion of the reactor trip system during reactor power operation without initiating a protective action unless a trip condition actually exists. This is because of the coincidence logic required for reactor trip. Source and intermediate range high neutron flux trips must be bypassed during testing. These tests may be performed at any plant power from cold shutdown to full

power. Before starting any of these tests with the plant at power, all redundant reactor trip channels associated with the function to be tested must be in the normal (untripped) mode in order to avoid spurious trips. Setpoints are documented in Reference [13] and incorporated into the Technical Specifications.

The Protection System is also designed to permit periodic response time testing of the reactor trip system, excluding neutron detectors.

Process Protection Channel Tests

The Eagle 21 process protection system accommodates automatic or manual surveillance testing of the digital process protection racks via a portable Man Machine Interface (MMI) test cart. The MMI test cart is connected to the process rack by inserting a cable/connector assembly into the process rack test panel. The rack installed test processor permits performance of operations such as channel calibration, channel response time tests, partial trip actuation tests, and maintenance activities.

Administrative controls and multiple levels of security are provided to limit access to setpoint and tuning constant adjustments. The system is designed to permit testing of any protection channel during power operations without initiating a protective action at the systems level.

Individual channels can be tested in either the "Channel Trip" or "Bypass" mode:

The Channel Trip mode interrupts the individual channel comparator output. Interruption of a comparator output in this mode for any reason (test, maintenance purposes or removed from service) causes that portion of the logic to be actuated and initiates a channel trip alarm and status light in the control room. Status lights on the process rack test panel indicate when the associated comparators have tripped.

The Bypass mode disables the individual channel comparator trip circuitry. Interruption of a comparator output in this mode effectively "bypasses" the channel in test causing the associated logic relays to remain in the non-tripped state until the "bypass" is removed. This feature of the protection system eliminates the potential for an unwarranted actuation in the event of a failure. This condition is also accompanied by an alarm in the control room.

Nuclear Instrumentation Channel Tests

The power range channels of the nuclear instrumentation system are tested by using the actual detector input to the channel and injecting test currents obtained from the detector response curves at various power levels. The output of the bistable is not placed in a tripped condition prior to testing. Also, since the power range channel logic is two out of four, bypass of this reactor trip function is not required.

Testing of a power range channel requires deliberate operator action and is annunciated in the control room. Bistable operation is tested by increasing the test signal up to its trip setpoint and verifying bistable relay operation by control board annunciator and trip status lights.

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

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

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

(a) Testing at plant shutdown

(1) Source range testing

(2) Intermediate range testing

(3) Power range testing

(b) Testing between P-6 and P-10 permissive power levels

(1) Intermediate range testing

(2) Power range testing

(c) Testing above P-10 permissive power level

(1) Power range testing

For a detailed description of the nuclear instrumentation system see References [2] and [15]. Reference [2] is applicable to the power range only.

Solid State Logic Testing

The logic trains of the reactor trip system are designed to be capable of complete testing at power. Logic matrices are tested from the Train A and Train B logic rack test panels. During this test, the logic inputs are actuated automatically in all combinations of trip and non-trip logic. Trip logic is not maintained sufficiently long enough to permit opening of the reactor trip breakers. The reactor trip undervoltage coils are 'pulsed' in order to check continuity. During logic testing of one train, the other train can initiate any required protective functions. Annunciation is provided in the control room to indicate when a train is in test (train output bypassed) and when a reactor trip breaker is bypassed. Details of the logic system testing are given in Reference [3].

A direct reactor trip resulting from undervoltage or underfrequency on the pump side of the reactor coolant pump breakers is provided as discussed in Section 7.2.1 and shown on Figure 7.2-1. 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 IEEE Standard 338-1971[10] as discussed in Table 7.1-1. Details of the method of testing and compliance with these standards are provided in References [l], [3], and [11].

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 Standards 279-1971 and 338-1971 as discussed in Table 7.1-1.

Testability of the interlocks associated with reactor trips for which credit is taken in the accident analyses is provided by the logic testing and semi-automatic testing capabilities of the solid state protection system. In the solid state protection system the undervoltage coils (reactor trip) and master relays (engineered safeguards actuation) are pulsed for all combinations of trip or actuation logic with and without the interlock signals. 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 protection system and nuclear instrumentation system channels, each channel comparator/bistable is placed in a trip mode causing one SSPS input relay in train A and one in train B to de-energize except when individual channels are tested in bypass with the reactor at power. 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, one of which (either train) normally remains in the A + B position. The A + B position allows information to be transmitted alternately from each train to the control board. During testing a steady status lamp indicates that both trains are receiving a trip mode logic input for the channel being tested. A flashing lamp indicates a failure in one train. 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 comparator/bistable input relays.

Actuation of the SSPS input relays provides the overlap between the testing of the logic protection system and the testing of those systems supplying the

inputs to the logic protection system. These test are performed periodically in accordance with the Technical Specifications. Test indications are status lamps and annunciators on the control board. Inputs to the logic protection system are checked one channel at a time, leaving the other channels in service. For example, a function that trips the reactor when two out of four channels trip becomes a one out of three trip when one channel is placed in the trip mode. Both trains of the logic protection system remain in service during this portion of the test.

(2) Check of logic matrices

Logic matrices are checked one train at a time. Input relays are not operated during this test. Partial reactor trips to the train being tested are inhibited with the use of the input error inhibit switch on the semi-automatic test panel in the train. Details of semi-automatic tester operation are given in Reference [3]. At the completion of the logic matrix tests, closure of the input error inhibit switch contacts is checked using an appropriate test method (verification of existing trip status lamps/computer points, or trip of one comparator/bistable for the appropriate protection system channel).

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

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

The general design features and details of the testability of the logic system are described in Reference [3]. 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. Each of the reactor trip breakers is tested with the corresponding bypass breaker in service.

Auxiliary contacts of the bypass breakers are connected into the SSPS General Warning Alarm System of their respective trains such that if either train is placed in test

while the bypass breaker of the other train is closed, both reactor trip breakers and both bypass breakers will automatically trip.

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

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

The complete reactor trip system is normally required to be in service. However, to permit online testing of the various protection channels or to permit continued operation in the event of a subsystem instrumentation channel failure, the Technical Specifications define the minimum number of operable channels. The Technical Specifications also define the required restriction to operation in the event that the channel operability requirements cannot be met.

(11) Channel Bypass or Removal from Operation

The Eagle 21 Process Protection System is designed to permit any channel to be maintained in a bypassed condition and, when required, tested during power operation without initiating a protective action at the systems level. This is accomplished without lifting electrical leads or installing temporary jumpers. If a channel in an Eagle 21 protection system rack has been bypassed for any purpose, a signal (1 per protection set) is provided to allow this condition to be continuously indicated in the control room. In addition, the Eagle 21 design has provided for administrative controls and multiple levels of security for bypassing a protection channel.

The channel bypass feature of the Eagle 21 system will be used for the following purposes:

(1) To allow for an inoperable Reactor Trip (RT) or Engineered Safety Features Actuation System (ESFAS) channel to be maintained in a bypassed condition up to six hours for the purpose of troubleshooting.

(2) To allow for a failed RT or ESFAS channel to be bypassed up to four hours for the purpose of surveillance testing a redundant channel of the same function.

(3) To routinely allow testing of a RT or ESFAS channel in the bypassed condition instead of the tripped condition for the purpose of surveillance testing.

The Nuclear Instrumentation System (NIS) is designed to permit routine periodic testing of the Source Range and Intermediate Range portion of the reactor trip system during reactor power operation. To enable testing of the one-out-of-two channel logic for the NIS Source Range and Intermediate Range during reactor power operation, a channel bypass feature has been provided. Use of this feature will permit routine required surveillance testing to be completed without initiating a protective action unless a trip condition exists.

(12) Operating Bypasses

Where operating requirements necessitate automatic or manual bypass of a protective function, the design of the protection system 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 protection 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. Bypasses associated with the reactor trip system are identified in Table 7.2-2.

(13) Indication of Bypasses

Bypass of a process protection channel during testing is indicated by an alarm in the control room. This is discussed further in Section 7.2.2.2, subsections 10 and 11.

(14) Access to Means for Bypassing

The design provides for administrative control of access to the means for manually bypassing channels or protective functions. For details, refer to References [1] and [11].

(15) 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 assure 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.

(16) Completion of Protective Action

The protection system is so designed that, once initiated, a protective action goes to completion. Normal operation is restored in accordance with established procedures.

(17) Manual Initiation

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

(18) Access to Setpoint Adjustments, Calibration and Test Points

The design provides for administrative control of access to all setpoint adjustments, processing electronics calibration adjustments, and test points. For details refer to References [1], [2], [11] and [15].

(19) Identification of Protective Actions

Indication and identification of protective actions is discussed in Item 20 below.

(20) Information Read Out

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

Any reactor trip will actuate an alarm and an annunciator. Such protective actions are indicated and identified by the parameter being measured.

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

(21) System Repair

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

(22) Identification

Identification of protection system equipment is discussed in Section 7.1.2.3.

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 (high flux) 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 Reactor Coolant Temperature

The accuracy of the narrow range resistance temperature detector loop temperature measurements is demonstrated during plant startup tests and periodically with surveillance tests. Testing compares temperature measurements from the narrow range resistance temperature detectors with one another as well as with the temperature measurements obtained from the wide range resistance temperature detectors located in the hot leg and cold leg piping of each loop. The comparisons are done with the reactor coolant system in an isothermal condition. During plant startup tests, ΔT measurements obtained from the hot leg and cold leg narrow range loop resistance temperature detectors are compared to plant power, and if required normalized to plant power. The absolute value of ΔT versus plant power is not important, per se, as far as reactor protection is concerned. Reactor trip system setpoints are based upon percentages of the indicated ΔT at nominal full power rather than on absolute values of ΔT. This is done to account for loop differences which are inherent. Therefore the percent ΔT scheme is relative, not absolute, and thus provides better protective action without the expense of accuracy. As part of the plant startup tests, the narrow range resistance temperature detector signals will be compared with the core exit thermocouple signals.

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

Since control is based on the highest of the loop average temperatures, 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 ΔT channels indicate an overtemperature or overpower condition.

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

7.2.2.3.3 Pressurizer Pressure

The pressurizer pressure protection channel signals are used for high and low pressure protection and as inputs to the overtemperature ΔT trip protection function. Isolated output signals from these channels are used for pressure control. These are used to control pressurizer spray and heaters and power operated relief valves. A coincident high pressure signal from two independent channels is needed for the actuation of each pressurizer PORV.

A spurious high pressure signal from one channel can cause decreasing pressure by turning off the heaters and actuation of spray. Additional redundancy is provided in the low pressurizer pressure reactor trip logic 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.

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.

Experience has shown that hydrogen gas can accumulate in the upper part of the condensate pot on conventional open reference leg systems in pressurizer water level service. At RCS operating pressures, high concentrations of dissolved hydrogen in the reference leg water are possible. On sudden depressurization accidents, it has been

hypothesized that rapid effervescence of the dissolved hydrogen could blow water out of the reference leg and cause a large level error, measuring higher than actual level. To eliminate the possibility of such effects, a bellows is used in a pot at the top of the reference leg to provide an interface seal and prevent dissolving of hydrogen gas into the reference leg water.

The reference leg is uninsulated and will remain at local ambient temperature. This temperature will vary somewhat over the length of the reference leg piping under normal operating conditions but will not exceed 140°F. During a blowdown accident, any reference leg water flashing to steam will be confined to the condensate steam interface in the condensate pot at the top of the temperature barrier leg and will have only a small (about one inch) effect on measured level. Some additional error may be expected due to effervescence of hydrogen in the temperature barrier water. However, even if complete loss of this water is assumed, the error will be small and can be tolerated.

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

Calibration of the sealed reference leg system is done in place after installation by application of known pressure to the low pressure side of the transmitter and measurement of the transmitter output. The effects of static pressure variations are predictable. The largest effect is due to the density change in the saturated fluid in the pressurizer itself. The effect is typical of level measurements in all tanks with two phase fluid and is not peculiar to the sealed reference leg technique. In the sealed reference leg, there is a slight compression of the fill water with increasing pressure, but this is taken up by the flexible bellows. A leak of the fill water in the sealed reference leg can be detected by comparison of redundant channel readings on line and by physical inspection of the reference leg off line. Leaks of the reference leg to atmosphere will be immediately detectable by off scale indications and alarms on the control board. A closed pressurizer level instrument shut off valve would be detected by comparing the level indications from the redundant level channels (three channels). In addition, there are alarms on one of the three channels to indicate an error between the measured pressurizer water level and the programmed pressurizer water level. There is no single instrument valve which could affect more than one of the three level channels.

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 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

The basic function of the reactor protection circuits associated with low steam generator water level is to preserve the steam generator heat sink for removal of long term residual heat. Should a complete loss of feedwater occur, the reactor would be tripped on low-low steam generator water level. In addition, redundant auxiliary feedwater pumps are provided to supply feedwater in order to maintain residual heat removal after trip. This reactor trip acts before the steam generators are dry to reduce the required capacity and increase the starting time requirements of the auxiliary feedwater pumps and to minimize the thermal transient on the reactor coolant system and steam generators.

Therefore, a low-low steam generator water level reactor trip is provided for each steam generator to ensure that sufficient initial thermal capacity is available in the steam generator at the start of the transient. It is desirable to minimize thermal transients on a steam generator for a credible loss of feedwater accident. To minimize perturbations on the feedwater control system, a control grade Median Signal Selector (MSS) is installed in the control system. Implementation of the MSS will prevent failure of a single steam generator water level channel from causing a feedwater control system disturbance requiring subsequent protective action. The application of the MSS in the feedwater control system will improve system reliability by providing a "median" signal for use by the control system to initiate control system actions based on this signal and eliminate the need for the low feedwater flow trip previously required to meet the intent of IEEE-Std. 279 Section 4.7, Control and Protection System Interaction. Thus, because of the design of the MSS (accepting three isolated level channel inputs and providing a "median" signal to the control system), the potential for a control and protection system interaction is eliminated. A more detailed discussion of the MSS relative to compliance with control and protection system interaction criteria is contained in References [12] and [14].

7.2.2.4 Additional Postulated Accidents

Loss of plant instrument air or loss of component cooling water is discussed in Section 7.3.2. 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 Section 7.7.1.4.1 and listed on 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 the Technical Specifications) being reached. Before such a limit is reached, protection will be available from the reactor trip system. At the power levels of the rod block setpoints, safety limits have not been reached; therefore these rod withdrawal stops do not come under the scope of safety-related systems and are considered as control systems.

7.2.3 Tests and Inspections

The reactor trip system meets the testing requirements of IEEE Standard 338-1971, Reference [10], as discussed in Section 7.1.2. The testability of the system is discussed in Section 7.2.2.2. The test intervals are specified in the Technical

Specifications. Written test procedures and documentation, conforming to the requirements of Reference [10], are utilized in the performance of periodic tests. Periodic testing complies with Regulatory Guide 1.22 as discussed in Sections 7.1.2 and 7.2.2.1.3.

To ensure the Median Signal Selector (MSS) functions as described in Section 7.2.2.3.5, operability of the MSS is verified commensurate with the Technical Specification surveillance interval for the associated narrow range steam generator level channels.

Signal selector testing consists of monitoring the three input signals and the one output signal. Comparison of the output signal to the input signals permits determination of whether or not the median signal is being passed and, consequently, whether the signal selector is functioning properly. Any output signal at a value other than that corresponding to the median signal is indicative of a unit failure.

The signal selector is tested concurrently with the process protection channels which provide inputs to the unit. Test signals are received from the protection system, as would normal process signals, when the individual protection channels are placed in the test mode. As the test signal magnitude is varied, that protection channel which represents the median signal will also be altered allowing the technician to determine the presence of proper signal selector action.

REFERENCES

(1) J. A. Nay, "Process Instrumentation for Westinghouse Nuclear Steam Supply Systems," WCAP 7671, May 1971.

(2) Lipchak, J. B., "Nuclear Instrumentation System," WCAP-8255, January 1974. Applicable to Power Range NIS only.

(3) Katz, D. N., "Solid State Logic Protection System Description," WCAP-7488-L, January 1971 (Proprietary) and WCAP-7672, June 1971 (Non-Proprietary).

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

(5) Burnett, T. W. T., "Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors," WCAP-7306, April 1969.

(6) Baldwin, M. S. et al., "An Evaluation of Loss of Flow Accidents Caused by Power System Frequency Transients in Westinghouse PWR's," WCAP-8424, Revision 1, May 1975.

(7) Doyle, J. P., "Noise, Fault, Surge and Radio Frequency Interference Test Report for Westinghouse Eagle 21 Process Protection Upgrade System," WCAP-11733 June 1988 (Westinghouse Proprietary Class 2); WCAP-11896 June 1988 (Westinghouse Proprietary Class 3).

(8) Lipchak, J. B. and Bartholomew, R. R., "Test Report Nuclear Instrumentation System Isolation Amplifier," WCAP-7506-P-A, April 1975 (Proprietary) and WCAP-7819-Revision 1-A, April 1975 (Non-Proprietary).

(9) The Institute of Electrical and Electronic Engineers, Inc., "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations," IEEE Standard 279-1971.

(10) The Institute of Electrical and Electronic Engineers, Inc., "IEEE Trial Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems," IEEE Standard 338-1971.

(11) Erin, L. E., "Topical Report, Eagle 21 Microprocessor-Based Process Protection System," WCAP-12374 Rev. 1 December 1991 (Westinghouse Proprietary Class 2); WCAP-12375 Rev. 1 December 1991 (Westinghouse Proprietary Class 3).

(12) Mermigos, J. F., "Median Signal Selector for Foxboro Series Process Instrumentation Application to Deletion of Low Feedwater Flow Reactor Trip," WCAP-12417 October 1989 (Westinghouse Proprietary Class 2); WCAP-12418 October 1989 (Westinghouse Proprietary Class 3).

(13) Reagan, J. R., "Westinghouse Setpoint Methodology for Protection Systems, Watts Bar Units 1 and 2, Eagle 21 Version," WCAP-12096 Rev. 5 (Westinghouse Proprietary Class 2).

(14) "Summary Report Process Protection System Eagle 21 Upgrade, NSLB, MSS, and TTD Implementation, Watts Bar Unit 1 and 2", WCAP-13462, June 1993.

(15) System Description, "Neutron Monitoring System" N3-92-4003.

(16) ISA-DS-67.04, 1982, "Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants."

Table 7.2-1 List of Reactor Trips
(Page 1 of 2)

	Reactor Trip	Coincidence Logic	Interlocks	Comments
1.	High neutron flux (Power Range)	2/4	Manual block of low setting permitted by P-10	High and low settings; manual block and automatic reset of low setting by P-10
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.	Power range high negative neutron flux rate	2/4	No interlocks	
6.	Overtemperature ΔT	2/4	No interlocks	
7.	Overpower ΔT	2/4	No interlocks	
8.	Pressurizer low pressure	2/4	Interlocked with P-7	Blocked below P-7
9.	Pressurizer high pressure	2/4	No interlocks	
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.	Reactor coolant pump bus undervoltage	2/4	Interlocked with P-7	Low voltage on all pumps permitted below P-7.

Table 7.2-1 List of Reactor Trips (Page 2 of 2)

	Reactor Trip	Coincidence Logic	Interlocks	Comments
13.	Reactor coolant pump bus underfrequency	2/4	Interlocked with P-7	Underfrequency on 2 pumps will trip all reactor coolant pump breakers and cause reactor trip; reactor trip and pump trip blocked below P-7
14.	Low-low steam generator water level	2/3 in any loop	No interlocks	Features Trip Time Delay (TTD) upgrade
15.	Turbine-generator trip*			
	a) Low auto stop oil pressure	2/3	Interlocked with P-9	Blocked below P-9
	b) Turbine stop valve close	4/4	Interlocked with P-9	Blocked below P-9
16.	Safety injection signal	Coincident with actuation of safety injection	No interlocks	(See Section 7.3 for Engineered Safety Features actuation conditions)
17.	Manual	1/2	No interlocks	

* Reactor trip on turbine trip is anticipatory in that no credit is taken for it in accident analyses.

Table 7.2-2 Protection System Interlocks
(Page 1 of 2)

Designation	Derivation	Function
	I POWER ESCALTION PERMISSIVES	
P-6	Presence of P-6: 1/2 neutron flux (intermediate range) above of source range setpoint	Allows manual blocks
	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 (back up for P-6)	
	Absence of P-10: 3/4 neutron flux (power range) below setpoint trip	Defeats the block of power range (low setpoint) reactor
	Defeats the block of a intermediate range reactor trip and intermediate range rod stops (C-1)	
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) pressurizer low pressure, and pressurizer high level	
P-8	Absence of P-8: 3/4 neutron flux (power range) below set on low reactor point	Blocks reactor trip coolant flow from one loop only

Table 7.2-2 Protection System Interlocks
(Page 2 of 2)

Designation	Derivation	Function
P-9	Absence of P-9: 3/4 neutron flux (power range) below on turbine trip setpoint	Block reactor trip
	Presence of P-9 defeats block of reactor trip on turbine trip	
P-13	Absence of 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
1.	Power range high neutron flux	1 to 120% power
2.	Intermediate range high neutron flux	10 decades of neutron flux overlapping source range by 2 decades and including 100% power
3.	Source range high neutron flux	6 decades of neutron flux (1 to 10^6 counts/sec)
4.	Power range high positive neutron flux rate	+2 to +30% of full power
5.	Power range high negative neutron flux rate	-2 to -30% of full power
6.	Overtemperature ΔT:	T_H 530 to 650°F T_C 510 to 630°F T_{avg} 530 to 630°F P_{PRZR} 1700 TO 2500 PSI F(ΔI) -60 to + 60% ΔT Setpoint 0 to 150% power
7.	Overpower ΔT	T_H 530 to 650°F T_C 510 to 630°F T_{avg} 530 to 630°F ΔT Setpoint 0 to 150% power
8.	Pressurizer low pressure	1700 to 2500 psig
9.	Pressurizer high pressure	1700 to 2500 psig
	Reactor Trip Signal	Typical Range
10.	Pressurizer high water level	Entire cylindrical portion of pressurizer
11.	Low reactor coolant flow	0 to 110% of rated flow
12.	Reactor coolant pump bus undervoltage	0 to 100% rated voltage
13.	Reactor coolant pump bus underfrequency	50 to 65 Hz
14.	Low-low steam generator water level	+ 6ft., - 12 ft. from nominal full load water level
15.	Turbine Trip (1)	

NOTES:
(1)The reactor trip on turbine trip is anticipatory in that no credit is taken for it in the accident analyses.

Table 7.2-4 Reactor Trip Correlation (Page 1 of 5)

	TRIP[a]		ACCIDENT[b]	TECH SPEC
1.	Power Range High Neutron Flux Trip (Low Setpoint)	1.	Uncontrolled Rod Cluster Control Assembly Bank Withdrawal From a Subcritical Condition (15.2.1)	3.3.1 Table 3.3.1-1 #2
		2.	Uncontrolled Boron Dilution (15.2.4) (Modes 1 and 2)	
		3.	Excessive Heat Removal Due to Feedwater System Malfunctions (15.2.10)	
		4.	Rupture of a Control Rod Drive Mechanism Housing (Rod Cluster Control Assembly Ejection) (15.4.6)	
2.	Power Range High Neutron Flux Trip (High Setpoint)	1.	Uncontrolled Rod Cluster Control Assembly Bank Withdrawal From a Subcritical Condition (15.2.1)	3.3.1 Table 3.3.1-1 #2
		2.	Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power (15.2.2)	
		3.	Uncontrolled Boron Dilution (15.2.4) (Modes 1 and 2)	
		4.	Startup of an Inactive Reactor Coolant Loop (15.2.6)	
		5.	Excessive Heat Removal Due to Feedwater System Malfunctions (15.2.10)	
		6.	Excessive Load Increase Incident (15.2.11)	
		7.	Rupture of a Control Rod Drive Mechanism Housing (Rod Cluster Control Assembly Ejection) (15.4.6)	
3.	Intermediate Range High Neutron Flux Trip	1.	Uncontrolled Rod Cluster Control Assembly Bank Withdrawal From a Subcritical Condition (15.2.1)	3.3.1 Table 3.3.1-1 #4

Table 7.2-4 Reactor Trip Correlation (Page 2 of 5)

	TRIP[a]		ACCIDENT[b]	TECH SPEC
4.	Source Range High Neutron Flux Trip	1.	Uncontrolled Rod Cluster Control Assembly Bank Withdrawal From a Subcritical Condition (15.2.1)	3.3.1 Table 3.3.1-1 #5
		2.	Uncontrolled Boron Dilution (15.2.4) (Modes 2, 3, 4, and 5)	
5.	Power Range High Positive Neutron Flux Rate Trip	1.	Uncontrolled Rod Cluster Control Assembly Bank Withdrawal From a Subcritical Condition (15.2.1)	3.3.1 Table 3.3.1-1 #3
		2.	Rupture of a Control Rod Drive Mechanism Housing (Rod Cluster Control Assembly Ejection) (15.4.6)	
6.	Power Range High Negative Flux Rate Trip	1.	Rod Cluster Control Assembly Misalignment (15.2.3)	3.3.1 Table 3.3.1-1 #3
7.	Overtemperature ΔT Trip	1.	Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power (15.2.2)	3.3.1 Table 3.3.1-1 #6
		2.	Uncontrolled Boron Dilution (15.2.4)	
		3.	Loss of External Electrical Load and/or Turbine Trip (15.2.7)	
		4.	Excessive Load Increase Incident (15.2.11)	
		5.	Accidental Depressurization of the Reactor Coolant System (15.2.12)	
		6.	Accidental Depressurization of the Main Steam System (15.2.13)	
		7.	Loss of Reactor Coolant From Small Ruptured Pipes or From Cracks in large Pipes Which Actuates ECCS (15.3.1)	
		8.	Single Rod Cluster Control Assembly Withdrawal at Full Power (15.3.6)	

Table 7.2-4 Reactor Trip Correlation (Page 3 of 5)

	TRIP[a]		ACCIDENT[b]	TECH SPEC
		9.	Major Rupture of a Main Steam Line (15.4.2.1)	
		10.	Major Rupture of a Main Feedwater Pipe (15.4.2.2)	
8.	Overpower ΔT Trip	1.	Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power (15.2.2)	3.3.1 Table 3.3.1-1 #7
		2.	Loss of External Electrical Load and/or Turbine Trip (15.2.7)	
		3.	Excessive Heat Removal Due to Feedwater System Malfunctions (15.2.10)	
		4.	Accidental Depressurization of the Main Steam System (15.2.13)	
		5.	Major Rupture of a Main Steam Line (15.4.2.1)	
9.	Pressurizer Low Pressure Trip	1.	Excessive Load Increase Incident (15.2.11)	3.3.1 Table 3.3.1-1 #8
		2.	Accidental Depressurization of the Reactor Coolant System (15.2.12)	
		3.	Accidental Depressurization of the Main Steam System (15.2.13)	
		4.	Inadvertent Operation of Emergency Core Cooling System (15.2.14)	
		5.	Loss of Reactor Coolant From Small Ruptured Pipes or From Cracks in Large Pipes Which Actuates ECCS (15.3.1)	
		6.	Major Reactor Coolant System Pipe Ruptures (LOCA) (15.4.1)	
		7.	Major Rupture of a Main Steam Line (15.4.2.1)	
		8.	Major Rupture of a Main Feedwater Pipe (15.4.2.2)	
		9.	Steam Generator Tube Rupture (15.4.3)	

Table 7.2-4 Reactor Trip Correlation (Page 4 of 5)

	TRIP[a]		ACCIDENT[b]	TECH SPEC
10.	Pressurizer High Pressure Trip	1.	Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power (15.2.2)	3.3.1 Table 3.3.1-1 #8
		2.	Loss of External Electrical Load and/or Turbine Trip (15.2.7)	
		3.	Loss of Normal Feedwater (15.2.8)	
		4.	Loss of Offsite Power to Station Auxiliaries (Station Blackout) (15.2.9)	
		5.	Major Rupture of a Main Feedwater Pipe (15.4.2.2)	
11.	Pressurizer High Water Level	1.	Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power (15.2.2)	3.3.1 Table 3.3.1-1 #9
		2.	Loss of External Electrical Load and/or Turbine Trip (15.2.7)	
		3.	Loss of Normal Feedwater (15.2.8)	
		4.	Loss of Offsite Power to Station Auxiliaries (Station Blackout) (15.2.9)	
		5.	Major Rupture of a Main Feedwater Pipe (15.4.2.2)	
12.	Low Reactor Coolant Flow	1.	Partial Loss of Forced Reactor Coolant Flow (15.2.5)	3.3.1 Table 3.3.1-1 #10
13.	Reactor Coolant Pump Bus Undervoltage Trip	1.	Complete Loss of Forced Reactor Coolant Flow (15.3.4)	3.3.1 Table 3.3.1-1 #11
14.	Reactor Coolant Pump Bus Underfrequency Trip	1.	Complete Loss of Forced Reactor Coolant Flow (15.3.4)	3.3.1 Table 3.3.1-1 #12
15.	Low-low Steam Generator Water Level Trip	1.	Loss of Normal Feedwater (15.2.8)	3.3.1 Table 3.3.1-1 #13
		2.	Loss of Offsite Power to the Station Auxiliaries (Station Blackout)(15.2.9)	
		3.	Major Rupture of a Main Feedwater Pipe (15.4.2.2)	

Table 7.2-4 Reactor Trip Correlation (Page 5 of 5)

	TRIP[a]		ACCIDENT[b]	TECH SPEC
16.	Turbine Trip-Reactor Trip	1.	Loss of External Electrical Load and/or Turbine Trip (15.2.7)	3.3.1 Table 3.3.1-1 #14
17.	Safety Injection Signal Actuation Trip	1.	Accidental Depressurization of the Main Steam System (15.2.13)	3.3.1 Table 3.3.1-1 #15
		2.	Inadvertent Operation of Emergency Core Cooling System (15.2.14)	
		3.	Major Rupture of a Main Steam Line (15.4.2.1)	
		4.	Major Rupture of a Main Feedwater Pipe (15.4.2.2)	
18.	Manual Trip		Available for all Accidents (Chapter 15)	3.3.1 Table 3.3.1-1 #1

NOTES:

a. Trips are listed in order of discussion in Section 7.2

b. References refer to accident analyses presented in Chapter 15

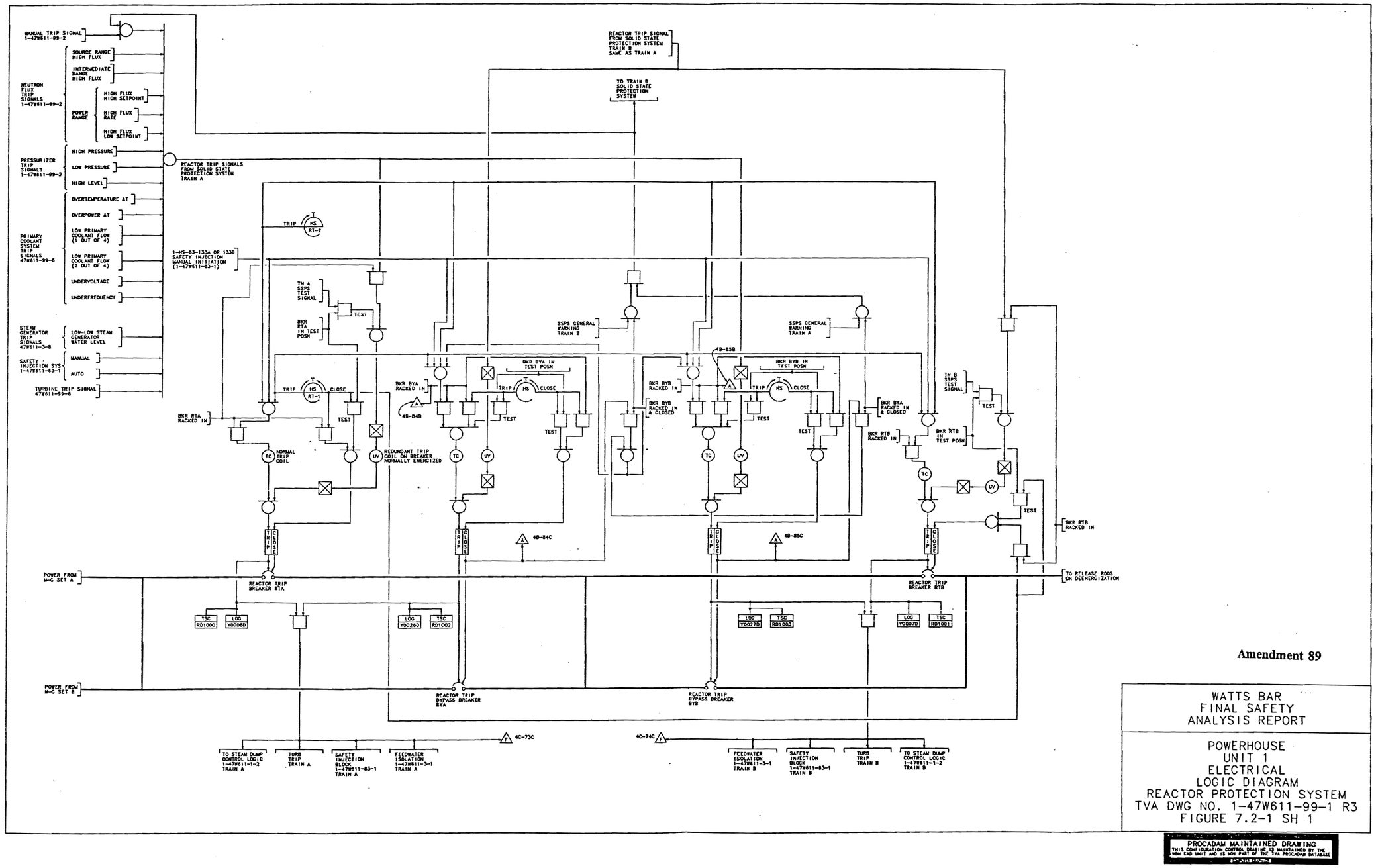


Figure 7.2-1-SH-1 Powerhouse Unit 1 Electrical Logic Diagrams - Reactor Protection System

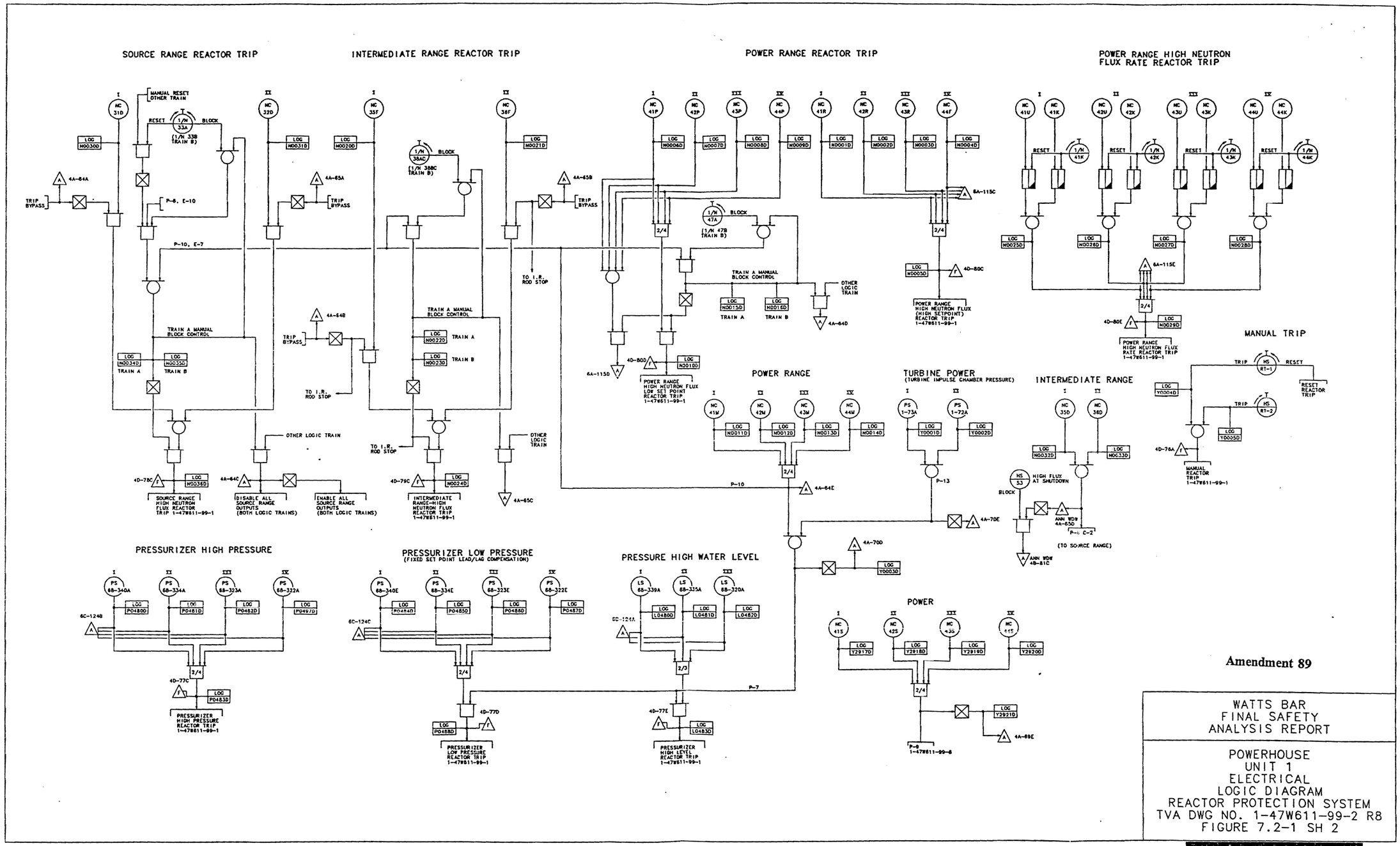


Figure 7.2-1-SH-2 Powerhouse Unit 1 Electrical Logic Diagrams - Reactor Protection System

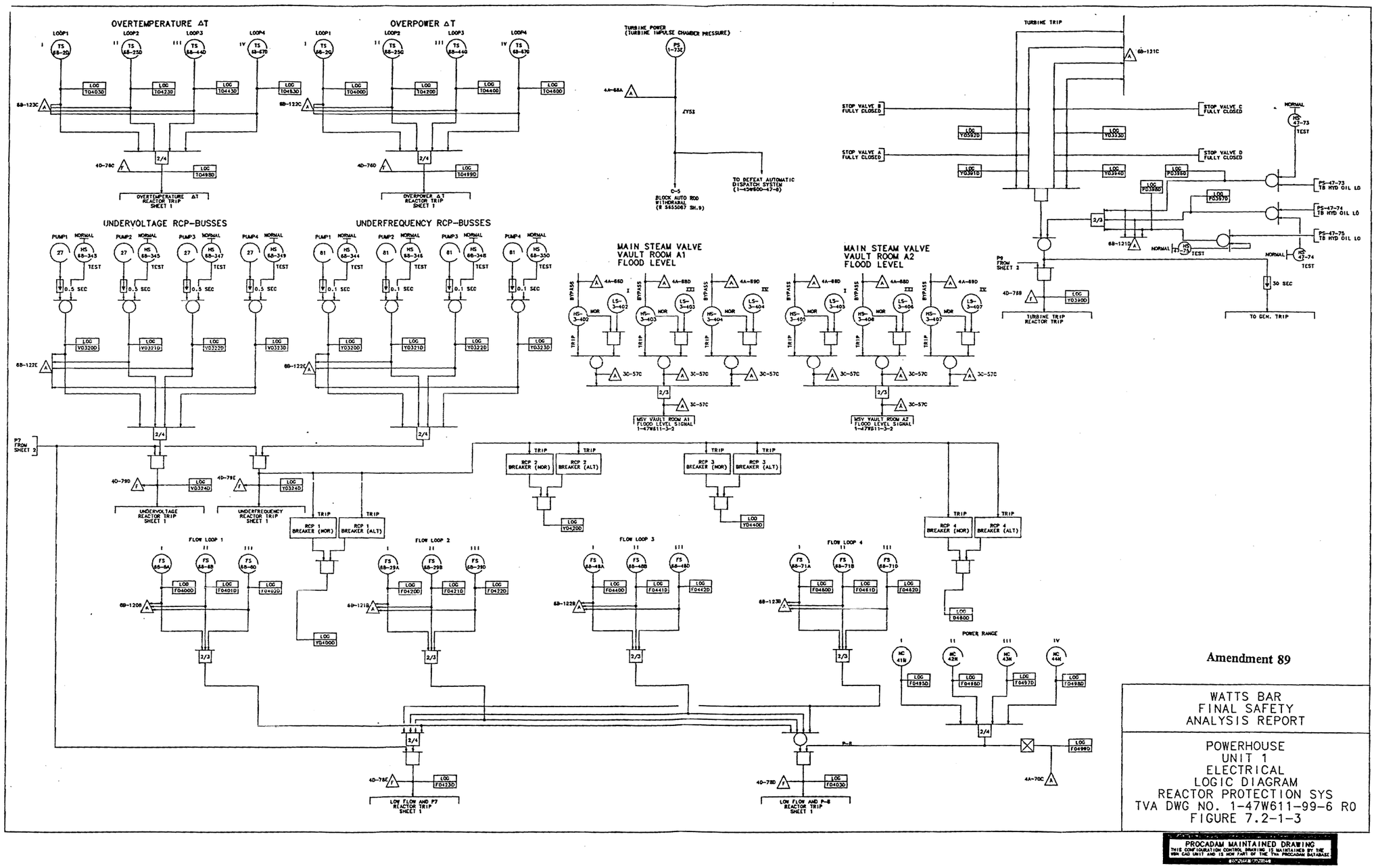
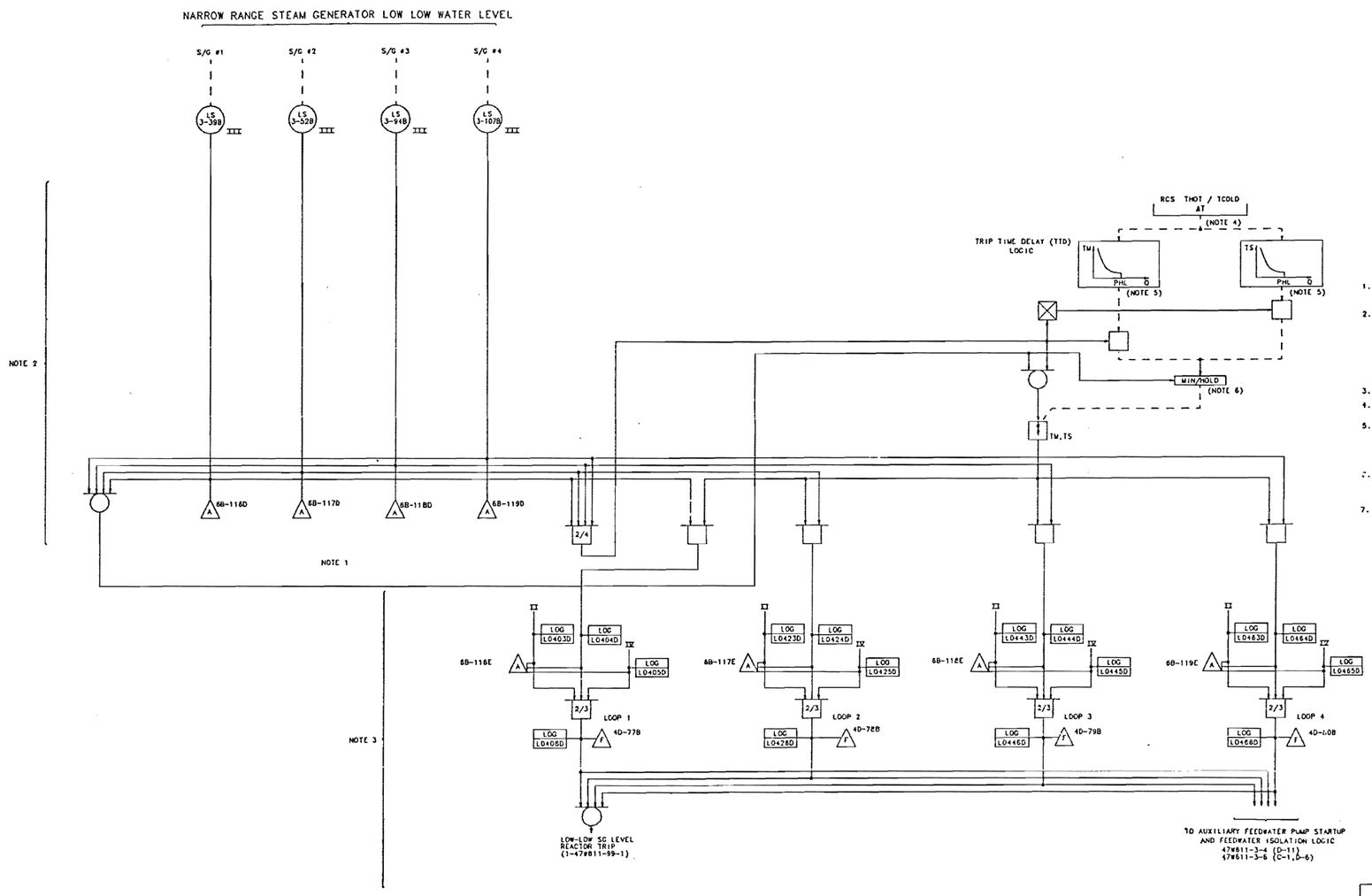


Figure 7.2-1-SH-3 Powerhouse Unit 1 Electrical Logic Diagrams - Reactor Protection System



1. ONE COMMON ANNUNCIATOR WINDOW FOR EACH STEAM GENERATOR IS SHARED WITH ALARMS GENERATED IN THE OTHER PROTECTION SETS. THE ALARMS ARE DISABLED ABOVE THE POWER HIGH LIMIT (PHL).
2. THIS LOGIC IS SPECIFIC FOR PROTECTION SET III AND IS TYPICAL FOR PROTECTION SETS II AND IV. THE BISTABLE TAG NUMBERS ASSIGNED TO PROTECTION SETS II & IV ARE AS FOLLOWS:

	S/G #1	S/G #2	S/G #3	S/G #4
PROTECTION SET II	LS-3-38B	LS-3-51B	LS-3-93B	LS-3-106B
PROTECTION SET IV	LS-3-42B	LS-3-55B	LS-3-97B	LS-3-110B

3. THIS LOGIC IS REDUNDANT AND IS PERFORMED IN THE SSPS.
4. ΔT IS A SPECIAL TEMPERATURE SIGNAL USED FOR POWER INDICATION ONLY. CONVERSION TO POWER IS PERFORMED PRIOR TO THE TIMER FUNCTION GENERATOR.
5. THE FOLLOWING DEFINITIONS APPLY TO THE FUNCTION GENERATOR:
   TM = ELAPSED TIME IF SETPOINT REACHED IN MULTIPLE STEAM GENERATORS.
   TS = ELAPSED TIME IF SETPOINT REACHED IN ONE STEAM GENERATOR.
   PHL = POWER HIGH LIMIT.
   Q = THERMAL POWER.
6. AFTER RECEIPT OF THE CONTROL LOGIC INPUT THE MIN/HOLD UNIT OUTPUT WILL BE ALLOWED TO DECREASE IF THE UNIT INPUT DECREASES. IF THE INPUT TO THE UNIT INCREASES, THE UNIT OUTPUT WILL HOLD THE MINIMUM VALUE, SINCE RECEIPT OF CONTROL LOGIC.
7. REFERENCE WESTINGHOUSE DRAWING 5655D87 SHEET 17.

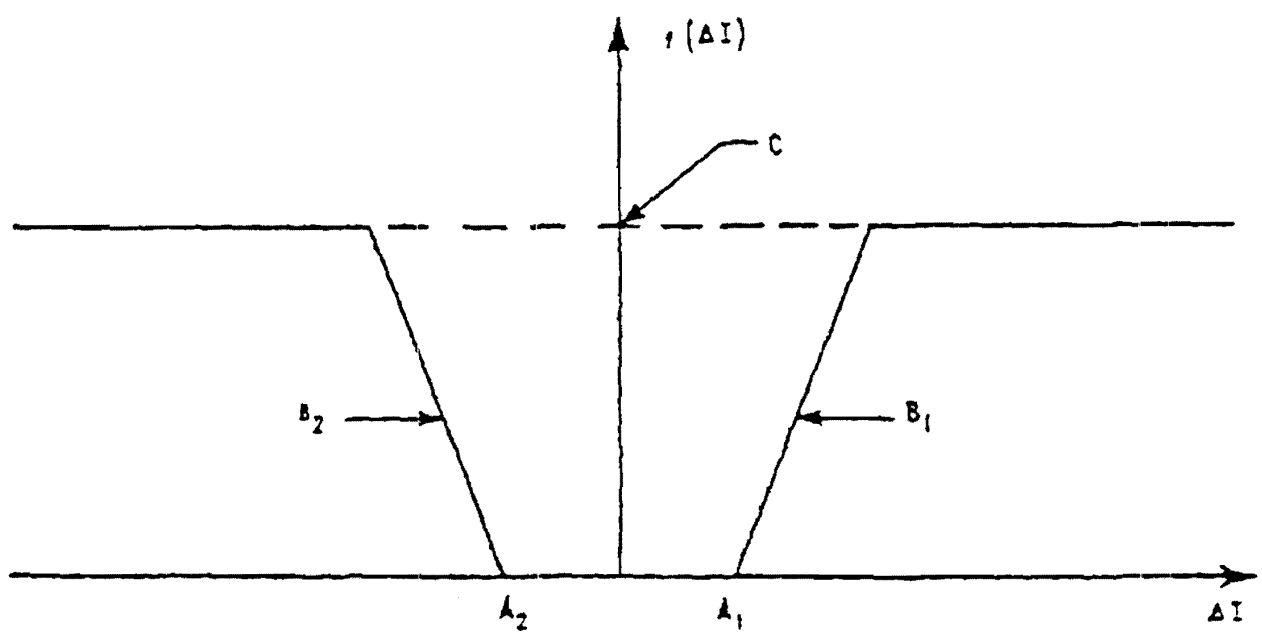
FOR SYMBOLS AND GENERAL NOTES SEE SHEET 1

REVISED BY AMMENDMENT 81

WATTS BAR
FINAL SAFETY
ANALYSIS REPORT

POWERHOUSE
UNIT 1
ELECTRICAL
LOGIC DIAGRAM
FEEDWATER SYSTEM
TVA DWG NO. 1-47W611-3-8 R1
FIGURE 7.2-1 SH 4

Figure 7.2-1-SH-4 powerhouse Unit 1 Electrical Logic Diagrams - Reactor Protection System



ΔI - NEUTRON FLUX DIFFERENCE BETWEEN UPPER AND LOWER LONG ION CHAMBERS

A_1, A_2 - LIMIT OF F (ΔI) DEADBAND

B_1, B_2 - SLOPE OF RAMP; DETERMINES RATE AT WHICH FUNCTION REACHES IT'S MAXIMUM VALUE ONCE DEADBAND IS EXCEEDED

C - MAGNITUDE OF MAXIMUM VALUE THE FUNCTION MAY ATTAIN

AMENDMENT 81

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

SETPOINT REDUCTION FUNCTION FOR OVERPOWER AND OVERTEMPERATURE ΔT TRIPS
FIGURE 7.2-2

SCANNED DOCUMENT
THIS IS A SCANNED DOCUMENT MAINTAINED ON THE WBNP OPTICRAPHICS SCANNER DATABASE

Figure 7.2-2 Setpoint Reduction Function for Overpower and Overtemperature ΔT Trips

THIS PAGE INTENTIONALLY BLANK

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-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 protection system 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 limits are being exceeded and, if they are, combines the signals into logic matrices sensitive to combinations indicative of primary or secondary system boundary ruptures (Class III or IV faults). Once the required logic combination is completed, the system sends actuation signals to the appropriate engineered safety features components. The engineered safety features actuation system meets the requirements of Criteria 13, 20, 27, 28 and 38 of the 1971 General Design Criteria (GDC).

7.3.1.1 System Description

The engineered safety features actuation system is a functionally defined system described in this section. The equipment which provides the actuation functions identified in Section 7.3.1.1.1 is listed below and discussed in this section and the references.

(1) Process Protection and Control System (References [1] and [5])

(2) Solid State Logic Protection System (Reference [2])

(3) Engineered Safety Features Test Cabinet

(4) Manual Actuation Circuits

The engineered safety features actuation system consists of two discrete portions of circuitry: 1) A process protection portion consisting of three or four redundant channels per parameter or variable to monitor various plant parameters such as the reactor coolant system and steam system pressure and temperatures and containment pressures; and 2) a logic portion consisting of two redundant trains which receive inputs from the process protection channels and perform the logic needed to actuate the engineered safety features. Each logic train is capable of actuating the engineered safety features equipment required. The intent is that any single failure within the

engineered safety features actuation system shall not prevent system action when required.

The redundant concept is applied to both the process protection and logic portions of the system. Separation of redundant process protection channels begins at the process sensors and is maintained in the field wiring, containment vessel penetrations and process 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 process protection circuitry as discussed in Reference [l] and in Section 7.2. The outputs from the process protection channels are combined into actuation logic as shown in Figure 7.3-3, Figure 7.2-1, and Figure 7.6-6 Sheet 1. 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 Section 7.1.2.

Controls provided on the control board for manual initiation of protective actions are discussed in Section 7.3.2.2.6.

7.3.1.1.1 Function Initiation

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

(1) A reactor trip, provided one has not already been generated by the reactor trip system.

(2) Cold leg injection isolation valves which are opened for injection of borated water by safety injection pumps into the cold legs of the reactor coolant system.

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

(4) Essential raw cooling water and component cooling water pumps start and heat exchanger valve realignment.

(5) Motor-driven and turbine-driven auxiliary feedwater pumps start to maintain the steam generator heat sink during emergency or accident conditions.

(6) Phase A containment isolation, whose function is to prevent fission product release (isolation of all lines not essential to reactor protection).

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

(8) Main feedwater isolation as required to prevent or mitigate the effect of excessive cooldown and the effects of MSVV flooding due to a main feedwater line break.

(9) Start the emergency diesels to assure backup supply of power to emergency and supporting systems components.

(10) Isolate the control room intake ducts to meet control room occupancy requirements following a loss-of-coolant accident.

(11) Emergency gas treatment system actuation.

(12) Containment ventilation isolation.

(13) Containment spray actuation which performs the following functions:

(a) Initiates containment spray to reduce containment pressure and temperature following a loss-of-coolant or steamline break accident inside containment.

(b) Initiates Phase B containment isolation which isolates the containment following a loss of coolant accident or a steam or feedwater line break within containment to limit radioactive releases. (Phase B isolation together with Phase A isolation results in isolation of all but safety injection and spray lines penetrating the containment).

(c) Initiates Phase B containment isolation of the following:

- Containment air return fans to cool containment and reduce pressure in event of an accident.
- Closure of the main steam isolation valves (MSIV) to limit reactor coolant system cooldown for breaks downstream of the MSIVs.

(14) Automatic switchover of the RHR pumps from the injection to the recirculation mode (Post-LOCA).

(15) Auxiliary Building isolation.

7.3.1.1.2 Process Protection Circuitry

The process protection system sensors and racks for the engineered safety features actuation system are described in References [1] and [5]. Discussed in these reports 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, orifice plates and flow elements, resistance temperature detectors, as well as automatic calculations, signal conditioning/processing and location and mounting of the devices.

The sensors monitoring the primary system are located as shown on the system flow diagrams in Chapter 5, Reactor Coolant System. The secondary system sensor locations are shown on the steam system flow diagrams given in Chapter 10.

Containment pressure is sensed by four physically separated transmitters mounted by strong supports outside of the containment. The distance from penetration to transmitter is kept to a minimum, and separation is maintained.

The following is a description of those functions not included in the reactor trip or engineered safety features actuation systems which enable additional monitoring in the post loss-of-coolant accident recovery period.

(1) High head and low head ECCS pumps flow.

These channels clearly show that the ECCS pumps are operating. The transmitters are outside the containment.

(2) ECCS Pumps Status

ECCS pumps status is provided by red (running) and green (stopped) indicating lights on the control board. These lights are operated by pump motor circuit breaker auxiliary contacts.

(3) Valve position

All engineered safety features remote operated valves have position indication on the control board to show proper positioning of the valves. The valve positions are displayed by red (open) and green (closed) lights with the exception of RHR heat exchanger outlet flow control valves (FCV-74-16 and 28) which have only a red light that is on when the valve is fully open. These indications are derived from contacts integral to the valve operators. See Section 7.7 for additional information. In the case of the accumulator isolation valves, position indication is provided by valve stem mounted limit switches which actuate annunciators on the control board when the valves are not correctly positioned for engineered safety features actuation. The stem mounted switches are independent of the limit switches in the motor operators. See Section 7.6 for additional information.

7.3.1.1.3 Logic 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 process protection channels are combined into actuation logic as shown on Figure 7.3-3, Figure 7.2-1, and Figure 7.6-6, Sheet 1.

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 Section 7.3.2.

7.3.1.1.4 Final Actuation Circuitry

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

(1) Safety injection system pump and valve actuators (see Chapter 6).

(2) Containment isolation: Phase A signal isolates all non-essential 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 high-high containment pressure signal (see Chapter 6).

(3) Essential raw cooling water and component cooling water pumps and valve actuators (see Chapter 9).

(4) Auxiliary feedwater pumps start (see Chapter 10).

(5) Diesel start (see Chapter 8).

(6) Feedwater Isolation (see Chapter 10).

(7) Containment ventilation isolation valve and damper actuators (see Chapter 9).

(8) Steamline isolation valve actuators (see Chapter 10).

(9) Containment spray pump and valve actuators (see Chapter 6).

(10) Control room isolation (see Chapter 9).

(11) Auxiliary building isolation (see Chapter 9).

In the event of an accident concurrent with a station electrical blackout, the engineered safety features loads are sequenced onto the diesel generators to prevent overloading them. This sequence is discussed in Chapter 8. The design meets the requirements of Criterion 35 of the 1971 GDC.

7.3.1.1.5 Support Systems

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

(1) Essential Raw Cooling Water System - heat removal (see Chapter 9).

(2) Component Cooling Water System - heat removal (see Chapter 9)

(3) Electrical Power Distribution Systems (see Chapter 8).

(4) Auxiliary Control Air System (see Chapter 9).

(5) Heating, Ventilating and Air Conditioning Systems (see Chapter 9).

7.3.1.2 Design Bases Information

The functional diagrams presented in Figure 7.3-3, Figure 7.2-1, and Figure 7.6-6, Sheet 1 provide a graphic outline of the functional logic associated with requirements for the engineered safety features actuation system. Requirements for the engineered safety features system are given in Chapter 6. Given below is the design bases information required in IEEE Standard 279-1971[3].

7.3.1.2.1 Generating Station Conditions

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

(1) Primary System:

(a) Rupture in small pipes or cracks in large pipes

(b) Rupture of a reactor coolant pipe (loss-of-coolant accident)

(c) Steam generator tube rupture

(2) Secondary System

(a) Minor secondary system pipe breaks resulting in steam release rates equivalent to a single dump, relief or safety valve

(b) Rupture of a major steam pipe

7.3.1.2.2 Generating Station Variables

The following list summarizes the generating station variables required to be monitored by the engineered safety features actuation system for the automatic initiation of protective actions during each accident identified in the preceding section. Post accident monitoring requirements and variables are given in Tables 7.5-1 and 7.5-2.

(1) Primary System Accidents

(a) Pressurizer pressure

(b) Containment pressure (not required for steam generator tube rupture)

(2) Secondary System Accidents

(a) Pressurizer pressure

(b) Steamline pressures

(c) Steamline pressure rate

(d) Containment pressure

7.3.1.2.3 Spatially Dependent Variables

The only variable sensed by the engineered safety features actuation system which has spatial dependence is reactor coolant temperature. The effect on the measurement is negated by taking multiple samples from the reactor coolant hot and cold legs and electronically averaging these samples in the process protection system.

7.3.1.2.4 Limits, Margin and Levels

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

7.3.1.2.5 Abnormal Events

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

(1) Loss-of-Coolant Accident (see Section 15.3 and 15.4)

(2) Steamline Breaks (see Sections 15.3 and 15.4)

(3) Earthquakes (see Chapters 2 and 3)

(4) Fire (see Section 9.5.1)

(5) Explosion (Hydrogen buildup inside-containment) (see Section 15.4)

(6) Missiles (see Section 3.5)

(7) Flood (see Chapters 2 and 3)

(8) Wind and tornadoes (See Section 3.3)

7.3.1.2.6 Minimum Performance Requirements

Minimum performance requirements are as follows:

(1) System Response Times:

The Engineered Safety Features Actuation System (ESFAS) response time is defined in Section 7.1.

The maximum allowable engineered safety features response times are provided in the Technical Requirements Manual. These values are verified in accordance with the Technical Specifications and are consistent with the safety analyses. See Table 7.1-1, Note 1, for a discussion of periodic response time verification capabilities.

(2) System accuracies:

Typical accuracies required for generating the required actuation signals for loss-of-coolant protection and streamline break protection are provided in Reference [6].

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

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

(a) Pressurizer pressure 1700 to 2500 psig

(b) Containment pressure -2 to 15 psig (ice condenser system)

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

(a) Steamline pressure 0 to 1300 psig

(b) Pressurizer pressure 1700 to 2500 psig

(c) Containment pressure -2 to 15 psig (Ice Condenser System)

7.3.1.3 Final System Drawings

The schematic diagrams and other drawings for the systems discussed in this section are referenced in Section 1.7.

7.3.2 Analysis

7.3.2.1 System Reliability/Availability and Failure Mode and Effect Analyses

A discussion on the reliability/availability of the Eagle 21 process protection system is provided in Section 7.2.2.

A failure mode and effects analysis (FMEA) was performed [Reference 4] on the logic portion of a generic Engineered Safety Features Actuation System (ESFAS) equipment similar to the Watts Bar Solid State Protection System (SSPS). The FMEA was performed down to the replaceable component level (e.g., transmitter, relay, module, etc.) for the SSPS. Concerning the output actuation functions considered, the analysis addressed the output functions available from the output cabinets of the SSPS. These output functions involve output slave relay contacts which in some cases close for final device actuation and in other cases open for final device actuation.

The results of the FMEA show that the ESFAS complies with the single failure criterion of IEEE 279-1971. No single failure was found which could prevent the ESFAS from generating the proper actuation signal on demand for an engineered safety feature. Failures are either in the safe direction, or a redundant channel or train ensures the necessary actuation capability. The actuation functions are essentially the same for the Watts Bar Nuclear Plant as for the generic system analyzed, although in the translation of these functions into the system design a few minor differences in the hardware cannot be precluded. The Watts Bar ESFAS has been designed to safety design criteria equivalent to the generic system analyzed. This ESFAS FMEA applies to all Watts Bar engineered safety features, both NSSS and BOP related, that are automatically actuated by the dry contacts of the slave relays in the output cabinets of the SSPS.

7.3.2.2 Compliance With Standards and Design Criteria

Discussion of the General Design Criteria (GDC) is provided in various sections of Chapter 7 where a particular GDC is applicable. Compliance with certain IEEE Standards and Regulatory Guides is presented in Section 7.1, Table 7.1-1. The discussion given below shows that the engineered safety features actuation system complies with IEEE Standard 279-1971, Reference [3].

7.3.2.2.1 Single Failure Criterion

The discussion presented in Section 7.2.2.2 (item 2) is applicable to the engineered safety features actuation system, with the following exception.

In the ESF, a loss of instrument power will call for actuation of ESF equipment controlled by the specific comparator that lost power (containment spray excepted). The actuated equipment must have power to comply. The power supply for the protection systems is discussed in Chapter 8. For containment spray, the final comparators are energized to trip to avoid spurious actuation. In addition, manual containment spray requires a simultaneous actuation of two manual controls. Two sets of manual containment spray controls are provided (one set/train and 2 switches/set). (Section 7.3.2.2.6 provides a discussion of protective action manual initiation capability.) This is considered acceptable because spray actuation on high-high containment pressure signal provides automatic initiation of the system via protection channels meeting the criteria in Reference [3]. Moreover, most ESF equipment (valves, pumps, etc.) can 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 1971 GDC.

7.3.2.2.2 Equipment Qualification

Equipment qualifications are discussed in Sections 3.10 and 3.11.

7.3.2.2.3 Channel Independence

The discussion presented in Section 7.2.2.2 (Item 6) is applicable. The ESF slave relay outputs from the solid state logic protection cabinets are redundant, and the

actuations associated with each train are energized up to and including the final actuators by the separate ac power supplies which power the logic trains.

7.3.2.2.4 Control and Protection System Interaction

The discussions presented in Section 7.2.2.2 (Item 7) are applicable.

7.3.2.2.5 Capability for Sensor Checks and Equipment Test and Calibration

The discussions of system testability in section 7.2.2.2 (Items 9,10, and 11) are applicable to the sensors, process protection system circuitry, and logic trains of the ESFAS.

The following discussions cover those areas in which the testing provisions differ from those for the reactor trip system.

Testing of ESFAS

The ESF systems are tested to provide assurance that they will operate as designed and will be available to function properly in the unlikely event of an accident. The testing program meets the requirements of Criteria 21, 37, 40, and 43 of the 1971 GDC and RG 1.22 as discussed in Table 7.1-1. The tests described in this section and further discussed in Section 6.3.4 meet the requirements on testing of the ECCS 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 RHR pumps are started and operated and their performance verified in a separate test discussed in Section 6.3.4. When the pump tests are considered in conjunction with the ECCS test, the requirements of GDC 37 on testing of the ECCS are met as closely as possible without causing an actual safety injection.

Testing as described in Sections 6.3.4., 7.2.2.2 (Item 10) and this section provides complete periodic testability during reactor operation of all logic and components associated with the ECCS. The program is as follows:

(1) Prior to initial plant operation, ESF system tests were conducted. (See Chapter 14.)

(2) Subsequent to initial startup, ESF system tests are conducted during each regularly scheduled refueling outage.

(3) During on-line operation of the reactor, all of the ESF process protection and logic circuitry are fully tested. In addition, essentially all of the ESF final actuators are fully tested. The remaining few final actuators whose operation is not compatible with continued on-line plant operation are checked by means of continuity testing.

Performance Test Acceptability Standard for the Safety Injection Signal and the Automatic Demand Signal for Containment Spray Actuation

During reactor operation the basis for ESFAS acceptability is the successful completion of the tests performed on the initiating system and the ESFAS. Checks of process indications verify operability of the sensors. Protection system checks and tests verify the operability of the circuitry. Solid state logic testing also checks the signal path from logic input relay contacts through the logic matrices and master relays and performs continuity tests on the coils of the output slave relays. Final actuator testing operates the output slave relays and verifies operability of those devices which require safeguards actuation and which can be tested without causing plant upset. A continuity check is performed on the actuators of the untestable devices. Operation of the final devices is confirmed by control board indication and visual observation that the appropriate pump breakers close and automatic valves have completed their travel.

The basis for acceptability for the ESF interlocks is control board indication of proper receipt of the signal upon introducing the required input at the appropriate setpoint.

Maintenance checks (performed in accordance with the plant procedures) such as resistance to ground of signal cables in radiation environments, are based on qualification test data which identifies what constitutes acceptable radiation, thermal, etc., degradation.

Frequency of Performance of Engineered Safety Features Actuation Tests

Testing is performed on a periodic basis in accordance with the Technical Specifications.

Engineered Safety Features Actuation Test Description

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

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

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

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

Description of Initiation Circuitry

Several systems comprise the total engineered safety features system, the majority of which may be initiated by different process conditions and be reset independently of each other. The remaining functions are initiated by a common signal (safety injection) which in turn may be generated by different process conditions. In addition, operation of all other vital auxiliary support systems, such as auxiliary feedwater, component cooling and service water, is initiated by the safety injection signal. Each function is

actuated by a logic circuit which is duplicated for each of the two redundant trains of engineered safety features initiation circuits. The output of each of the initiation circuits consists of a master relay which drives slave relays for contact multiplication as required. The logic, master, and slave relays are mounted in the SSPS cabinets designated Train A and Train B, respectively, for the redundant counterparts. The master and slave relay circuits operate various pump and fan circuit breakers or starters, motor operated valve contactors, solenoid operated valves, emergency generator starting, etc.

Process Protection System Testing

Process protection system testing is identical to that used for reactor trip circuitry and is described in Section 7.2.2.2 (Item 10). 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 the same as that discussed in Section 7.2.2.2 (Item 10). Logic matrices are tested from the Train A and Train B logic rack test panels. During this test, each of the logic inputs is actuated automatically in all combinations of trip and non-trip logic. Trip logic is not maintained sufficiently long enough to permit master relay actuation; master relays are "pulsed" in order to check continuity. Following the logic testing, the individual master relays are actuated electrically to test their mechanical operation. Actuation of the master relays during this test will apply low voltage to the slave relay coil circuits to allow continuity checking but not slave relay actuation. Annunciation is provided in the control room to indicate when a train is in test. During logic testing of one train, the other train can initiate the required engineered safety features function. Additional details of the logic system testing are given in 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. Slave relays do not operate because of reduced voltage.

The ESFAS final actuation device or actuated equipment testing is performed from the engineered safeguards test cabinets, which are located near the SSPS logic cabinets. One test cabinet is provided for each of the two protection Trains A and B. Each cabinet contains individual test switches necessary to actuate the slave relays. To prevent accidental actuation, test switches are of the type that must be rotated and then depressed to operate the slave relays. Assignments of contacts of the slave relays for actuation of various final devices or actuators have been made such that groups of devices or actuated equipment can be operated individually during plant operation without causing plant upset or equipment damage. In the unlikely event that an ESFAS signal is initiated during the test of the final device that is actuated by this ESFAS signal, the device will already be in its safeguard position.

During this last procedure, close communication between the main control room operator and the operator at the test panel is required. Prior to the energizing of a slave

relay, the main control room (MCR) operator assures that plant conditions will permit operation of the equipment that will be actuated by the relay. After the tester has energized the slave relay, the MCR operator observes that all equipment has operated as indicated by appropriate indicating lamps, monitor lamps, and annunciators on the control board, and, using a prepared check list, records all operations. He then resets all devices and prepares for operation of the next slave relay actuated equipment.

By means of the procedure outlined above, all ESF devices actuated by ESFAS initiation circuits, with the exceptions noted in Table 7.1-1 Note 2, are operated by the test circuitry.

Actuator Blocking and Continuity Test Circuits

Those few final actuation devices that cannot be actuated during plant operation (discussed in Section 7.1) have been assigned to slave relays for which additional test circuitry has been provided to individually block actuation of a final device upon operation of the associated slave relay during testing. Operation of these slave relays, including contact operations, and continuity of the electrical circuits associated with the final devices' control are checked in lieu of actual operation. The circuits provide for monitoring of the slave relay contacts and the devices' control circuit cabling, control voltage, and actuation solenoids. These continuity test circuits for components that cannot be operated online are verified by proving lights on the safeguards test cabinets. 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.

Time Required for Testing

It is estimated that testing of a process protection system channel can be performed within one hour. Logic testing of either Train A or B can be performed in less than 2 hours. Testing of actuated components (including those which can only be partially tested) requires the involvement of a control room operator. It is expected to require several shifts to accomplish these tests. During this procedure automatic actuation circuitry will override testing, except for those few devices associated with a single slave relay whose outputs must be blocked. It is anticipated that continuity testing associated with a blocked slave relay could take several minutes. During this time the redundant devices in the other train would be functional.

Summary of On-Line Testing Capabilities

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

logic rack. To check the final actuation device a continuity test of the individual control circuits is performed.

The procedure requires testing at various locations:

(1) Process protection system testing and verification of comparator setpoints are accomplished at protection system racks. Verification of comparator relay operation is done at the MCR status lights, except for those channels which may be tested in bypass.

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

(3) Testing of pumps, fans and valves is done at the safeguards test cabinets located near the logic racks in combination with actions initiated by the control room operator.

(4) Continuity testing for those circuits that can not be operated is also done at the safeguards test cabinets.

Testing During Shutdown

Emergency core cooling system tests are performed at each major fuel reloading with the reactor coolant system isolated from the emergency core cooling system by closing the appropriate valves. A test safety injection signal will then be applied to initiate operation of active components (pumps and valves) of the emergency core cooling system. This is in compliance with Criterion 37 of the 1971 GDC.

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

Periodic Maintenance Inspections

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

Typical maintenance procedures include the following:

(1) Check cleanliness of accessible exterior and interior surfaces.

(2) Check fuses for corrosion.

(3) Inspect for loose or broken control knobs and burned out indicator lamps.

(4) Inspect for moisture and condition of cables and wiring.

(5) Mechanically check connectors and terminal boards for looseness, poor connection, or corrosion.

(6) Inspect the components of each assembly for signs of overheating or component deterioration.

(7) Perform complete system operating check.

The balance of the requirements listed in Reference [3] (paragraphs 4.11 through 4.22) are discussed in Section 7.2.2.2.

7.3.2.2.6 Manual Initiation, Reset and Blocks of Protective Actions

Capability is provided at the system level for manual initiation of reactor trip, safety injection, Phase A containment isolation and containment spray (along with Phase B containment isolation and containment ventilation isolation). Manual reset capability of these protective actions is also provided. This design meets the requirements of IEEE 279-1971, Section 4.17 and Regulatory Guide 1.62.

However, the manual initiation of both steamline isolation, and switchover from injection to recirculation following a loss of primary coolant accident are performed at the component level only, so that the initiation of these two systems is not specifically designed to meet Section 4.17 of IEEE 279-1971.

The main steam isolation valves are included in the plant design to mitigate the consequences resulting from steam line breaks, and protection logic is provided in the plant design to automatically close the valves when necessary. There are four individual main steam isolation valve momentary control switches (one per loop) mounted on the control board. Each switch when actuated will isolate one of the main steam lines.

The inadvertent manual closure of any single MSIV or the simultaneous closure of all MSIV's both create Condition II events. If all valves are closed simultaneously when the plant is operating at full power, a loss-of-load accident will result with a consequent primary and secondary side pressure increase, reactor trip and secondary side safety valve release. In the event that only one valve closes on inadvertent manual actuation when the plant is operating at full power, the steam flow in the other loops will increase in an attempt to restore full power steam flow. The non-symmetric steam flow can cause an increase in reactor power due to the non-symmetric loop temperatures and to the moderator temperature coefficient of reactivity. Consequently margins to DNB are reduced.

Since remote individual closure of the steam line isolation valves from the control room is required for operational reasons, it is not felt that putting additional manual capabilities which can lead to the inadvertent closure of all steam stop valves is in the direction of reactor safety.

The manual operations performed at the component level for switchover from safety injection to cold leg recirculation following a loss of primary coolant accident are

described in Table 6.3.2-4. An evaluation of the associated time sequences is presented in Table 6.3.2-5.

The manual block features associated with pressurizer and steam line safety injection signals provide the operator with the means to block initiation of safety injection during plant startup or shutdown/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.

7.3.2.3 Further Considerations

In addition to the considerations given above, a loss of one train of auxiliary control air or loss of a component cooling water train to vital equipment has been considered. Neither the loss of an auxiliary control air train nor the loss of one component cooling water train can cause safety limits as given in the Technical Specifications to be exceeded. Likewise, loss of either one of the two trains will not adversely affect the core or the reactor coolant system nor will it prevent safe shutdown if this is necessary. Furthermore, in general, pneumatically operated valves and controls will assume a preferred operating position upon loss of control air.

In its present design, Westinghouse does not provide any circuitry which will directly trip the reactor coolant pumps on a loss of component cooling water. Normally, 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.

In regards to the auxiliary feedwater system, there are two motor driven pumps and one turbine driven pump. Starting of the motor driven pumps and closing of blowdown isolation and sampling valves for all steam generators are initiated automatically by any of the following signals:

(1) Safety injection.

(2) Blackout sequence signal.

(3) 2/3 low-low level in any steam generator.

(4) Manual start.

(5) Trip of all main feed pumps.

(6) AMSAC (Anticipated Transients Without Scram Mitigation System Actuation Circuitry).

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

(1) 2/3 low-low level in 2/4 steam generators.

(2) Manual start.

(3) Blackout signal.

(4) Safety injection.

(5) Trip of all main feed pumps.

(6) AMSAC

7.3.2.4 Summary

The effectiveness of the engineered safety features actuation system is evaluated in Chapter 15, 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.

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

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

7.3.2.4.1 Loss-of-Coolant Protection

By analysis of the 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 loss-of-coolant accident is reliably detected by the low pressurizer pressure signal; the emergency core cooling system is actuated in time to prevent or limit core damage. (Refer to Section 15.3.1.)

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. (Refer to Section 15.4.1.)

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; that is, the engineered safety features actuation system detects the leakage of the coolant into the containment. The generation time of the actuation signal of about 1.5 seconds, after detection of the consequences of the accident, is adequate.

Containment spray will provide additional emergency cooling of containment and also limit fission product release upon sensing elevated containment pressure (high-high) to mitigate the effects of a loss-of-coolant accident.

The delay time between detection of the accident condition and the generation of the actuation signal for these systems is assumed to be about 1.0 second; well within the capability of the protection system equipment. However, this time is short compared to that required for startup of the fluid systems.

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

7.3.2.4.2 Steam Line Break Protection

The emergency core cooling system is also actuated in order to protect against a steam line break. About 2.0 seconds elapses between sensing low steam line 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 for a steam line break in time to limit or prevent further core damage for steam line break cases. There is a reactor trip but the core reactivity is further reduced by the 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 steamline break accident is provided by closure of all steam line isolation valves in order to prevent uncontrolled blowdown of all steam generators. The generation of the protection system signal (about 2.0 seconds) is again short compared to the time to trip the fast acting steam line isolation valves which are designed to close in less than 6 seconds.

In addition to actuation of the engineered safety features, the effect of a steamline break accident also generates a signal resulting in a reactor trip on overpower or following emergency core cooling system actuation. However, the core reactivity is further reduced by the borated water injected by the emergency core cooling system.

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

REFERENCES

(1) Nay, J., "Process Instrumentation for Westinghouse Nuclear Steam Supply System (4 Loop Plant)" WCAP-7671, April, 1971 (Non-Proprietary).

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

(3) The Institute of Electrical and Electronics Engineers, Inc., IEEE Standard: 'Criteria for Protection System for Nuclear Power Generating Stations,' IEEE Standard 279-1971.

(4) Mesmeringer, J. C., "Failure Mode and Effects Analysis (FMEA) of the Engineered Safety Features Actuation System," WCAP-8584 Revision 1, February 1980 (Proprietary) and WCAP-8760, February 1980 (Non-Proprietary).

(5) Erin, L. E., "Topical Report, Eagle 21 Microprocessor-Based Process Protection System," WCAP-12374 Rev. 1 December 1991 (Westinghouse Proprietary Class 2); WCAP-12375 Rev. 1 December 1991 (Westinghouse Proprietary Class 3).

(6) Reagan, J. R., "Westinghouse Setpoint Methodology for Protection Systems, Watts Bar Units 1 and 2, Eagle 21 Version," WCAP-12096 Rev. 5, May 1993 (Westinghouse Proprietary Class 2).

Table 7.3-1 Instrumentation Operating Condition For Engineered Safety Features

NO.	FUNCTIONAL UNIT	NO. OF CHANNELS	NO. OF CHANNELS TO TRIP
1.	SAFETY INJECTION		
1a.	Manual	2	1
1b.	Containment Pressure High	3	2
1c.	Pressurizer Pressure Low*	3	2
1d.	Steamline Pressure Low (Lead-Lag compensated)*	12 (3/steamline)	2/3 in any steamline
2.	CONTAINMENT SPRAY		
2a.	Manual**	4	2
2b.	Containment Pressure High-High	4	2

*Interlocked with Permissive P-11; see functional description of P-11 in Table 7.3-3

**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 single failure requirements of IEEE Standard 279-1971. Simultaneous operation of two switches is desirable to prevent inadvertent spray actuation.

Table 7.3-2 Instrumentation Operating Condition For Isolation Functions (Page 1 of 2)

NO.	FUNCTIONAL UNIT	NO. OF CHANNELS	NO. OF CHANNELS TO TRIP
1.	CONTAINMENT ISOLATION		
1a.	Automatic Safety Injection (Phase A)	See Item No. 1b through 1d of Table 7.3-1.	
1b.	Containment Pressure High-High (Phase B)	4	2
1c.	Manual Phase A	2	1
	Phase B	See Item No. 2a of Table 7.3-1.	
2.	STEAMLINE ISOLATION		
2a.	Steamline Pressure Low* (Lead-lag compensated)	12 (3/Steamline)	2/3 in any Steamline
2b.	High Steamline Pressure Rate (Rate-Lag compensated)*	12 (3/Steamline)	2/3 in any steamline
2c.	Containment Pressure High-High	4	2
3.	FEEDWATER LINE ISOLATION		
3a.	Safety Injection	See Item No. 1 of Table 7.3-1.	
3b.	Steam Generator Level High-High	12 (3/Steam Generator	2/3 in any Steam Generator
3c.	Main Steam Valve Vault High Flood Level	6 (3/MSVV)	2/3 in any MSVV
4.	CONTAINMENT VENTILATION ISOLATION		
4a.	Manual Containment Isolation Phase A Containment Spray	See Item No. 1c above See Item No. 2a of Table 7.3-1.	
4b.	Containment Gas Monitor Radioactivity High	1	1
4c.	Auxiliary Building Gas Monitor Radioactivity High	1	1

Table 7.3-2 Instrumentation Operating Condition For Isolation Functions (Page 2 of 2)

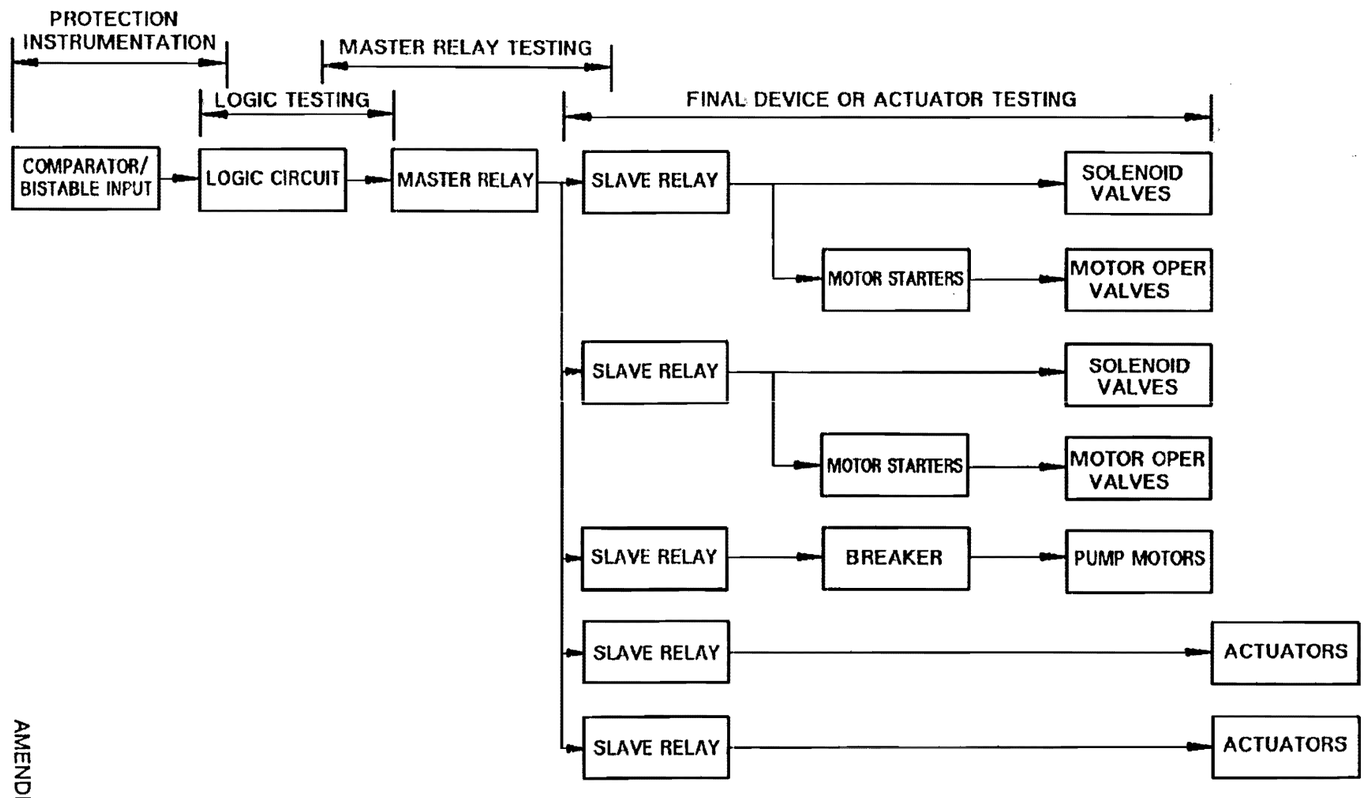
NO.	FUNCTIONAL UNIT	NO. OF CHANNELS	NO. OF CHANNELS TO TRIP
4d.	Auxiliary Building Air Particulate Monitor Radioactivity High	1	1
4e.	Safety Injection	See Item No. 1 of Table 7.3-1.	

*Interlocked with Permissive P-11; see functional description of P-11 in Table 7.3-3.

Table 7.3-3 Interlocks For Engineered Safety Features Actuation System

Designation	Input	Function Performed
P-4	Reactor trip	Actuates turbine trip
		Closes main feedwater valves on T_{avg} below low setpoint
		Prevents opening of main feedwater valves which were closed by safety injection or High-High steam generator water level
		Allows manual block of the automatic actuation or reactuation of safety injection
	Reactor not tripped	Defeats the block preventing automatic actuation or reactuation of safety injection
P-11	2/3 Pressurizer pressure below setpoint	Allows manual block of safety injection actuation on low pressurizer pressure signal. Allows manual block of safety injection and steamline isolation on low steamline pressure. Steamline isolation on high negative rate steamline pressure is permitted when this manual block is accomplished.
	2/3 Pressurizer pressure above setpoint	Defeats manual block of safety injection actuation. Defeats manual block of safety injection and steamline isolation on low steamline pressure and defeats steamline isolation on high negative rate steamline pressure.
P-12	2/4 T_{avg} below low-low setpoint	Blocks steam dump condenser dump valves
		Allows manual bypass of steam dump block for the cooldown valves only
	3/4 T_{avg} above low-low setpoint	Defeats the manual bypass of steam dump block
P-14	2/3 steam generator water level above setpoint on one or more steam generators	Closes all feedwater control valves and isolation valves
		Trips all main feedwater pumps which closes the pump discharge valves.
		Actuates turbine trip.
		Trips condensate booster pumps and condensate demineralizer pumps

THIS PAGE INTENTIONALLY BLANK



SCANNED DOCUMENT
THIS IS A SCANNED DOCUMENT MAINTAINED ON THE LBNP OPTISRAPHICS SCANNER DATABASE

AMENDMENT 81

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

E S F TEST CIRCUIT
(TYPICAL)
FIGURE 7.3-1

Figure 7.3-1 ESF Test Circuits (Typical)

Figure 7.3-2 Deleted by Amendment 81

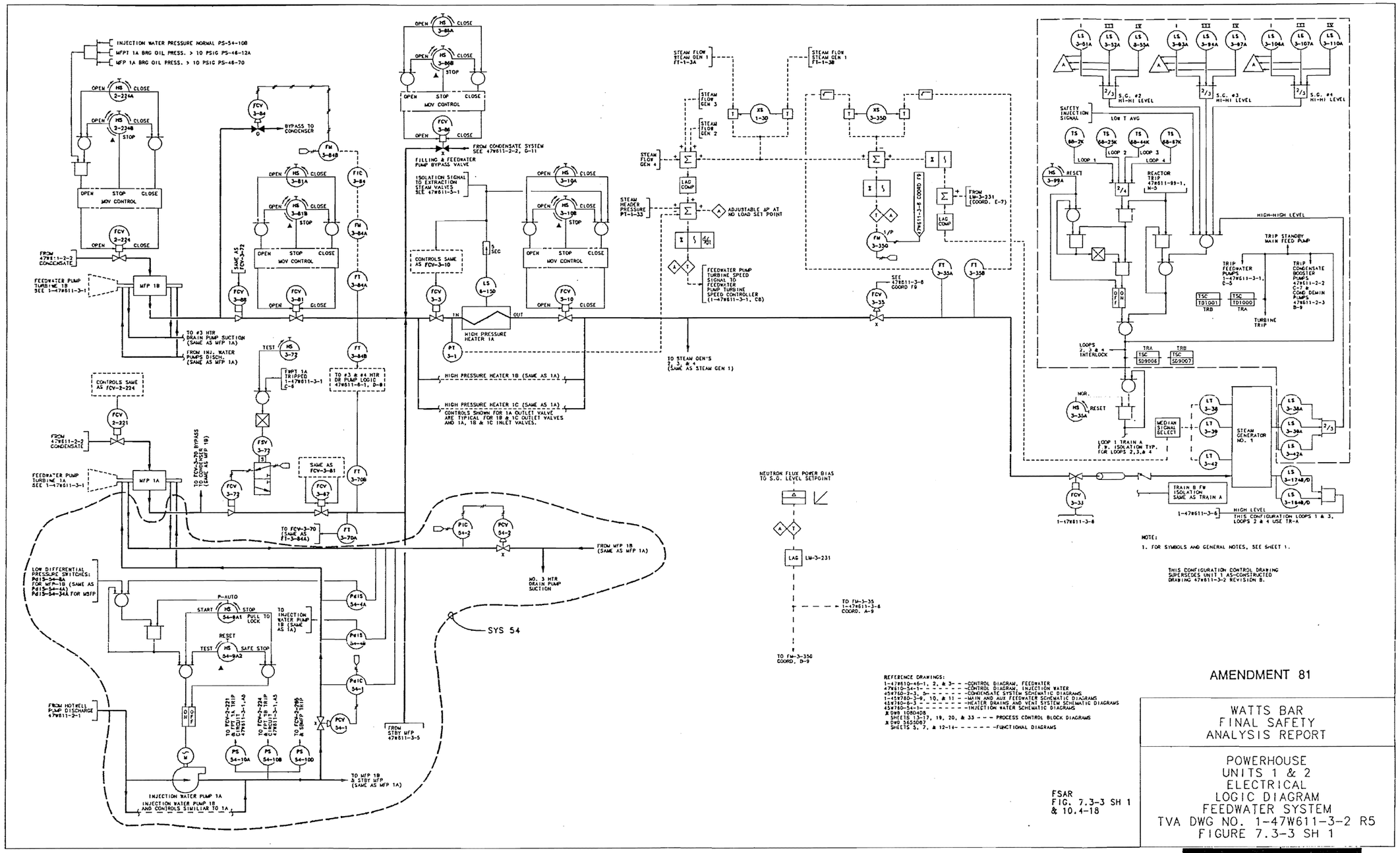
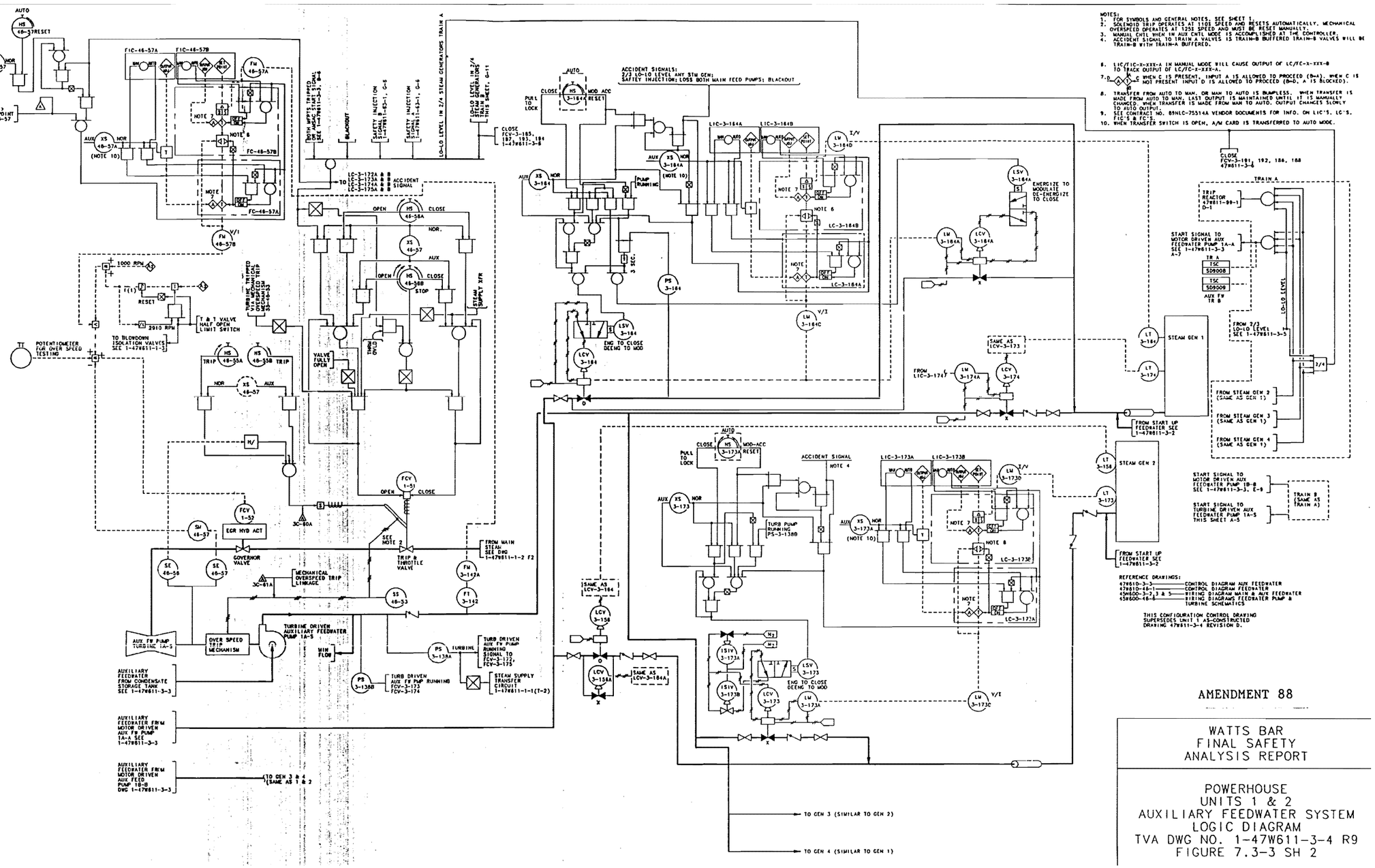


Figure 7.3-3-SH-1 Powerhouse Units 1 & 2 Electrical Logic Diagram Feedwater System



AMENDMENT 88

WATTS BAR
FINAL SAFETY
ANALYSIS REPORT

POWERHOUSE
UNITS 1 & 2
AUXILIARY FEEDWATER SYSTEM
LOGIC DIAGRAM
TVA DWG NO. 1-47W611-3-4 R9
FIGURE 7.3-3 SH 2

Figure 7.3-3-SH-2 Powerhouse Units 1 & 2 Auxiliary Feedwater System Logic Diagram

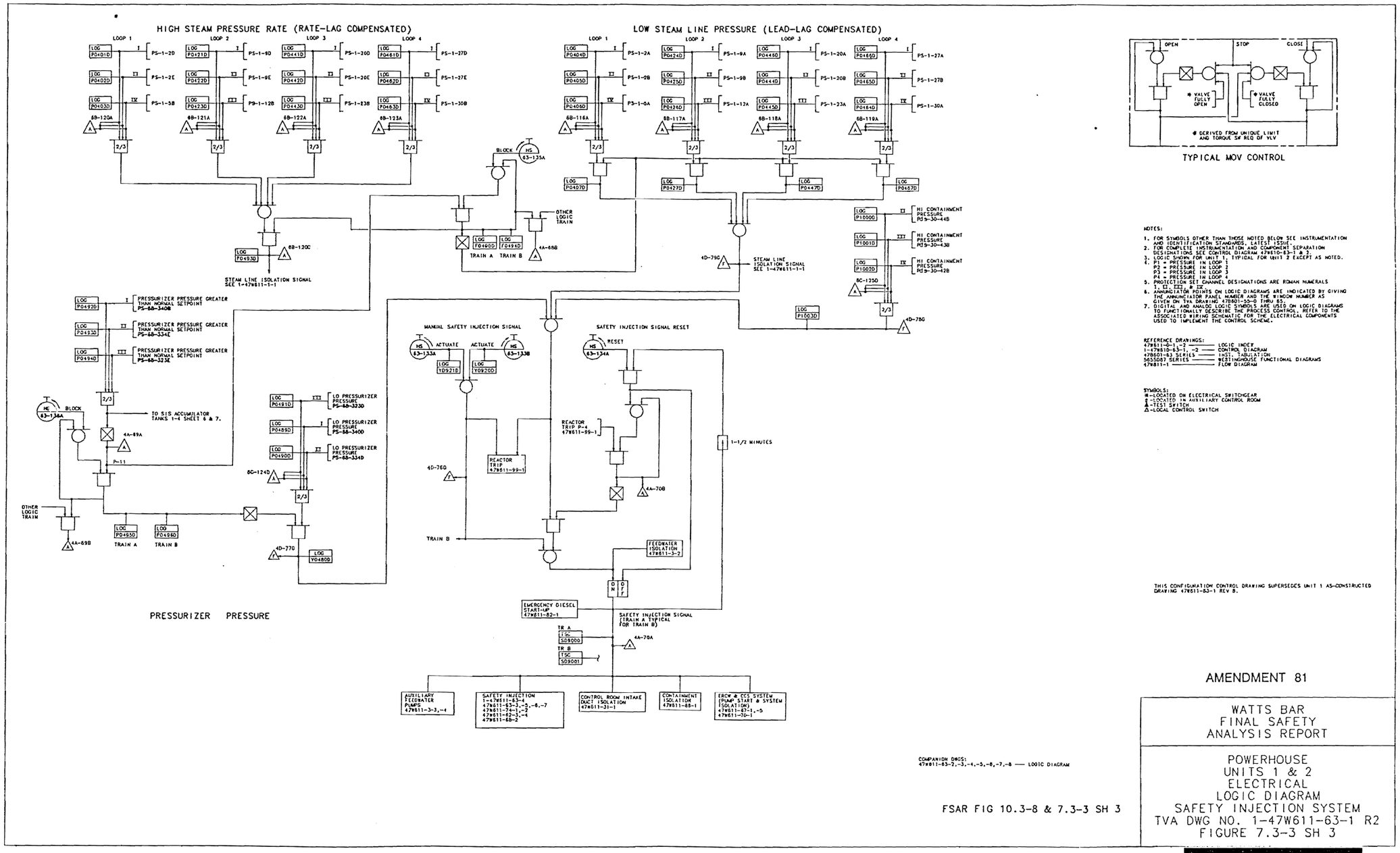
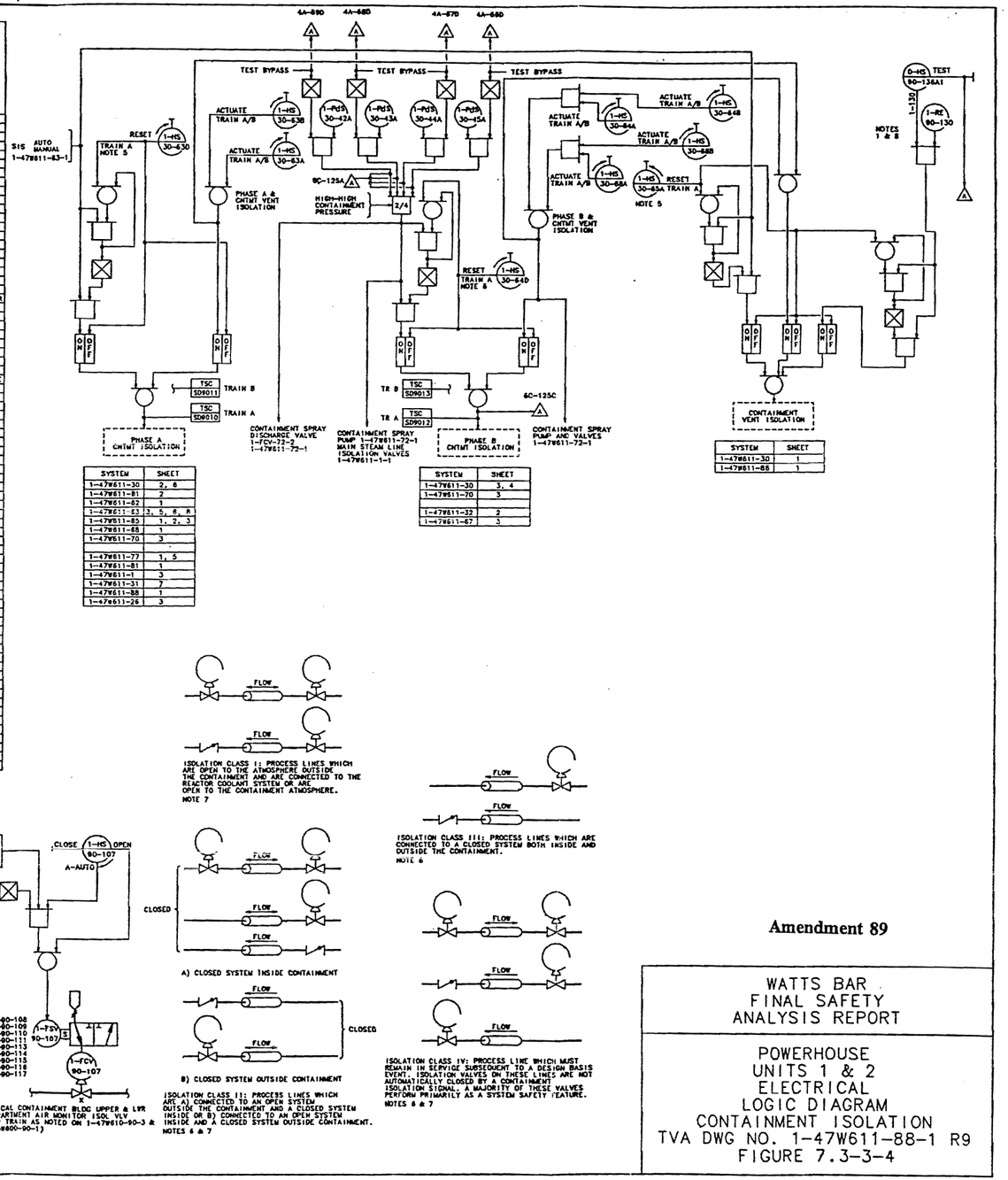


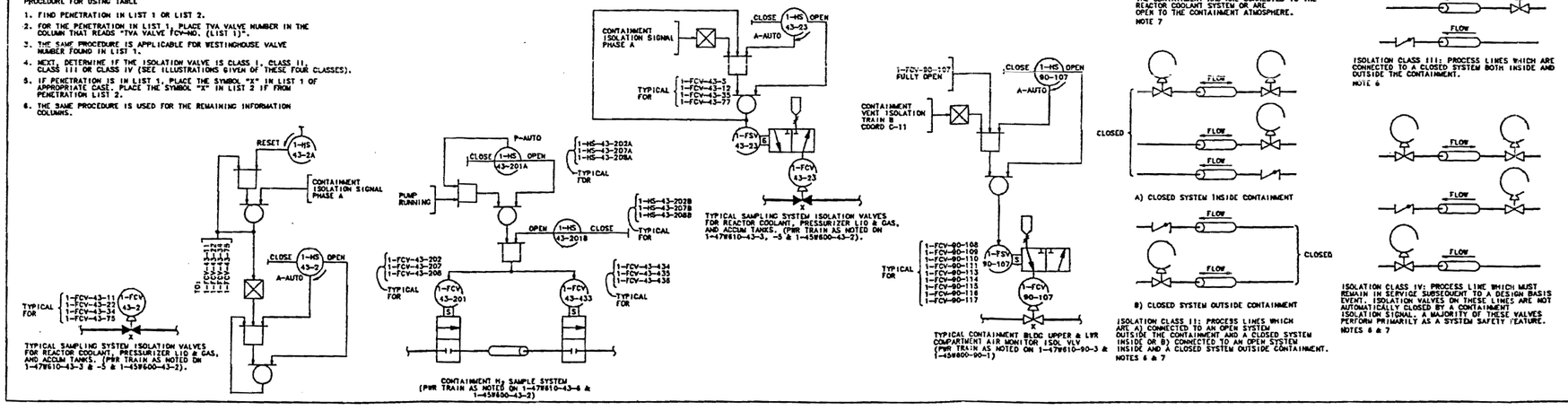
Figure 7.3-3-SH-3 Powerhouse Units 1 & 2 Electrical Logic Diagram for Safety Injection System

CONTAINMENT PENETRATIONS LIST 1	WESTINGHOUSE VALVE NO. (LIST 1) IN-BOARD	WESTINGHOUSE VALVE NO. (LIST 1) OUT-BOARD	TVA VALVE NO. (LIST 2) IN-BOARD	TVA VALVE NO. (LIST 2) OUT-BOARD	ISOLATION VALVE SYSTEM LIST 1	ISOLATION VALVE SYSTEM LIST 2	ISOLATION VALVE SYSTEM LIST 1	ISOLATION VALVE SYSTEM LIST 2	ISOLATION VALVE SYSTEM LIST 1	ISOLATION VALVE SYSTEM LIST 2	CONTAINMENT VENT ISOLATION PHASE A LIST 1	CONTAINMENT VENT ISOLATION PHASE A LIST 2	CONTAINMENT VENT ISOLATION PHASE B LIST 1	CONTAINMENT VENT ISOLATION PHASE B LIST 2	CONTAINMENT VENT ISOLATION MANUAL LIST 1	CONTAINMENT VENT ISOLATION MANUAL LIST 2	CONTAINMENT VENT ISOLATION MOV-TYPE LIST 1	CONTAINMENT VENT ISOLATION MOV-TYPE LIST 2	AIR-OPERATED OR SELF-OPERATED LIST 1	AIR-OPERATED OR SELF-OPERATED LIST 2	WESTINGHOUSE VALVE NO. (LIST 1) IN-BOARD	WESTINGHOUSE VALVE NO. (LIST 1) OUT-BOARD	TVA VALVE NO. (LIST 2) IN-BOARD	TVA VALVE NO. (LIST 2) OUT-BOARD	CONTAINMENT PENETRATIONS LIST 2
LOWER COMPT PURGE AIR SUPPLY			30-17	30-18	X	X						X				X	X	X	X	X	8047	8033	CK VLV	88-305	WDS #3 TO PZR RLF TK
LOWER COMPT PRESSURE RELIEF			30-40	30-37	X	X						X				X	X	X	X	X	9159A	9159B	73-16	77-17	RC DR TANK TO GAS ANALYZER
LOWER COMPT PURGE AIR EXH			30-54	30-57	X											X		X		X					
INSTR ROOM PURGE AIR EXH			30-58	30-58	X	X										X		X		X			WHL VLV	WHL VLV	TO REFUELING CAVITY UNIT 1
UPPER COMPT PURGE AIR EXH			30-50	30-51	X	X										X		X		X			WHL VLV	WHL VLV	WDS REFUELING CAVITY UNIT 1 TO EFP
UPPER COMPT PURGE AIR EXH			30-52	30-53	X											X		X		X					
UPPER COMPT PURGE AIR SUPPLY			30-10	30-8	X											X		X		X					
UPPER COMPT PURGE AIR SUPPLY			30-8	30-7	X											X		X		X					
LOWER COMPT PURGE AIR SUPPLY			30-15	30-14	X											X		X		X					
INSTR ROOM PURGE AIR SUPPLY			30-30	30-18	X											X		X		X					
						X						X								X			43-75	43-77	DOWNSTREAM EXCESS LETDOWN HX
						X						X				X				X	8871	8844,8888	63-71	63-84,23	ACCUMULATOR TO HOLD UP TANK
STEAM GEN BLOW DOWN			1-182	1-14			X				X							X		X					
STEAM GEN BLOW DOWN			1-181	1-7		X	X				X	X						X		X			43-34	43-36	ACCUMULATOR SAMPLE
STEAM GEN BLOW DOWN			1-184	1-32			X				X							X							
STEAM GEN BLOW DOWN			1-183	1-25			X				X							X							
LETDOWN LINE	8149A-C	8152	63-72,73,74,76	63-77	X						X							X							CNTMT PRESSURE MONITOR
NORMAL CHARGE LINE	8381	8183	CK VLV	62-80	X										X		X								
RHR RETURN	8841ABC	8840	CK VLV	63-172		X				X		X		X	X		X			X	9835	9834	81-67	81-66	GLYCOL INLET TO FLOOR COOLER
RHR SUPPLY	8701		74-2			X				X		X		X	X		X			X	9833	9832	81-122	81-110	GLYCOL OUTLET FROM FLOOR COOLER
SUMP SUCT TO RHR PUMP A-A		8811A		63-72						X					X		X								
LOW HD SIS	8818BC	8809A	CK VLV	63-83						X					X		X								
LOW HD SIS	8818A&D	8809B	CK VLV	63-84						X					X		X								
SIS PUMP DISCHARGE COLD LEG	8818A-D	8835	CK VLV	63-23				X		X		X			X		X			X			43-540	43-55	STGEN BLWDN NO. 1 SAMPLE
B INJ TK-CHRG PUMP DISCH	8805	8801ABB	CK VLV	63-93,96				X		X		X			X		X			X			43-580	43-58	STGEN BLWDN NO. 2 SAMPLE
WDS N_2 TO ACCUMULATOR	8968	8880	CK VLV	63-84	X			X				X	X							X			43-590	43-61	STGEN BLWDN NO. 3 SAMPLE
SIS RELIEF VALVE DISCHARGE	8087		CK VLV	REL VLV	X			X					X							X			43-630	43-64	STGEN BLWDN NO. 4 SAMPLE
PZR S1 SP SMPL			43-7	43-3	X							X							X						
PZR L10 SP SMPL			43-11	43-12	X	X						X	X					X	X				CK VLV	26-240	FIRE PROTECTION CNTMT STANDPIPE
RC OUTLET HDRS SAMPLE			43-22	43-23	X	X						X	X					X	X				CK VLV	26-243	FIRE PROTECTION RCP
SUMP SUCT TO RHR PUMP B-B		8811B		63-73						X					X		X								
CCS TO RC PUMP OIL COOLERS			CK VLV	70-140	X									X		X		X							
MAIN STEAM				1-4			X											X							
MAIN STEAM				1-11			X											X							
MAIN STEAM				1-22		X	X								X			X	X				CK VLV	32-80	CONTROL AIR
MAIN STEAM				1-29		X	X								X			X	X				CK VLV	32-102	CONTROL AIR
CCS FROM EXCESS LETDOWN HX				70-65		X	X					X			X			X	X				CK VLV	82-110	CONTROL AIR
AUX FEEDWATER TURB LOOP 1				CK VLV							X														
AUX FEEDWATER TURB LOOP 3				CK VLV							X														
AUX FEEDWATER TURB LOOP 3				CK VLV							X														
AUX FEEDWATER TURB LOOP 4				CK VLV		X					X				X	X		X					87-89	87-83	ERCW-LOWER CNTMNT CLRS
PZR RLF TK TO GAS ANALZ	8024	8025	68-308	68-307	X	X						X			X	X		X	X				87-87	87-88	ERCW-LOWER CNTMNT CLRS
AUXILIARY FEEDWATER LOOP 1				CK VLV		X					X				X	X		X					87-97	87-91	ERCW-LOWER CNTMNT CLRS
AUXILIARY FEEDWATER LOOP 2				CK VLV		X					X				X	X							87-95	87-96	ERCW-LOWER CNTMNT CLRS
AUXILIARY FEEDWATER LOOP 3				CK VLV		X					X				X	X		X					87 105	87-99	ERCW-LOWER CNTMNT CLRS
AUXILIARY FEEDWATER LOOP 4				CK VLV		X					X				X	X		X					87-103	87-104	ERCW-LOWER CNTMNT CLRS
FLOOR SUMP PUMP DISCHARGE			77-127	77-128	X	X						X			X	X		X	X				67-113	87-107	ERCW-LOWER CNTMNT CLRS
						X									X	X		X					87-111	87-112	ERCW-LOWER CNTMNT CLRS
TO RC PUMP SEALS	8348A		CK VLV			X	X						X			X			X				31-308	31-305	CW-INSTR ROOM CLRS
TO RC PUMP SEALS	8348B		CK VLV			X	X						X			X			X				31-308	31-309	CW-INSTR ROOM CLRS
TO RC PUMP SEALS	8348C		CK VLV			X	X						X			X			X				31-327	31-328	CW-INSTR ROOM CLRS
TO RC PUMP SEALS	8348D		CK VLV			X	X						X			X			X				31-329	31-330	CW-INSTR ROOM CLRS
FROM RC PUMP SEAL	8112	8100	62-61	62-63	X	X						X		X	X	X		X	X				CK VLV	67-141	ERCW-UPPER CNTMNT CLRS
RC DR TK & PRI TO VENT HDR	9160A	9160B	77-18	77-19	X	X						X		X		X		X	X				CK VLV	87-136	ERCW-UPPER CNTMNT CLRS
RC DRAIN TK PUMP DISCHARGE	9170	1003	77-9	77-10	X	X						X			X	X		X	X				CK VLV	87-133	ERCW-UPPER CNTMNT CLRS
GLYCOL OUT	9777	9775	81-194	81-193	X	X					*	X			X	X		X	X				CK VLV	87-130	ERCW-UPPER CNTMNT CLRS
GLYCOL IN	9773	9771	81-192	81-191	X	X						X			X	X		X	X				67-298	87-142	ERCW-UPPER CNTMNT CLRS
CONTAINMENT SPRAY		9001B	CK VLV	72-2		X				X				X	X	X	X	X					67-297	67-139	ERCW-UPPER CNTMNT CLRS
CONTAINMENT SPRAY		9001A	CK VLV	72-38		X				X				X	X	X	X	X					67-294	67-134	ERCW-UPPER CNTMNT CLRS
RHR SPRAY		9026A	CK VLV	72-40		X				X				X	X	X	X	X					67-295	67-131	ERCW-UPPER CNTMNT CLRS
RHR SPRAY		9026B	CK VLV	72-41						X					X		X								
RCP THERMAL BARRIER RETURN			70-87	70-90	X	X							X	X	X	X		X		X	8048	8028	CK VLV	81-12	PRIMARY WATER MAKE-UP
RCP THERMAL BARRIER SUPPLY			CK VLV	70-134	X									X		X		X							
SIS PUMP B-B DISCHARGE	8905BBD	8802B	CK VLV	63-157		X				X					X			X					CK VLV		DEMINERALIZER WATER
CCS FROM RC PUMP OIL COOLERS			70-89	70-92	X	X							X		X			X					CK VLV		SERVICE AIR
EXCESS LETDOWN HX SUPPLY				70-143		X	X					X			X	X	X	X		X			90-108,109	90-107	CNTMT BLDG LWR COMPT AIR MON
						X									X		X			X			90-110	90-111	CNTMT BLDG LWR COMPT AIR MON
SIS PUMP A-A DISCHARGE	8905ABC	8802A	CK VLV	63-158		X				X				X	X		X	X		X			90-114,115	90-113	CNTMT BLDG UPR COMPT AIR MON
FEEDWATER				CK VLV		X	X								X		X			X			90-116	90-117	CNTMT BLDG UPR COMPT AIR MON
FEEDWATER				CK VLV			X																		
FEEDWATER				CK VLV			X																		
FEEDWATER				CK VLV			X																		

PROCEDURE FOR USING TABLE

1. FIND PENETRATION IN LIST 1 OR LIST 2.
2. FOR THE PENETRATION IN LIST 1, PLACE TVA VALVE NUMBER IN THE COLUMN THAT READS "TVA VALVE FCV-NO. (LIST 1)".
3. THE SAME PROCEDURE IS APPLICABLE FOR WESTINGHOUSE VALVE NUMBER FOUND IN LIST 1.
4. NEXT, DETERMINE IF THE ISOLATION VALVE IS CLASS I, CLASS II, CLASS III OR CLASS IV (SEE ILLUSTRATIONS GIVEN OF THESE FOUR CLASSES).
5. IF PENETRATION IS IN LIST 1, PLACE THE SYMBOL "X" IN LIST 1 OF APPROPRIATE CASE. PLACE THE SYMBOL "X" IN LIST 2 IF FROM PENETRATION LIST 2.
6. THE SAME PROCEDURE IS USED FOR THE REMAINING INFORMATION COLUMNS.





Amendment 89

WATTS BAR
FINAL SAFETY
ANALYSIS REPORT

POWERHOUSE
UNITS 1 & 2
ELECTRICAL
LOGIC DIAGRAM
CONTAINMENT ISOLATION
TVA DWG NO. 1-47W611-88-1 R9
FIGURE 7.3-3-4

PROCADAM MAINTAINED DRAWING
THIS CONFIGURATION CONTROL DRAWING IS MAINTAINED BY THE WBN CAD UNIT AND IS NOW PART OF THE TVA PROCADAM DATABASE

Figure 7.3-3-SH-4 Powerhouse Units 1 & 2 Logic Electrical Diagram for Containment Isolation

7.4 SYSTEMS REQUIRED FOR SAFE SHUTDOWN

The functions necessary for safe shutdown are available from instrumentation channels associated with major systems in both the primary and secondary of the nuclear steam supply system (NSSS). These channels normal alignment to serve a variety of operational functions, including startup and shutdown as well as protective functions. There are no systems identified strictly as “safe shutdown systems.” However, procedures can institute appropriate alignment of selected systems to secure and maintain the plant in a safe condition. Other sections of the FSAR contain discussions of these systems with applicable codes, criteria and guidelines. Discussions in Chapter 6 and Section 7.3 involve alignment of shutdown functions associated with engineered safety features under postulated limiting fault situations.

Discussed in this section is the minimum number of instrumentation and control (I&C) functions required for maintaining safe shutdown of the reactor. These functions permit the necessary operations that will:

(1) Prevent the reactor from achieving criticality in violation of the technical specifications and

(2) Provide an adequate heat sink such that design and safety limits are not exceeded.

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:

(1) Boration

(2) Adequate supply for auxiliary feedwater (AFW)

(3) Residual heat removal

These systems are identified in the following sections together with the associated I&C provisions. The sections identify those monitoring indicators (Section 7.4.1.1) and controls (Section 7.4.1.2) necessary for maintaining hot standby. The equipment required for cold shutdown is identified in Section 7.4.1.3.

7.4.1.1 Monitoring Indicators

Indicators for the following process functions are provided both inside and outside the main control room (MCR). The indicators satisfy monitoring the four capabilities for maintaining a safe shutdown.

(1) Water level indicator for each steam generator

(2) Pressure and saturation temperature indicator for each steam generator

(3) Pressurizer water level indicator

(4) Pressurizer pressure indicator

(5) Source range neutron flux

(6) Reactor coolant system hot leg temperature

(7) Auxiliary feedwater flow to each steam generator

(8) Essential raw cooling water header flow

(9) Charging pumps discharge header pressure and flow

(10) Letdown heat exchanger outlet temperature

(11) Emergency boration flow

(12) Component Cooling System (CCS) flow to miscellaneous equipment

(13) CCS surge tank level

(14) CCS pumps discharge header pressure

(15) Volume control tank level

7.4.1.2 Controls

Controls provide the hardware and logic to shutdown the reactor and to maintain the plant in shutdown condition.

7.4.1.2.1 General Considerations

The following lists actions (including possible locations) and considerations that are prerequisites to alignment of systems for safe shutdown.

(1) The turbine is tripped (this can be accomplished at the turbine as well as in the MCR).

(2) The reactor is tripped (this can be accomplished at the reactor trip switchgear as well as in the MCR).

(3) Automatic systems continued functioning (discussed in Sections 7.2 and 7.7).

(4) Equipment listed in Sections 7.4.1.2.2, 7.4.1.2.3 and 7.4.1.2.4 have motor controls outside the MCR. These controls have a selector switch which transfers control of the switchgear from the MCR to its auxiliary control station(s). Placing the local selector switch in the auxiliary operating position will give an alarm in the MCR.

7.4.1.2.2 Pumps and Fans

The following pumps and fans provide safe shutdown functions:

(1) Auxiliary feedwater pumps

In the event of a main feedwater pump stoppage due to a loss of electrical power, the AFW pumps, which are powered from the emergency diesel generator (EDG), start automatically or can be started manually from inside the MCR. Additionally, the turbine driven AFW pump starts automatically or can be started manually from either the MCR or locally.

(2) Charging and boric acid transfer pumps

Start/stop motor controls provided for both the centrifugal charging pumps (CCPs) and the boric acid transfer pumps are located in the MCR and at the pump switchgear for the CCP and at the pump for the boric acid transfer pumps.

(3) Essential raw cooling water pumps

These pumps, which are powered by the EDGs, sequence automatically following a loss of normal electrical power. Start/stop motor controls are located in the MCR and at the electrical switchgear.

(4) Component cooling water pumps

These pumps, energized from the EDGs, start automatically following a loss of normal electrical power. Start/stop controls are located in the MCR and at the electrical switchgear.

(5) Auxiliary control air compressors

These compressors start automatically on low air pressure.

(6) Reactor containment fan cooler units

Start/stop motor controls with a selector switch are provided for the fan motors. The controls are located in the MCR and at the electrical switchgear.

7.4.1.2.3 Diesel Generators

These units start automatically following a loss of normal AC power. However, manual controls for diesel startup are provided locally (normal start only not emergency start) at the EDGs as well as in the MCR and auxiliary control room (ACR)).

7.4.1.2.4 Valves and Heaters

The following valves and heaters provide safe shutdown actions:

(1) Charging flow control valves

Manual control for the charging line flow control valves are provided in both the MCR and the ACR.

(2) Letdown orifice isolation valves

Open/close controls with a selector switch for the letdown orifice isolation valves are provided both in the MCR and the ACR.

(3) AFW control valves

(4) Automatic and manual control for the AFW control valves are located in both the MCR and the ACR for valves associated with the motor driven pumps or at the turbine pump room for valves associated with the turbine driven pump.Steam dump/atomospheric steam dump

Automatic and manual control for the condenser steam dump is provided in the MCR. Condenser steam dump is blocked on high condenser pressure. Atmospheric steam dump (ASD), in the form of SG PORVs, has automatic and manual control in both the MCR and ACR. Additionally, ASD has manual pneumatic controls locally located.

(5) Pressurizer heater control

On-off control with selector switch is provided for two backup heater groups. The heater groups are connected to separate buses, such that each can be connected to separate diesels in the event of loss of outside power. The control is both in the MCR and at the switchgear.

Instrumentation and controls listed in Sections 7.4.1.1 and 7.4.1.2 used to achieve and maintain safe shutdown (hot standy) can also be used for an evacuation of the MCR. Through the use of suitable procedures, these I&C channels together with the equipment identified in Section 7.4.1.3, available for the hot standby and cold shutdown, constitute the body of equipment potentially available to achieve cold shutdown after an MCR evacuation

7.4.1.3 Equipment and Systems Available for Cold Shutdown

(1) Reactor coolant pumps (See Chapter 5)

(2) Auxiliary feedwater pumps (See Chapter 10)

(3) Boric acid transfer pumps (see Chapter 9)

(4) Charging pumps (See Chapter 9)

(5) Service water pumps (Emergency raw cooling water pumps) (See Chapter 9)

(6) Containment fans (See Chapter 9)

(7) Control room ventilation (See Chapter 9)

(8) Component cooling pumps (See Chapter 9)

(9) Residual heat removal pumps (see Chapter 5)

(10) Class 1E power systems (See Chapter 8)

(11) Controlled steam release and feedwater supply (See Section 7.7 and Chapter 10)

(12) Boration capability (See Chapter 9)

(13) Nuclear instrumentation system (source range or intermediate range) (See Section 7.2 and 7.7)

(14) Reactor coolant inventory control (charging and letdown) (See Chapter 9)

(15) Pressurizer pressure control including opening control for pressurizer relief valves (PORVs Heaters and Spray) (See Chapter 5)

To achieve cold shutdown, the safety injection signal trip circuit must be defeated and the accumulator isolation valves closed.

7.4.2 Analysis

Hot standby is a stable plant condition, automatically attained 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 MCR is restricted, the plant can be safely kept at hot standby until the control room can be reentered by the use of the indicators and controls listed in Sections 7.4.1.1 and 7.4.1.2 until the MCR can be reentered. These indicators and controls are provided outside as well as inside the MCR.

The safety evaluation for maintaining shutdown with these systems and associated instrumentation and controls includes consideration of the accident consequences that might jeopardize safe shutdown conditions. The germane accident consequences are

those that would tend to degrade the capabilities for boration, adequate supply for auxiliary feedwater, or residual heat removal.

Instrumentation and controls for these systems may require some realignment in order that their functions may be performed from outside the MCR. Procedures for realignment of these controls and instruments are prepared in advance, upgraded as necessary, and available when needed. Note that the reactor plant design does not support attaining the cold shutdown condition from outside the MCR. An assessment of plant conditions can be made on the long term basis to establish the necessary physical realignment to I&C equipment in order to attain cold shutdown. During such time the plant could be safely maintained at hot standby condition.

The I&C functions which are required to be aligned for maintaining safe shutdown of the reactor that are discussed above and are the minimum number of I&C functions under non-accident and nontransient conditions. Some of the equipment that provides some of these I&C functions are control systems discussed in Section 7.7 that are not part of the protection system. Proper operation of the control systems will allow a safe shutdown to be attained and maintained by preventing a transient. In considering more restrictive conditions than Section 7.4 examines, certain accidents and transients are postulated in Chapter 15.0 safety analyses which take credit for safe shutdown when the protection system's reactor trip terminates the transient and the engineered safety features system mitigates the consequences of the accident. In these transients, in general, no credit is taken for the operation of control systems listed in Section 7.7 should such operation mitigate the consequences of a transient. Should such operation not mitigate the consequences of a transient, no penalties are taken in the analyses for incorrect control system actions over and above the incorrect action of the control system whose equipment failure was assumed to have initiated the transient. The Chapter 15.0 analyses show that safety is not adversely affected when a limited number of such transients are postulated. Such transients include the following:

(1) Uncontrolled boron dilution

(2) Loss of normal feedwater

(3) Loss of external electrical load and/or turbine trip

(4) Loss of AC power to the station auxiliaries (station blackout).

REFERENCES

None

THIS PAGE INTENTIONALLY BLANK

7.5 INSTRUMENTATION SYSTEMS IMPORTANT TO SAFETY

7.5.1 Post Accident Monitoring Instrumentation (PAM)

7.5.1.1 System Description

Post Accident Monitoring (PAM) instrumentation is required to monitor plant and environs conditions during and following design basis Condition II, III and IV faults as described in FSAR Chapter 15. PAM instrumentation will enable the Main Control Room (MCR) operating staff (operator) to take preplanned manual actions, provide information on whether critical safety functions are being accomplished, provide information for potential or actual breach of the barriers to fission product release, provide information of individual safety systems, and provide information on the magnitude of the release of radioactive materials.

Table 7.5-2 lists the process information required at the initiation of an accident. The variables' descriptions were selected through a systematic evaluation of parameters required for the mitigation of design basis events at Watts Bar, a comprehensive review of the Emergency Instructions (EIs), Function Restoration Guidelines (FRGs), and Condition II, III and IV faults in Chapter 15 of the FSAR. In some cases, the EIs and FRGs address mitigation of events which may extend beyond the design of the plant. Instrumentation used for beyond design basis events may be exempted from being PAM instrumentation. Table 7.5-2 furnishes the appropriate variable classification types/categories for each variable description. PAM variable types/categories were determined using the guidance given in U.S. NRC Regulatory Guide 1.97, R2[1] and General Design Criteria for Nuclear Power Plants[12].

7.5.1.2 Variable Types

Five (5) classifications of variable types, A, B, C, D and E, were identified to provide the PAM instrumentation. These classifications meet the PAM classifications contained in Regulatory Guide 1.97, R2. These five classifications are not mutually exclusive, in that a given variable (or instrument) may be included in one or more types. When a variable is included in one or more of the five type classifications, the equipment monitoring this variable meets the most stringent category qualification requirements as noted in Table 7.5-1. Type A variables provide primary information to the operators to allow them to take preplanned manually controlled actions to mitigate the consequences of a Chapter 15 design basis event. Types B, C, D and E are variables for following the course of an accident and are to be used (1) to determine if the plant is responding to the safety measures in operation and (2) to inform the operator of the necessity for unplanned actions to mitigate the consequences of an accident should plant conditions evolve differently than predicted by Chapter 15.

Type A Variables

Those variables that provide primary information to the MCR operators to allow them to take preplanned manually controlled actions for which no automatic action is provided and that are required for safety systems to accomplish their safety functions

for Chapter 15 design basis events. Primary information is information that is essential for the direct accomplishment of specified safety functions.

Type B Variable

Those variables that provide information to monitor the process of accomplishing critical safety functions. Critical safety functions are those safety functions which are essential to prevent a direct and immediate threat to the health and safety of the public. These are defined as reactivity control, core cooling, maintaining reactor coolant system integrity, and maintaining containment integrity (including radioactive effluent control).

Type C Variable

Those variables that provide information to indicate the potential for breaching or the actual breach of the barriers to fission product release (including high level radioactive release through identifiable release points, i.e., plant vents). The barriers to fission product release are fuel cladding, reactor coolant pressure boundary and primary reactor containment.

Type D Variable

Those variables that provide information to indicate the operation of individual safety systems and other plant systems. These variables are to help the operator make appropriate decisions in using the individual systems in mitigating the consequences of an accident.

Type E Variable

Those variables used in determining the magnitude of the release of radioactive materials and for continuously assessing such releases.

7.5.1.3 Variable Categories

The five types of variables are functionally classified into three (3) qualification categories (1, 2, and 3) according to the safety function provided by the variable. Descriptions of the three categories are given below. Table 7.5-1 briefly summarizes the qualification criteria of the three designated categories.

The differentiation in the 3 categories was made in order that importance of information hierarchy could be recognized in specifying accident monitoring instrumentation. Category 1 instrumentation has the highest pedigree and should be utilized for information which is essential to the main control room operating staff in order for them to determine if the plant critical safety functions are being performed. Category 2 and 3 instruments are of lesser importance in determining the state of the plant and do not require the same level of operational assurance.

The primary differences between category requirements are in the qualification, application of single failure, power supply, and display requirements.

7.5.1.4 Design Bases

7.5.1.4.1 Definitions

Primary Information

Primary information is information that is essential for the direct accomplishment of the specified functions; it does not include those variables that are associated with contingency actions that may also be identified in written procedures.

Key Variable

A key variable is that single variable (or minimum number of variables) that provides primary information and most directly indicates the accomplishment of a safety function (in the case of Types B and C) or the operation of a safety system (in the case of Type D) or radioactive material release (in the case of Type E).

Backup Variable

Additional variables beyond those classified as key that provide diagnostic or confirmatory information.

Diverse Variable

Where failure of a Category 1 channel results in information ambiguity that can lead the operator to defeat or fail to accomplish a required safety function, a second variable shall be identified to allow the operators to deduce the actual condition in the plant. The second variable, qualified identically to the first, is called a diverse variable and bears a known relationship to the multiple channels of the key variable.

Diverse variables are identified in Table 7.5-2.

7.5.1.4.2 Selection Criteria

Type A variables are key variables and are designated Category 1.

Type B and C variables are determined to be either key or backup variables depending on their particular usage. Those variables determined to be key shall be classified as Category 1 except for those classified as Category 2 in accordance with the specific guidance presented in Regulatory Guide 1.97, R2, Table 2. Backup variables are considered Category 3.

The Type D and E variables determined to be key are classified as Category 2 except for those classified as Category 1 in accordance with the specific guidance presented in Regulatory Guide 1.97, R2, Table 2. Backup variables are considered Category 3.

The variable types were determined through (1) the guidance given in Regulatory Guide 1.97 R2, Table 2, (2) a review of the Emergency Instruction and Function Restoration Guidelines and, (3) a safety analysis performed for the FSAR Chapter 15 design basis accidents. These three steps insure that sufficient instrumentation is available to the operator to keep the plant in a safe condition under accident scenarios.

7.5.1.4.3 Design Criteria For Category 1 Variables

(A) Redundant Class 1E qualified continuous indication of these variables has been provided. Qualification applies from the sensor to the display. The variables have been provided with a minimum of two independent channels (PAM 1 and PAM 2) for monitoring each variable. These two redundant channels allow the operator to deduce actual plant conditions.

Where failure of a channel would present ambiguous or confusing information to the operator, preventing the operator from taking action or misleading the operator, an additional redundant (PAM 3) channel has been provided. The PAM 3 channel has been qualified to the same requirements as the first two channels. Table 7.5-2 lists the redundancy requirements for each Category 1 variable.

(B) PAM instrumentation has components and cables environmentally qualified and installed to function in plant conditions for which they are expected to operate. Qualification is in accordance with 10 CFR 50.49 requirements.

(C) PAM instrumentation continues to function after a design basis seismic event in accordance with Watts Bar Nuclear Plant Design Criteria.

(D) Transmission of signals from PAM Category 1 devices to non-qualified equipment is only through an isolation device qualified to Category 1 requirements. No credible failure at the output of the isolation device prevents the monitoring channel from meeting its minimum performance requirements.

(E) Category 1 instrumentation supplied from Class 1E standby power sources is capable of operating independently of offsite power, and backed up by batteries. The physical separation between redundant channels has been preserved in field wiring by combining outputs from Train A or channels from instrumentation cabinets I or III into the PAM 1 channels. The redundant PAM 2 channels are from Train B or channels from instrumentation cabinets II or IV. PAM 3 channels are physically separated from both PAM 1 and PAM 2 channels.

(F) Category 1 analog variables have at least one of the redundant instrument loops recorded on the Emergency Response Facilities Data System (ERFDS) computer. In addition to the ERFDS computer, a hardwired recorder for at least one instrument loop of the variable has been provided when trending of the Category 1 variable enhances the operator's ability to cope with mitigating various design basis events.

(G) Category 1 variables follow quality assurance requirements as described in FSAR Chapter 17 for safety related devices.

7.5.1.4.4 Design Criteria For Category 2 Variables

(A) Redundant or Class 1E circuitry is not required for Category 2 variables. However, the parent system may require the instrumentation to be classified Class 1E for non-PAM functions. Where this instrumentation has been used to provide PAM Category 2 indication, the Class 1E qualification applies from the sensor through the isolator/buffer. The display need not meet Class 1E requirements.

(B) PAM instrumentation has components and cables environmentally qualified and installed to the plant conditions for which they are expected to operate. Nondivisional and Class 1E PAM instrumentation located in a harsh environment has been qualified in accordance with 10 CFR 50.49 requirements. Mild environment Category 2 components do not have any special qualification requirements.

(C) There are no specific requirements for seismic operability. However, specific system requirements above that required for post accident monitoring may exist. In those cases, the most restrictive qualification level applies. In addition, components are designed and mounted such that they do not have an adverse effect on safety systems during a seismic event.

(D) Category 2 instruments are powered from highly reliable power sources, not necessarily divisional power, and are diesel generator or battery backed.

(E) Potential plant release point effluent radioactivity monitors and area radiation monitors are trended on a MCR recorder or on the ERFDS computer.

(F) Category 2 instrumentation located in a harsh environment follows quality assurance requirements as described in FSAR Chapter 17 for safety related devices.

7.5.1.4.5 Design Criteria For Category 3 Variables

(A) Category 3 PAM instrumentation is high-quality commercial grade equipment. No redundancy, qualification, or signal isolation is required.

(B) Category 3 PAM loops are powered from normal station power supplies, such as nondivisional power.

(C) Components are designed and mounted such that they do not have an adverse effect on safety systems during design basis seismic events. Instruments that are not part of a safety related system are not seismically qualified unless the Watts Bar FSAR specifies seismic requirements for the associated system.

(D) The meteorology monitors are trended on the ERFDS computer.

7.5.1.5 General Requirements

7.5.1.5.1 Display Requirements

Category 1 parameters are displayed on individual devices located in the main control room.

Category 2 and 3 devices are either displayed on individual instruments located in the main control room or processed for display by one of the computer-based systems available in the MCR except as described below.

Portable or postaccident sampling devices are not displayed in the main control room. In addition, a limited number of Category 2 and 3 devices are displayed on local panels if the following guidelines are met:

(1) The information displayed is of a non-critical or non-diagnostic nature.

(2) The local panel display is accessible under accident conditions.

(3) The information can be retrieved in a time frame necessary to support the operator's actions.

(4) The parameter changes slowly such that only infrequent updates are needed.

Human factors principles have been used in determining the types and locations of the displays. To the extent practical, the same instruments are used for accident monitoring as are used for the normal operations of the plant. This enables the operators to use instruments with which they are most familiar during accident situations. Monitoring instrumentation is from sensors that directly measure the desired variables. Indirect measurements are made only when it can be shown by analysis to provide equivalent or unambiguous information. The PAM parameters have associated required accident ranges. The minimum required ranges are given in Table 7.5-2. The range of the instrumentation is sufficient to keep the indication on scale at all times. Where the required range of monitoring instrumentation results in a loss of instrumentation sensitivity or accuracy in the normal operating range by using a single instrument (such as radiation monitors), multiple instruments are used to encompass the entire required range. Where two or more instruments are needed to cover a particular range, overlapping of instrument spans and accuracies has been provided to ensure one of the two instruments will be on scale at all times.

7.5.1.5.2 Identification

The Category 1 and 2 displays are uniquely identified on the main control board so that the operator can easily discern that they are intended for use under accident conditions. PAM Category 1 display devices have been identified with a nameplate with black background, white letters and the symbol "C1" inscribed on the nameplate. PAM Category 2 display devices (which are not also PAM Category 1) have been

identified with a nameplate with a white background, black letters with the symbol "C2" inscribed on the nameplate.

Category 1 indicators are identified on the control diagrams as P1 and P2 (as well as P3 when a third redundant channel is required) to denote each redundant train of instrumentation. Category 1 and 2 components are identified as such in the Instrument Tabulation drawings. Applicable Category 1 and 2 components are identified in the 10CFR50.49 List.

7.5.1.6 Analysis

For Condition II, III and IV events sufficient duplication of information is provided to ensure that the minimum information required is available. The information is part of the operational monitoring of the plant which is under surveillance by the operator during normal plant operation. This is functionally arranged on the main control board to provide the operator with ready understanding and interpretation of plant conditions.

Redundant sensors are provided to develop the necessary information to enable the required manual functions to be performed following a Condition IV event. These sensors are environmentally and seismically qualified.

Range and accuracy requirements are determined through the analysis of Condition II, III, or IV events as described in FSAR Chapter 15. The display system meets the following requirements:

(a) The range of the readouts extends over the maximum expected range of the variables being measured.

(b) The combined indicated accuracies are within the errors used in the safety analysis.

Other information systems such as the emergency response facilities data system are integrated with the PAM instrumentation described in this section. In order to provide the operator adequate information to prevent and/or cope with events, those displays have been included in the Human Factors engineering review.

As described throughout FSAR Section 7.5, WBN meets the intent of Regulatory Guide 1.97, R2. Deviations from the Regulatory Guide have been identified to the NRC.[9, 10, 11, 13, 14, 15, 16] The deviation numbers are given in the notes column of Table 7.5-2 and correspond to the deviation numbers in the above references.

7.5.1.7 Tests and Inspections

7.5.1.7.1 Programs

Services, testing and calibration programs are specified to maintain the capability of the monitoring instrumentation. For those instruments where the required interval between testing is less than the normal interval between station shutdowns, capability for testing during operation is provided.

7.5.1.7.2 Removal of Channels from Service

Whenever a means for removing channels from service is included in the design, the design facilitates administrative control for such removal. The system is designed to permit at least one channel to remain operable when required during power operation. During removal from service, the active parts of the channel need not continue to meet the single failure criteria. As such, monitoring systems comprised of two redundant channels are permitted to violate the single failure criterion during channel bypass. The bypass time interval allowed for a maintenance operation is specified in the plant technical specifications.

7.5.1.7.3 Administrative Control

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

7.5.2 Emergency Response Facilities Data System (ERFDS)

The ERFDS acquires, processes, and displays all data to support the assessment capabilities of the MCR, Technical Support Center (TSC) and the Emergency Operation Facility (EOF) as stated in NUREG - 0696[2] and NUREG - 0737, Supplement 1[3]. The ERFDS also provides the safety parameter display system and the bypassed and inoperable status indications system for WBN.

Each unit has its own ERFDS running on a real time data acquisition and analysis computer system. This computer system also drives display equipment in the Technical Support Center (TSC) and provides plant data to the off-site computer located at the Emergency Operations Facility (EOF).

The operators use a keyboard and/or touch screen to request additional detailed information about the parameters used to determine the Critical Safety Functions (CSF) status as well as other plant conditions. This information is provided in three formats: mimic, tabular, and trend displays.

The data undergoes several validation steps before being presented to the operators. When redundant sensors are used, the data received by the computer can be processed by software to determine if the quality of one or more points is questionable.

7.5.2.1 Safety Parameter Display System

7.5.2.1.1 System Description

The principal purpose and function of the Safety Parameter Display System (SPDS) is to aid control room personnel during abnormal and emergency conditions in determining the safety status of the plant and in assessing if abnormal conditions require corrective action by the operators to avoid a degraded core. During emergencies the SPDS serves as an aid to evaluating the current safety status of the plant, executing function-oriented emergency procedures, and monitoring the impact of engineered safeguards or mitigation activities. The SPDS also operates during

normal operations, continuously displaying information from which the plant safety status can be readily and reliably accessed.

Each of the unit's SPDS has at least two color graphic cathode-ray tube (CRT) monitors in the main control room which continuously display information on the CSF.

7.5.2.1.2 Design Bases

Location of SPDS

The SPDS is conveniently located in the control room on at least two CRTs for use by the control room operating staff.

Although both of these terminals are expected to be operational, only one is required to be operational in order for the SPDS to be considered available.

Continuous and Reliable Display of Plant Safety Status Information

The SPDS displays information from which the plant safety status can be readily and reliably assessed by control room personnel responsible for the avoidance of degraded and damaged core events. This is accomplished by presenting the status of each CSF on every SPDS display. The status of the CSF is indicated on all ERFDS displays by use of a target on each screen. Redundant sensor algorithms are used to aid the operators in determining if display information is reliable.

The quality of the information is identified as being good, poor, bad, or manually entered. Data is tagged as poor if it is inconsistent with redundant sensors. Data is tagged as bad if it is outside the process sensor limits, or data acquisition system span, or because hardware checks indicated a malfunctioning input device. Data is tagged as manually entered when the value is operator entered. If a point is not poor, bad, or manually entered it is considered good. Calculated-points are tagged as poor if any of their constituent points are not good.

The SPDS software and changes undergo formal verification and validation. Software changes are documented, approved, and controlled by qualified personnel and procedures.

Concise Display of Critical Plant Variables

The SPDS provides a concise display of critical plant variables which provide information to plant operators about the following critical safety functions:

(a) Reactivity control

(b) Reactor core cooling and heat removal from the primary system

(c) Reactor coolant system integrity

(d) Radioactivity control

(e) Containment conditions

When the SPDS logic determines the plant may not be in a safe condition, the operator is informed of the problem. After the SPDS indication is verified to be correct, the operator is directed to follow appropriate recovery procedures.

Human Factors

Human factors are taken into account in the design of the SPDS. Color coding is used to inform operators of the severity of SPDS alarm conditions. Page keys are used to page up, down, left and right. Alarms are acknowledged with keystrokes at any control room SPDS keyboard.

Additional information is presented to control room personnel in numeric format, numeric displays, deviation barcharts, and trend displays.

Electrical and Seismic Qualification

The SPDS is not class 1E qualified and is not powered from a class 1E power source. As such, the SPDS is electrically isolated from equipment and sensors used in safety systems.

The SPDS equipment including display hardware has three power sources:

Normal: Common board AC power rectified and inverted to 120V AC
Alternate: Station battery 250V DC inverted to 120V AC
Maintenance: Regulated 120V AC from 480V AC station unit board

The hard copy equipment does not have to be powered by uninterruptable power.

The SPDS is not required to operate during or after a seismic event. SPDS equipment is designed so that it will not adversely affect any equipment important to safety, either during or after a seismic event.

7.5.2.2 Bypassed and Inoperable Status Indication System (BISI)

WBN fully complies with the intent of RG 1.47, Revision 0[5].

The BISI system is a computer based system that provides automatic indication and annunciation of the abnormal status of each ESFAS actuated component of each

redundant portion of a system that performs a safety-related function. The determination of the bypassed or inoperable status of a system is left up to the reactor operator.

Abnormal status indication may be applied administratively by the control room operators or automatically from monitored equipment.

Compliance with Regulatory Guide 1.47 is described below:

(1) An abnormal indication is provided for each safety system. Abnormal includes any deliberate action which renders a protection system inoperable. The following systems are monitored:

main and auxiliary feedwater
safety injection
residual heat removal
containment spray
emergency gas treatment
essential raw cooling water
chemical and volume control
heating, ventilation, and air conditioning
component cooling
control air (including auxiliary control air)
standby diesel generator

(2) Support system indication is provided for each safety system that requires auxiliary or support system(s) operation to perform its safety function.

(3) The indicators are at the system level with separate indication for each train.

(4) Sublevel information is provided to the control room operator for determination of the abnormal condition at the component level.

(5) The abnormal indicators are operated automatically by actions which meet all of the following criteria:

(a) The action is deliberate. It is not the intent of the system to show operator errors or component failures.

(b) The action is expected to occur more often than once a year.

(c) The action is expected when the protection system must be operable per technical specifications.

(d) The action renders the system inoperable, not merely potentially inoperable.

(e) The deliberate action has taken place in the safety system or a necessary supporting system.

(6) The abnormal indication is separate from other plant indicators.

(7) A manual capability is provided to operate each safety system abnormal indication. This allows the operator to activate abnormal indication for an event that renders a safety system inoperable but does not automatically operate the BISI.

(8) Abnormal indication is accompanied by an audible alarm.

(9) There is no capability to defeat an automatic operation of an abnormal indication. (However audible alarms may be silenced.)

(10) The indication system is mechanically and electrically isolated from the safety system to avoid degradation of the safety system. The BISI is not safety-related; i.e., it is not designed to safety system criteria such as IEEE Standard 279-1971[6].

(11) In accordance with IEEE-279-1971, Paragraph 4.20[6], the operator must be able to determine why a system level abnormal status is indicated. This information can be accessed by the operator for display.

(12) Essential raw cooling water and diesel generator systems abnormal status indication are provided. These (support) systems are unique and important enough to warrant abnormal status indication.

(13) The system design meets the recommendations of ICSB-21[8] as follows:

(a) Each safety system has a Train A and Train B bypass indicator. Support systems are arranged together with the associated train of

bypass indicators. Safety system indicators are lit whenever any support subsystem is abnormal.

(b) Means by which the operator can cancel erroneous bypassed indications are not provided.

(c) The BISI system does not perform functions essential to safety. No operator action is required based solely on the abnormal status indication.

(d) The BISI system has no effect on plant safety systems.

(e) The abnormal status indicating and annunciating function can be tested during normal plant operation.

7.5.2.3 Technical Support Center and Nuclear Data Links

7.5.2.3.1 Technical Support Center

The information available includes the SPDS displays as well as special displays for use in the TSC. The display is similar to the main control room and the software and man/machine interface is the same.

7.5.2.3.2 Communication Data Links

The ERFDS provides a means of acquiring data from and supplying data to computer based systems both on and off site. The communications data links interconnect the following computer systems:

(1) Emergency Operations Facility (EOF)

In response to NUREG 0737 Supplement 1[3], all data (real and calculated) along with status and quality information is available for transmission by data link to a compatible processor capable of displaying the information in the EOF. Upon request ERFDS will send the Central Emergency Control Center (CECC) computer a dynamic data base snapshot (a maximum of 200 process variables) every 15 seconds over a high speed communications link. This data meets the requirements of NUREG-1394, Emergency Response Data System[7].

(2) Environmental Data Station (EDS)

Communications between the ERFDS and the EDS Computer allows the ERFDS to access variables that are input to the EDS computer. All EDS data required by RG 1.23[4] and required to support the TSC functions can be transmitted at a rate of once per minute and displayed with the radiation release data.

(3) Plant Computer

Communication between the plant computer and ERFDS is one way to the ERFDS to access any required points in the plant computer data base.

REFERENCES

(1) U. S. NRC Regulatory Guide 1.97, Rev. 2 (December 1980) and Rev. 3 (May 1983) "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident".

(2) NUREG 0696, Functional Criteria for Emergency Response Facilities, dated February 1981.

(3) NUREG-0737, Supplement 1, Requirements for Emergency Response Capability, Generic Letter 82-33, dated December 17, 1982.

(4) Regulatory Guide, 1.23, Onsite Meteorological Programs (Safety Guide 23) Revision 0.

(5) Regulatory Guide 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems, Revision 0.

(6) IEEE-Standard 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations (ANSI-N42.7-1972).

(7) NUREG-1394, Emergency Response Data System Implementation.

(8) Branch Technical Position ICSB-21, Guidance for Application of Regulatory Guide 1.47.

(9) TVA letter to NRC dated August 31, 1990, Watts Bar Nuclear Plant (WBN) Conformance to Regulatory Guide (RG) 1.97 Revision 2. (RIMS L44 900831 804)

(10) TVA letter to NRC dated October 29, 1991, Watts Bar Nuclear Plant WBN-Emergency Response Capability, Regulatory Guide 1.97, Revision 2 - Request for Additional Information Response. (RIMS T04 911029 848)

(11) NUREG-0847, Supplement 9, "Safety Evaluation Report Related to the Operation of Watt Bar Nuclear Plant, Unit 1 and 2," June 1992.

(12) "General Design Criteria for Nuclear Power Plant," Appendix A to Title 10 CFR 50, Criterion 13, 19, and 64.

(13) TVA letter to NRC dated May 9, 1994, Watts Bar Nuclear Plant (WBN) - Regulatory Guide (RG) 1.97, Revision 2, Postaccident Monitoring System (PAM) - Supplemental Response (RIMS T04 940509 901).

(14) TVA Letter to NRC dated April 21, 1995, Watts Bar Nuclear Plant (WBN) Units 1 & 2 - Regulatory Guide (RG) 1.97, Revision 2, Post-Accident Monitoring System (PAM) - Supplemental Response (RIMS T04 950421 117).

(15) TVA Letter to NRC dated July 18, 1995, Watts Bar Nuclear Plant (WBN) Units 1 and 2 - Regulatory Guide (RG) 1.97, Revision 2, Post-Accident Monitoring System (PAM) - Supplemental Response (RIMS T04 950718 165)

(16) TVA Letter to NRC dated October 12, 1995, Watts Bar Nuclear Plant (WBN) Units 1 & 2 - Regulatory Guide (RG) 1.97, Revision 2, Post-Accident Monitoring System (PAM) - Supplemental Response (T04 951012 228)

Table 7.5-1 Post Accident Monitoring Instrumentation Component Qualification Matrix (See Note)

Criteria	Category 1	Category 2	Category 3
Redundancy	At least 2 channels required	Not Required	Not Required
EQ (10 CFR 50.49)	Qualify Per WB-DC-40-54, components placed in 10CFR50.49 program	Qualify per WB-DC-40-54, components placed in 10CFR50.49 program	Not Required
Seismic	Must function after seismic event per WB-DC-40.31.2	Not Required	Not Required
QA	Yes	Yes-Equipment in harsh environment same as Category 1	Not required
Power Supply	Class-1E Per WB-DC-30-27	Non-Class 1E, diesel or battery-backed	Non-Class 1E
Physical Separation	Required per WB-DC-30-4	Not required	Not Required
Electrical Separation	Non-1E circuit interfaces are through qualified isolation devices. (See WB-DC-30-4)	Not required	Not Required
Indication	Hardwired indicator (RVLIS and CET use plasma display and recorder), light	Meter, indicator light,computer display, or annunciator window	Meter, indicator light, computer display, or annunciator window
Special Labeling on MCR Board	C1 engraved on MCR label or window	C2 engraved on MCR label or window.	Not Required
Testing and Maintenance	Required	Required	Required
Isolation Device Accessibility	Required	Required for loops with isolation devices	Not required
Recording	At least 1 channel per analog variable is recorded as indicated in Table 7.5-2. Recording is qualified to Category 2 requirements. The ERFDS has at least 1 channel per analog variable trended.	Effluent and area radiation monitors are recorded. Not required for others.	Recorder or computer for meteorology; not required for others

Note: These are only post accident monitoring requirements. Normal system requirements may impose more stringent qualification requirements on components selected for PAM use and in those cases the most stringent requirements are met.

Table 7.5-2 Regulatory Guide 1.97 Post Accident Monitoring Variables Lists Legend

Legend

The following table of variables provides a listing of specific design requirements for the PAM instruments. The table represents the minimum required to conform to Regulatory Guide (RG) 1.97, Revision 2. Additional qualification may be provided as a result of other plant, system, or design requirements. The topics de~cribed are:

- Variable Name
- Type and Category
- Redundant Channels
- Range, Range Units
- Notes

Type and Category

The variable's type(s) and associated category are identified. Entries in this column are derived from the Type selection analys~s and RG 1.97.

Redundancy -The number of instrument channels required to monitor the variable. For Category 1 variables, the number of channels is determined from the PAM single failure analysis. Diverse indication used to supplement or replace redundant information is also identified in Note 1.

Range -The required range and engineering units of the instrumentation are developed in the Type selection analyses or the required range and accuracy analysis. The radiation monitor ranges may reflect the interpreted range and not the equipment's scale.

Notes -Additional information is provided for clarification including any deviations from R.G. 1.97 R2. The deviations are found in references 9, 10, 11, 13, 14, 15, 16.

Table 7.5-2 Regulatory Guide 1.97 Post Accident Monitoring Variables Lists Legend (Page 1 of 14)

VAR NUM	VARIABLE NAME	TYPE/ CATEGORY	REDUNDANT CHANNELS	MINIMUM RANGE FROM	MINIMUM RANGE TO	RANGE UNITS	NOTES
1.	Auxiliary Feedwater Flow	A1 D2	P1 P20 2 channels Per Loop	0	700	GPM	(Note 1)
2.	Containment Lower Compartment Atmoshere Temperature	A1 D2	P1 P2 2 Channels	0	350	DEG F	Deviation #8
3.	Containment Pressure	215PSIG	4 Channels	-2	PSIG	15	Deviation #24 (Narrow Range) Note 9
4.	4Containment RadiationA1 C3 E1P1 P21Note 9	A1 C3 E1	P1 P2	2 Upper 2Lower	1.0E7	R/hr	Note 9 Deviation #36
5.	Containment Sump Level (Wide Range)	A1 B1 C1 D2	P1 P2	0	20	Ft	Deviation #32
6.	Core Exit Temperature	A1 B1 C1 D2	P1 P2 8 PAM 8 PAM 2	200	2300	Deg F	Minimum of 16 Operable Thermocouples, 4 from each quarant (note 1,9, 10) Deviation #30 & #37
.7	Main Steam Line Radiation	C2 E2	1 Channel per Steam Generator	1 0E 1	1.0E3	UCI/cc	Note 7

Table 7.5-2 Regulatory Guide 1.97 Post Accident Monitoring Variables Lists Legend (Page 2 of 14)

VAR NUM	VARIABLE NAME	TYPE/ CATEGORY	REDUNDANT CHANNELS	MINIMUM RANGE FROM	MINIMUM RANGE TO	RANGE UNITS	NOTES
8.	Nuclear Instrumentation	A1 B1 D2		P1 P2	1.0E6	CPS	Note 9
9.	RCS Pressurizer Level	A1 D1	P1 P2 P3	0	100	%	Note 9 & 12
10.	RCS Pressure Wide Range	A1 B1 C1 D2	p1 P2 P3	0	3000	PSIG	Note 9 & 12
11.	RCS Temperature T Cold	A1 B1 C1 D2	4 Channels 1 Per Loop	50	700	Deg F	Note 1 & 9 Deviation #1
12.	RCS Temperature T Hot	A1 D2	4 Channels 1 Per Loop	50	700	Deg F	Note 1 & 9 Deviation #1
13.	Refueling Water StorageTank Level	A1 D2	P1 P2	100	0	%	Note 9
14	Steam Generator Level (Narrow Range)	A1 B1	P1 P2 P3 3 Channels Per Steam Generator	0	100	%	Note 1, 9, 12
15	Steam Generator Pressure	A1 B1 D2	P1 P2 2 Channels Per SG	0	1300	PSIG	Notes 1 & 9 Deviation #3
16	Subcooling Margin Monitor	A1 B2 C1 D2	P1 P2	200	35	Deg F	200 Deg. Subcooling to 35 Deg. Superheat Notes 9 & 10

Table 7.5-2 Regulatory Guide 1.97 Post Accident Monitoring Variables Lists Legend (Page 3 of 14)

VAR NUM	VARIABLE NAME	TYPE/ CATEGORY	REDUNDANT CHANNELS	MINIMUM RANGE FROM	MINIMUM RANGE TO	RANGE UNITS	NOTES
17	Auxiliary Building Passive Sump Level	B1 C1	P1 P2	12.5	72.5	Inches	Note 9
18	Containment Isolation Valve Position Indication	B1 D2	1 Per Valve	Closed	Not Closed	N/A	Deviation #20
19	Containment Hydrogen Concentration	B1 C1 D2	P1 P2	0	10	%	Deviation #2
20	Control Rod Position	D3	1 Channel Per Bank	0	235	Steps	Deviation #35
21	Nuclear Instrumentation (Intermediate Range)	B1 D2	P1 P2	1.0E 8	200	%Power	Note 9
22	REACTOR VESSEL LEVEL	B1 C1 D2	P1 P2	See below			(See Notes 5, 9, & 10)

Table 7.5-2 Regulatory Guide 1.97 Post Accident Monitoring Variables Lists Legend (Page 4 of 14)

VAR NUM	VARIABLE NAME	TYPE/ CATEGORY	REDUNDANT CHANNELS	MINIMUM RANGE FROM	MINIMUM RANGE TO	RANGE UNITS	NOTES
22a	Static Mode			0	100	%	0% represents reactor (Pumps Not Running) vessel empty. 100% represents reactor vessel full.
22b	Dynamic Mode			20	100	%	100% represents (Pumps Running)reactor vessel full
23	Containment Pressure (Wide Range)	C1	P1 P2	-5	60	PSIG	Note 9
24	Shield Building Vent (Noble Gas Activity)	C2 E2	1 Channel	1.0E-6	1.0E4	uCi/cc	
25	ABGTS High Pressure Alarm Per Fan	D2	1 Channel	NA	-0.2	inch H_20	
26	ACAS Pressure	D2	1 Channel Per Train	0	150	PSIG	

Table 7.5-2 Regulatory Guide 1.97 Post Accident Monitoring Variables Lists Legend (Page 5 of 14)

VAR NUM	VARIABLE NAME	TYPE/ CATEGORY	REDUNDANT CHANNELS	MINIMUM RANGE FROM	MINIMUM RANGE TO	RANGE UNITS	NOTES
27	AFW Valve Status	D1	1 Channel Per Valve	Open	Closed	NA	
28	Accumulator Flow Isolation Valve Status	D3	1 Channel Per Valve	Open	Closed	NA	Deviation #16
29	Accumulator Tank Level	D3	1 Channel Per Tank	7632	8264	GAL	Deviation #15
30	Accumulator Tank Pressure	D3	1 Channel Per Tank	0	700	PSIG	Deviation #6
31	Annulus Pressure	D2	1 Channel	-10	0	inch H_20	
32	Aux. Feed Pump Turbine Steam Supply IsolationValve Status	D3	1 Channel Per Valve	Open	Closed	NA	
33	Battery Current (125VD21 dc Vital)	D2	1 Channel Per Battery	-200	+600	AMPS	
34	Bus Voltage (125V dc Vital)	D2	1 Channel Per Battery	75	150	VOLTS	
35	Bus Voltage (480V Shutdown)	D2	1 Channel Per Train	0	600	VOLTS	

Table 7.5-2 Regulatory Guide 1.97 Post Accident Monitoring Variables Lists Legend (Page 6 of 14)

VAR NUM	VARIABLE NAME	TYPE/ CATEGORY	REDUNDANT CHANNELS	MINIMUM RANGE FROM	MINIMUM RANGE TO	RANGE UNITS	NOTES
36	Bus Voltage (6.9KV Shutdown)	D2	1 Channel Per Train	6400	7400	VOLTS	Analog Scale & Digital Display
37	CCS Surge Tank Level Abnormal	D3	1 Channel Per Train	0	100	%	
38	Centrifugal Charging PumpTotal Flow	D2	1 Channel	0	1000	GPM	
39	Charging Header Flow	D3	1 Channel	0	110	GPM	Deviation #17
40	Component Cooling Water To ESF Flow	D2	1 Channel Per Hx	0	5561	GPM	
41	Component Cooling Water Supply Temperature	D2	1 Channel Per Train	50	150	Deg F	Deviation #7
42	Condensate Storage Tank Water Level	D3	1 Channel Per Tank	0	385,000	GAL	Not Primary Source of Aux. Feedwater. See Variable 27.
43	Containment Air Return Fan Status	D2	1 Channel Per Fan	On	Off	N/A	(Breaker Status

Table 7.5-2 Regulatory Guide 1.97 Post Accident Monitoring Variables Lists Legend (Page 7 of 14)

VAR NUM	VARIABLE NAME	TYPE/ CATEGORY	REDUNDANT CHANNELS	MINIMUM RANGE FROM	MINIMUM RANGE TO	RANGE UNITS	NOTES
44	Containment Cooling Valve Status	D3	1 Channel Per Valve	Open	Closed	NA	
45	Containment Spray Flow	D2	1 Channel Per Train	0	4400	GPM	
46	Containment Spray HXOutlet OutletTemperature	D2	1 Channel Per HX	0	200	Deg F	
47	Containment Sump Water Level (Narrow Range)	D3	1 Channel	2	66	Inches	Deviation #12
48	Containment Sump Water Temperature	D2	1 Channel	50	400	Deg F	Used RHR TemperatureInl et
9	Diesel Generator Power	D2	1 Channel	0	4.8	MWATTS	
50	Diesel Generator Volts	D2	1 Channel Per DG	0	6900	VOLTS	
51	ECCS Valve Status	D2	1 Channel Per Valve	Open	Closed	NA	
52	ERCW Header Flow	D2	1 Channel Per Header	0	20,000	GPM	

Table 7.5-2 Regulatory Guide 1.97 Post Accident Monitoring Variables Lists Legend (Page 8 of 14)

VAR NUM	VARIABLE NAME	TYPE/ CATEGORY	REDUNDANT CHANNELS	MINIMUM RANGE FROM	MINIMUM RANGE TO	RANGE UNITS	NOTES
53	ERCW Supply Temperature	D2	1 Channel Per Header	32	200	Deg F	
54	Emergency Gas Treatment Damper Position	D2	1 Channel Per Damper	Open	Closed	NA	
55	Emergency Ventilation Damper Status	D2	1 Channel Per Damper	Open	Closed	NA	
56	Hydrogen Recombiner Status	D3	1 Channel Per Recombiner	On	Off	NA	
57	Igniter Group Status	D3	1 Channel Per Group	On	Off	NA	
58	Inverter Current (120V ac Vital)	D2	1 Channel Per Inverter	0	167	AMPS	Local Indication Note 8
59	Inverter Voltage (120V ac Vital)	D2	1 Channel	115	125	VOLTS	Local Indication Note 8
60	Letdown Flow	D3	1 Channel	0	144	GPM	Deviation #18
61	MCR Pressure	D3	1 Channel	0	0.50	inch H_20	
62	MCR Radiation Level	D2	1 Channel	1E-1	1E4	mR/Hr	

Table 7.5-2 Regulatory Guide 1.97 Post Accident Monitoring Variables Lists Legend (Page 9 of 14)

VAR NUM	VARIABLE NAME	TYPE/ CATEGORY	REDUNDANT CHANNELS	MINIMUM RANGE FROM	MINIMUM RANGE TO	RANGE UNITS	NOTES
63	Main Feedwater Flow	D3	1 Channel Per Loop	0	4,372,720	lb/hr	
64	Normal Emergency Boration Flow	D2	1 Channel	0	150	GPM	Deviation #4
65THIS LINE INTENTIONALLY LEFT BLANK							
66	Pressurizer Heater Status (Electric Current)	D2	1 Channel Per Group	0	50.5	AMPS	(See Note 3)
67	Pressurizer Pressure Relief Valve Position (PORV, Block, and Code)	D2	1 Channel Per Valve	Closed	Not Closed	N/A	
68	Pressurizer Relief Tank Level	D3	1 Channel	0	100	%	
69	Pressurizer Relief Tank Pressure	D3	1 Channel	0	100	PSIG	
70	Pressurizer Relief Tank Temperature	D3	1 Channel	50	400	Deg F	Deviation #11
71	RCP Seal Injection Flow	D3	1 Channel Per RCP	0	13.2	GPM	

Table 7.5-2 Regulatory Guide 1.97 Post Accident Monitoring Variables Lists Legend (Page 10 of 14)

VAR NUM	VARIABLE NAME	TYPE/ CATEGORY	REDUNDANT CHANNELS	MINIMUM RANGE FROM	MINIMUM RANGE TO	RANGE UNITS	NOTES
72	RCS Head Vent Valve Status	D2	1 Channel Per Valve	Closed	Not Closed	NA	
73	RHR Heat Exchanger Outlet Temperature	D2	1 Channel Per HX	50	400	Deg F	Deviation #9
74	RHR Pump Flow (RHR System Flow)	D2	1 Channel Per Pump	0	5500	GPM	
78	Safety Injection System Valve Status	D3	1 Channel Per Valve	Open	Closed	NA	
79	Spent Fuel Pool Level Alarm	D2	1 Channel	748'111/2	749'21/2	ft,in	Range Reflects Low and High Alarm Setpoints
80	Spent Fuel Pool Temperature Alarm	D2	1 Channel	NA	127	Deg F	Upper Range Is Alarm Setpoint
81	Steam Generator Blowdown Isolation Valve Status	D2	1 Channel Per Valve	Closed	Not Closed	NA	
82	Steam Generator Level (Wide Range)	D1	4 Channels 1 Per SG	0	100	%	Deviation #10 Notes 1 & 9
83	Main Steam Flow	D2	1 Channel Per SG	0	4,500,000	lb/hr.	

Table 7.5-2 Regulatory Guide 1.97 Post Accident Monitoring Variables Lists Legend (Page 11 of 14)

VAR NUM	VARIABLE NAME	TYPE/ CATEGORY	REDUNDANT CHANNELS	MINIMUM RANGE FROM	MINIMUM RANGE TO	RANGE UNITS	NOTES
84	Tritiated Drain Collector Tank Level	D3	1 Channel Per Train	4	96	%	Local Indication Deviation #25
85	Volume Control Tank Level	D3	1 Channel	0	100	%	Deviation #19
86	Waste Gas Decay Tank Pressure	D3	1 Channel Per TankI	0	150	PSIG	Local ndication Deviation #23
87	Radiation Exposure Meters	E3	NA	NA	NA	NA	Deviation #22
88	Airborne Radiohalogens And Particulate	E3	Portable	1.0E-9	1.0E-3	uCi/cc	Airborne I 131 sand particulates
89	Plant And Environs Radiation	E3	Portable	1.0E-3	1.0E4		
90	Plant And Environs Radioactivity	E3	Portable	NA	NA	NA	Multi Channel Gamma Ray Spectrometer
91	Auxiliary Building Vent (Noble Gas)	E2	1 Channel	1.0E-6	1.0E-2	uCi/cc	Deviation #13 (Noble Gas)

Table 7.5-2 Regulatory Guide 1.97 Post Accident Monitoring Variables Lists Legend (Page 12 of 14)

VAR NUM	VARIABLE NAME	TYPE/ CATEGORY	REDUNDANT CHANNELS	MINIMUM RANGE FROM	MINIMUM RANGE TO	RANGE UNITS	NOTES
92	Auxiliary Building Vent (Flow Rate)	E2	1 Channel	0	250,800	CFM	
93	Auxiliary Building Vent (Particulates and Onsite Halogens)	E3	1 Channel	----See Note 11----		uCi/cc	Sampling With Analysis Capability Deviation #14
94	Condenser Vacuum Pump Exhaust Vent (Flow Rate)	E2	1 Channel	0	45	SCFM	
95	Condenser Vacuum Pump Exhaust Vent (Noble Gas)	C3 E2	1 Channel	4.0E-7	2.4E+3	uCi/cc	Deviation #33
96	ERCW Radiation Monitors	E2	1 Channel Per Discharge Point	3.3E-4	1.65E-2	uCi/cc	
97	POST ACCIDENT SAMPLE SYSTEM	E3	1 System	See below			Sampling With Onsite Analysis Capability
97a	Reactor Coolan Chloride Concentration t	E3	NA	1	20	ppm	Deviation #29
97b	Reactor Coolant Dissolved Hydrogen	E3	NA	100	2000	cc/kg (STP)	Deviation #21

Table 7.5-2 Regulatory Guide 1.97 Post Accident Monitoring Variables Lists Legend (Page 13 of 14)

VAR NUM	VARIABLE NAME	TYPE/ CATEGORY	REDUNDANT CHANNELS	MINIMUM RANGE FROM	MINIMUM RANGE TO	RANGE UNITS	NOTES
97c	Reactor Coolant Dissolved Oxygen	E3	NA	1	20	ppm	Deviation #34
97d	Reactor Coolant Total Dissolved Gas	E3	NA	100	2000	cc/kg(STP)	Deviation #34
97e	Reactor Coolant Boron	E3	NA	50	6000	ppm	Deviation #26
97f	Reactor Coolant pH	E3	NA	1	13	pH	
97g	Reactor Coolant Sample Activity	C3 E3	NA	10uCi/ml	10Ci/ml	Ci/ml	Deviation #5
97h	Reactor Coolant Gamma Spectrum	E3	NA	NA	NA	NA	Isotopic Analysis
98	CONTAINMENT AIR						
98a	Containment Air Hydrogen	E3	NA	0	10	% by volume	Also Measured by Hydrogen Analyzer Deviation #2
98b	Oxygen Content		NA	NA	NA	NA	Deviation #27
98c	Gamma Spectrum Sample	E3	NA	NA	NA	NA	Isotopic Analysis
99	Shield Building Vent Flow	E2	1 Channel Per Unit	0	28,000	CFM	Per Unit

Table 7.5-2 Regulatory Guide 1.97 Post Accident Monitoring Variables Lists Legend (Page 14 of 14)

VAR NUM	VARIABLE NAME	TYPE/ CATEGORY	REDUNDANT CHANNELS	MINIMUM RANGE FROM	MINIMUM RANGE TO	RANGE UNITS	NOTES
100	Shield Building Vent Monitor (Particulate Per UnitOnsite And Iodine)	E3	1 Channel	1.0E-3	1.0E2	uCi/cc	Sampling With Analysis Capability
101	Steam Generator Discharge Vent (Flow Per Release Rate and Noble Gas)	E2	1 Channel	Note 4	Note 4	Note 4	
102	METEOROLOGY						
102a	Vertical Temperature Difference	E3	1 Channel	-9	+18	Deg F	
102b	Wind Direction	E3	1 Channel	0	360	Deg	
102c	Wind Speed	E3	1 Channel	0	50	MPH	Deviation #28
103	Radiation Exposure Rate	E3	Portable	1.0E- 3	1.0E4	R/hr	Deviation #31

Notes:

1. The following parameters are identified as diverse.
   ParameterDiverse Parameter
   T (Hot)Core Exit Temperature
   Core Exit TemperatureT (Hot)
   T (Cold)SG Pressure
   Auxiliary Feedwater FlowSG NR/WR Level
2. Deleted.
3. Pressurizer Heater Status required only for safety related heater banks (backup heater 1A A and 1B B). Range is given in amps per element.
4. Recorder shall be provided for duration of release from all discharge points.
   Noble Gas Activity (See Main Steam Line Radiation, Variable No. 7)
   Steam Flow Rate0 to 4,945,200 lb/hr PORV and Safety Valves
   0 to 63,375 lb/hr To Aux. Feedwater Pump Turbine
5. Vessel level on the plasma display is the compensated actual vessel level derived from a microprocessor algorithm using the upper range, lower range, dynamic range differential pressure, wide range temperature, and wide range pressure.
6. Deleted.
7. Also monitors steam generator discharge vent noble gas activity. Required range of sensitivity specified is met by indication displaying in units of dose rate. Conversion to required range is performed using conversion factor specified in Calc. WBNAPS3 048.
8. The 120V AC vital Inverter has a trouble alarm in the MCR which notifies of trouble on the bus.
9. At least one of the redundant loops is trended on a non divisional trend recorder qualified to meet Category 2 requirements.
10. The Core Exit T/C Temperature (hottest), reactor vessel level, and Saturation Margin are trended on redundant Class 1E plasma displays (the last 30 minutes trending only) in the main control room.
11. The range for the Auxiliary Building particulate is 10-10 to 10-5 ?Ci/cc and the range for halogens (Iodine) is 10-9 to 10-4 ?Ci/cc.
12. The requirements for Category I variables which require a third independent channel to resolve ambiguity resulting when redundant displays disagree are being implemented at WBN as follows:
    The requirements for each channel is assigned to a redundant protection set (I, II, III, and IV) and electrical independence is maintained from sensor to the isolator in the Auxiliary Instrument Room. From the isolator to the indicator in the Main Control Room, third channel (PAM 3) cables may be routed with either PAM 1 or PAM 2 cables (but not both) depending on its associated protection set.

Table 7.5-3 Deviations From Regulatory Guide 1.97[1]
(Page 1 of 5)

DEVIATION 11

VARIABLE (70)

Quench Tank (Pressurizer Relief Tank [PRT]) Temperature

DEVIATION FROM RG 1.97 GUIDANCE

The range for this variable is recommended to be 50 to 750°F in accordance with RG 1.97, Revision 2. WBN recommends the range to be 50 to 400°F.

JUSTIFICATION

The purpose of this variable is to monitor operation. The PRT rupture disk is designed to operate between 86-100 psig. Assuming that the rupture disk operates at 100 psig and the pressurizer is at 2500 psig at saturated conditions, the maximum temperature during discharge when all valves in the line are open could be approximately 350°F. High temperature due to discharges or leakage into the tank from the pressurizer or other sources would produce an early upward trend in PRT temperature above normal. Temperatures far below the RG 1.97 recommended temperature of 750°F or the 400°F WBN recommended temperature would be sufficient to alert the operator to an abnormal condition and the potential need to check related PAM variables. Therefore, the recommended range of 50 to 400°F is sufficient to permit the operator to monitor plant operation.

DEVIATION 13

VARIABLE (91)

Auxiliary Building Exhaust Vent Radiation Level - Noble Gas Release

DEVIATION FROM RG 1.97 GUIDANCE

The range recommended in RG 1.97, Revision 2, is 10^{-6} to 10^{3} microcuries/cubic centimeter (cc); the recommendation for WBN is 10^{-6} to 10^{-2} microcuries/cc.

JUSTIFICATION

Table 7.5-3 Deviations From Regulatory Guide 1.97[1]
(Page 2 of 5)

The Auxiliary Building vent monitor is provided to continuously monitor the airborne radioactivity released through the Auxiliary Building exhaust vent. An accident causing Auxiliary Building radiation level to be high will cause all ventilation paths exhausting into the Auxiliary Building vent duct to automatically close and the Auxiliary Building gas treatment system to be activated. Because the isolation function occurs before accident-range activity is reached, a normal-range monitor only is employed to monitor activity in the Auxiliary Building exhaust vent. Therefore, the recommended range of 10^{-6} to 10^{-2} microcuries/cc is adequate for detecting and measuring noble gas concentrations.

DEVIATION 32

VARIABLE (5)

Containment Sump Level (Wide Range)

DEVIATION FROM RG 1.97 GUIDANCE

The range recommended in RG 1.97, Revision 2, is "Bottom of containment to 600,000-gallon level equivalent." Watts Bar recommends a range from 0-20 feet (with the "0" level starting at six inches above the reactor floor) (see Note).

JUSTIFICATION

Watts Bar utilizes a containment sump level monitoring system that starts measuring at six inches above the containment floor (level tap located at elevation 703' 3-3/8"). The range of the instrument is 20 feet (723' 3-3/8"). The total volume of water available to flood containment post-LOCA is 844,000 gallons, which equals a maximum transient flood level of 720' 0". Therefore, the recommended range is fully adequate to monitor the maximum flood level that would a be experienced.

Note:The containment sump level monitoring system is utilized only during an accident. During normal operation reactor coolant leakage is monitored by the reactor building floor and equipment drain pocket sump. For post accident monitoring, the operator is aware that the "0" level actually begins at 6" above the floor and will realize that there is extra water inside containment when the sump monitor begins to indicate.

DEVIATION 33

VARIABLE 95

Table 7.5-3 Deviations From Regulatory Guide 1.97[1]
(Page 3 of 5)

Condenser Vacuum Pump Exhaust Vent (Noble Gas)

DEVIATION FROM RG 1.97 GUIDANCE

The R.G. 1.97 R2 required range for the condenser vacuum pump exhaust monitors is l.0E-6 to l.0E+5 µCi/cc.

JUSTIFICATION

TVA has determined the total gas required range of the condenser vacuum pump exhaust monitors to be 3.2E-7 to 3.5E+3 µCi/cc.

The steam generator tube rupture is the only credible accident monitored by the condenser vacuum pump exhaust monitor. NUREG 0800 R2 requires that the tube rupture accident be analyzed using the highest isotope concentrations allowed by the Watts Bar Technical Specifications. The specific activity of the reactor coolant is limited to:

a) Less than or equal to 1 µCi/gm Dose Equivalent Iodine-131 and

b) Less than or equal to 100/ µCi/gm.

The Dose Equivalent I-131 is 4.95 times more restrictive than the 100/ limit. The 100/ limit is more conservative and is used for this calculation. The highest concentration of mixed noble gas isotopes that can be present under the 100/ limit is 9.89E+2 µCi/cc as determined in TVA calculation WBNAPS-048. Therefore the Watts Bar required range for the condenser vacuum exhaust monitor meets the intent of RG 1.97 R2.

DEVIATION 34

VARIABLE 97c & 97d

Primary Coolant Dissolved Total Gas (97d) and Dissolved Oxygen (97c)

DEVIATION FROM RG 1.97 GUIDANCE

Table 7.5-3 Deviations From Regulatory Guide 1.97[1]
(Page 4 of 5)

RG 1.97, R2 indicates the range for variable 97d is from 0 to 2000 cc/Kg and the range for variable 97c is 0 to 20 ppm. The TVA required range for variable 97d is 100 to 2000 cc/Kg, and 1 to 20 ppm for variable 97c.

JUSTIFICATION

The TVA required ranges for variable 97c and 97d permit adequate assessment of the primary system for these dissolved gases, and therefore, meets the intent of RG 1.97.

DEVIATION 35

VARIABLE (20)

Control Rod Position

DEVIATION FROM RG 1.97 GUIDANCE

RG 1.97 recommends that control rod position indication be a Type B, Category 3 variable (B3) to monitor for reactivity control. Watts Bar recommends that this variable be a Type D, Category 3 variable (D3).

JUSTIFICATION

Control rod position indication is an indirect variable. It provides backup indication for monitoring reactivity control. Neutron flux (category 1) is a direct variable that allows the operator to determine if reactivity is under control (i.e., the reactor has tripped and the core is in a subcritical condition). Since this provides backup indication, utilizing it as a Type D variable is sufficient.

DEVIATION 36

VARIABLE 4

Containment Area Radiation, High Range

Table 7.5-3 Deviations From Regulatory Guide 1.97[1]
(Page 5 of 5)

DEVIATION FROM RG 1.97 GUIDANCE

Note 7 of RG 1.97, R2 for the subject variable states, "detectors should respond to gamma photons within any energy range from 60 KeV to 3 MeV with an energy response accuracy of 20 percent at any specific photon energy from 0.1 MeV to 1 MeV. Overall system accuracy should be within a factor of 2 over the entire range. TVA meets the requirements of RG I.97, R3 Note 7 for the subject variable, which states, "Detectors should respond to gamma radiation photons within any range from 60 KeV to 3 MeV with a dose rate response accuracy within a factor of 2 over the entire range."

JUSTIFICATION

It is acceptable to meet the requirements of RG 1.97, R3.

1.This Table only includes deviations not included in References [9] or [10] and any revisions to deviations included in those references.

7.6 ALL OTHER SYSTEMS REQUIRED FOR SAFETY

7.6.1 120V ac and 125V dc Vital Plant Control Power System

This system is described in Section 8.3.

7.6.2 Residual Heat Removal Isolation Valves

7.6.2.1 Description

There are two motor-operated gate valves (FCV 74-1 (8702) and FCV 74-2 (8701) as shown in control diagram, Figure 5.5-4) in series in the inlet line from the Reactor Coolant System (RCS) to the Residual Heat Removal (RHR) System. They are normally closed and are only opened for residual heat removal after system pressure is reduced to less than 370 psig and system temperature has been reduced to less than 350°F. (See Chapter 5 for details of the RHR system.)

The RHR system inlet isolation valves are interlocked with a pressure signal to prevent them from being opened whenever the system pressure is greater than the nominal setpoint of 370 psig.

Should either or both of these valves fail to open when required, a letdown path can be established via bypass valves which have been provided around valves FCV 74-2 (8701) and FCV 74-1 (8702). The bypass valves are FCV 74-8 (8703) and FCV 74-9 (8704). A given set of two of these parallel valves is provided with trained power, so that failure of one power train will not defeat the establishment of the necessary letdown flow path.

Whenever the RHR isolation inlet and/or bypass valves are open and RCS pressure rises to the nominal setpoint of 375 psig, a high pressure alarm in the main control room (MCR) alerts the operator to the RHR system alignment. The isolation valves should be closed before the pressure reaches the RHR suction line pressure relief valve setpoint but only if there is a steam bubble in the pressurizer or the charging pump has been stopped.

The motor-operated bypass valves are located in bypass lines paralleling the normal RHR suction isolation valves FCV 74-1 and FCV 74-2 which are in series in the flowpath. Valves FCV 74-8 and FCV 74-9 are normally closed and remain closed with power locked out unless one of the two main isolation valves (FCV 74-1 or FCV 74-2) cannot be opened and the plant must be cooled down. Then, the redundant flowpath through the appropriate bypass valve is used to provide RHR cooling flow. Valves FCV 74-8 and FCV 74-9 are interlocked with signals from RCS pressure transmitters PT 68-63 and PT 68-64, respectively, as shown in Figure 7.6-7. These interlocks prevent inadvertent opening when RCS pressure is above the nominal 370 psig setpoint. The letdown bypass valves are monitored by the plant computer with an automatic printout in the main control room if either of the valves is not in its fully closed position.

7.6.2.2 Analysis

Based on the scope definitions presented in Reference [2] (IEEE 279-1971) and Reference [3] (IEEE 338-1971), it is considered that these criteria do not apply to the residual heat removal isolation valve interlocks. However, in order to meet NRC requirements and because of the possible severity of the consequences of loss of function, the requirements of IEEE 279-1971 will be applied with the following comments.

(1) For the purpose of applying IEEE 279-1971 to this circuit the following definitions will be used.

(a) Protective System

The two valves in series and all components of their interlocking and closure circuits.

(b) Protective Action

(1) The automatic initiation of interlocks to prevent opening of inlet isolation and bypass valves to maintain residual heat removal system isolation from the reactor coolant system for reactor coolant system pressure at or above the nominal setpoint of 370 psig.

(2) Initiation of an alarm in the MCR to alert the operator to the RHR system alignment whenever the RHR inlet isolation and/or bypass valves are open and the RCS pressure is equal to or greater than the nominal setpoint of 375 psig. Operator action in response to the alarm is required to close the valves in accordance with NRC Generic Letter 88-17 and References [4] and [5].

(2) IEEE Standard 279-1971, Paragraph 4.15: This requirement does not apply, since the setpoints are independent of mode of operation and are not changed.

Environmental qualification of the valves and wiring are discussed in Section 3.11.

7.6.3 Refueling Interlocks

Electrical interlocks (i.e., limit switches) as discussed in Section 9.1.4 are provided for minimizing the possibility of damage to the fuel during fuel handling operations.

7.6.4 Deleted by Amendment 63.

7.6.5 Accumulator Motor-Operated Valves

The design of the interconnecting of the signals to the cold leg accumulator isolation valve meets the following criteria established in previous NRC positions on this matter (see Figure 7.6-3):

(1) Automatic opening of the accumulator valves when (a) the primary coolant system pressure exceeds a preselected value (to be specified in the Technical Specifications) or (b) a safety injection signal has been initiated. Both signals are provided to the valves.

(2) Utilization of a safety injection signal to automatically override any features that are provided to allow an isolation valve to be closed.

The valves and control circuits are discussed in Sections 6.3.2.15, 7.3.1.1.2, and 6.3.5.5.

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 during normal operation such that:

(1) They open automatically on receipt of an "S" signal.

(2) They open automatically whenever the RCS pressure is above the safety injection unblock pressure as specified in the Technical Specifications.

(3) They cannot be closed as long as an "S" signal is present. The main control board switches for these valves are three position switches which provide a "spring return to auto" from the open position and closed position.

During plant shutdown, the accumulator valves are in a closed position. To prevent an inadvertent opening of these valves during that period, the accumulator valve power will be removed.

Administrative control is again required to ensure that power to these valves is restored during the prestartup procedures. During startup the valves are manually opened prior to RCS pressure exceeding 1000 psig. After the valves are open, power is removed to prevent inadvertent valve closure. During cooldown, power is restored and the valves manually closed from the MCR before RCS pressure decreases below the cold leg accumulator pressure.

These normally open motor-operated valves have an alarm indicating a mispositioning (with regard to their Emergency Core Cooling System (ECCS) function during the injection phase). The alarms sound in the MCR.

7.6.6 Spurious Actuation Protection for Motor Operated Valves

The design of Watts Bar Nuclear Plant is such that the failure of any single valve to operate on demand cannot result in the loss of capability to perform a system safety function. However, in the case of possible inadvertent valve misalignment, the following motor operated valves have been identified as valves whose spurious operation could result in the loss of a system safety function. (Westinghouse valve numbers are in parentheses).

FCV	63-1	(8812)	FCV	63-67	(8808D)	FCV 63-98	(8808B)
FCV	63-3	(8813)	FCV	63-72	(8811A)	FCV 63-118	(8808A)
FCV	63-5	(8806)	FCV	63-73	(8811B)	FCV 63-156	(8802A)
FCV	63-8	(8804A)	FCV	63-80	(8808C)	FCV 63-157	(8802B)
FCV	63-11	(8804B)	FCV	63-93	(8809A)	FCV 63-172	(8840)
FCV	63-22	(8835)	FCV	63-94	(8809B)	FCV 62-98	(8110)
						FCV 62-99	(8111)

Means have been provided to preclude such spurious misalignment. Except for FCV 62-98 and FCV 62-99, the design consists of modified control circuits for these valves to ensure that no single failure will be able to energize the opening and/or closing coils for the valve operator. The design utilizes redundant contacts which are wired before and after each opening and closing coil as required. Figure 7.6-4 illustrates this protection scheme. In this typical schematic, isolation of the opening and closing coils is provided by contacts R11-R12, R31-R32, L2l-L22, and (L41-L42). Valves FCV 63-67, FCV 63-72, FCV 63-73, FCV 63-80, FCV 63-98, and FCV 63-118 require this protection scheme only for the closing coil.

In addition, single failure has been considered on the part of the operator. The design modification will include easily accessible, clear protective covers to be attached to the main control board panel over each respective control room switch except FCV-63-1. The operator would be required to open this protective cover before he operates the control switch.

For FCV 63-1, FCV 63-5, FCV 63-22, FCV 63-67, FCV 63-80, FCV 63-98, and FCV 63-118 operating instructions specify the removal of power during normal operation. For FCV 62-98 and FCV 62-99, the motive power has been removed.

7.6.7 Loose Part Monitoring System (LPMS) System Description

The Loose Part Monitoring System (LPMS) provides the capability to detect acoustic disturbances indicative of loose parts within the reactor coolant system pressure boundary.

The loose part monitoring function of this system has two sensors located at each of the six natural collection regions, the top and bottom plenums of the reactor vessel and the primary coolant inlet plenum to each steam generator. One sensor at each of the six locations is an active sensor and the other is an installed spare sensor. The lower-plenum reactor vessel sensors are mounted on the incore instrumentation guide tubes. The upper-plenum reactor vessel sensors are stud-mounted on the vessel head lifting lugs. The steam generator inlet sensors are installed on a mounting pad attached to the steam generators. The redundant instrumentation channels are physically separated, starting at the sensor location and extending out to the containment electrical penetrations.

The system cabinet is located in the control building at elevation 708.0 in the unit 1 auxiliary instrument room. This one cabinet contains equipment which electronically monitors both nuclear steam supply systems in the plant. The loose part monitoring function consists of six active channels for each unit. These channels include alarm units which, when their set threshold is exceeded, provide an alarm in the main control room and automatically start a frequency-modulated tape recorder to record the disturbance. All six channels for loose part monitoring are individually recorded. An audio monitor provides a capability to "listen" audibly to the output signal of a selected channel. A computer-based analytical system is used to perform spectral and statistical analysis of channel performance. This system provides improved techniques in obtaining important information concerning proper channel performance, trend data for comparing channel behavior, and loose part impact events. The quality of data is assessed and maintained in accordance with Reference [7]. Initial channel calibration is performed by use of a mechanical impact device to demonstrate proper channel calibration. The channel sensitivity is set to detect a loose part that impacts the reactor coolant boundary within 3 feet of the sensor having a kinetic energy of 0.5 ft-lb. Channel frequency spectra data is recorded during initial calibration for comparison to suspected loose part impact events. Channel calibration during normal refueling outages is performed by a mechanical impact device, except for sensors located in areas where plant personnel radiation exposure is considered by Plant Management to be excessive. The above described computer-based analytical system may be used, as an option to using a mechanical input device, to verify proper channel calibration. Periodic online channel checks, audio checks and functional tests shall be made in accordance with References [6] and [7] to ensure that the required sensitivity is maintained during normal operation.

The anticipated major sources of internal and external noises are operation of the reactor coolant pumps, reactor coolant hydraulic excitation, and stepping of the control rod drive mechanisms. Normal background noises present during the various plant operating modes are accounted for in the signal processing circuitry. The system automatically adjusts its impact alert alarm level above the background noise, detecting only those signals which rise above the changing average. This feature permits the impact alert alarm level to be adjusted to a maximum sensitivity level consistent with the short-term averaging of the normal background noises over a preselected time period. The LPMS, although not a Class 1E system, has been designed and qualified to endure seismic events. The portion of the system inside the reactor building (sensors and cabling) will operate and remain functional through an Operating Basis Earthquake (OBE). The portion of the system outside the reactor building (cabling and instrument cabinet containing electronic indicating, alarming, recording, and analysis instrumentation) will remain structurally intact through a Safe Shutdown Earthquake (SSE) as seismic Category I(L) equipment. The audio alarm is qualified to operate and function after exposure to an OBE. The system is qualified for the normal and abnormal operating radiation, vibration, temperature, and humidity of its environment.

In addition to the primary-side sensors described above, there are also two passive sensors (accelerometers) associated with each steam generator for secondary-side

monitoring. One of these sensors is located on the steam generator trunnion and the other one is on the feedwater piping.

During preoperational testing, preliminary alert levels shall be documented to demonstrate the ability of the system to perform its functions. This is required in accordance with Reference [6].

Description of the diagnostic procedures used to confirm a loose part are addressed in Reference [7].

Maintenance procedures to minimize radiation exposure are addressed in References [6] and [7].

The training program scope is addressed in Reference [6].

The limiting conditions for operation of the loose parts monitoring system are addressed in Reference [8].

7.6.8 Interlocks for RCS Pressure Control During Low Temperature Operation

The basic function of the RCS overpressure mitigation system during low temperature operation is discussed in Section 5.2.2.4. As noted in Section 5.2.2.4, this pressure control system includes manually armed semi-automatic actuation logic for the 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 when plant operation is at a temperature below the arming setpoint. The monitored system temperature signals are processed to generate the reference pressure limit program which is compared to the actual measured system pressure. This comparison will provide an actuation signal to an actuation device which will open the PORV when the device is manually armed as necessary to prevent pressure conditions from exceeding allowable limits. See Figure 7.6-5 for the block diagram showing the interlocks for RCS pressure control during low temperature operation.

The station variables required for this interlock are channelized as follows:

(1) Protection Set I

(a) Wide Range RCS Temperature (TE-68-1, TE-68-18, TE-68-24, TE-68-41)

(2) Protection Set II

(a) Wide Range RCS System Pressure (PT-68-68).

(b) Wide Range RCS Temperature (TE-68-43, TE-68-60, TE-68-65, TE-68-83)

(3) Protection Set III

(a) Wide Range RCS System Pressure (PT-68-66).

The wide range temperature signals, as inputs to the Protection Sets I and II, continuously monitor RCS temperature conditions. In Protection Set I, the existing RCS wide range temperature channels on RCS loops 1 and 2 provides an input to the Eagle 21 digital processing instrumentation. An isolation device in the Eagle 21 instrumentation provides a continuous analog input to an auctioneering device, which is located in the Process Rack of Control Rack Group 1. The lowest reading is selected to 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 III is the wide range RCS pressure signal which also inputs to the Eagle 21 digital processor and 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 auctioneered temperature signal will annunciate a main control room alarm whenever the measured temperature approaches, within a predetermined amount, the reference temperature for arming the system. Similarly, whenever the measured pressure approaches within a predetermined amount of the programmed setpoint, a second alarm will be generated. On an increase in measured pressure above the allowable reference pressure, the actuation signal from Control Rack Group 1 will control the Train A PORV (PCV-68-340A), and the third alarm, "PORV-340A Actuate", will be generated indicating that the actuation signal has been provided to the PORV. The manually armed permissive allows the PORV to open when actual pressure exceeds the allowable pressure. The manually armed permissive prevents a spurious pressurizer PORV opening due to instrumentation failure whenever the permissive is absent.

The monitored generating station variables that generate the actuation signal for the Train B PORV (PCV-68-334) are processed in a similar manner. In the case of the Train B PORV, the reference temperature is generated in Control Rack Group 2 from the lowest auctioneered wide range RCS loop 3 and 4 temperature. The auctioneering device derives its inputs from the RCS wide range temperature in Protection Set II and the actual measured pressure signal is available from Protection Set II. Therefore, the generating station variables used for the Train B PORV are derived from a protection set that is independent of the sets from which generating station variables used for the train A PORV are derived. The error signal derivation itself used for the actuation signals is available from the Control Group.

Upon receipt of the actuation signal, the actuation device will automatically cause the PORV to open when the manually armed permissive is present. Upon sufficient RCS inventory letdown, the operating RCS pressure will decrease, clearing the actuation signal. Removal of this signal causes the PORV to close.

7.6.8.1 Analysis of Interlock

Many criteria presented in IEEE 279-1971 and IEEE 338-1971 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 into dual channels. Either of the two PORVs can accomplish the RCS pressure control function.

The design of the low temperature interlocks for RCS pressure control is such that pertinent features include:

(1) No credible 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.

(2) Testing capability for elements of the interlocks within (not external to) the protection sets that generate the temperature and pressure process signals for the overpressure mitigation system is consistent with the testing principles and methods discussed in Section 7.2.1.1.3.

(3) 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.

7.6.9 Switchover From Injection to Recirculation

The details of achieving cold leg recirculation following safety injection and after a loss-of-coolant-accident (LOCA) are given in Section 6.3.2.2 and Table 6.3-3.

7.6.9.1 Description of Instrumentation Used for Switchover

As noted in Table 6.3-3, protection logic is provided with the main control board switch in "auto." This logic automatically opens the two Safety Injection System (SIS) recirculation sump isolation valves FCV 63-72 (8811A) in Train A and FCV 63-73 (8811B) in Train B with the following logic satisfied: two out of four RWST level less than the Low level setpoint and two out of four high sump level signal in conjunction with the maintained "SI" signal following a LOCA. The "SI" signal is maintained by the contact of a slave relay in the solid state protection system (SSPS) output cabinet that closes on safety injection and remains closed until manually reset from the control board. This manual reset switch is separate from the main safety injection reset switch which is not associated with this circuit. The purpose of the sump valve automatic open circuit reset switch is to permit the operator to remove the actuation signal in the event the corresponding sump isolation valve must be closed and retained in a closed position following a LOCA, such as for maintenance purposes. Although IEEE 279-1971 scope is not applicable to this circuit, applicable criteria is considered in accordance with the following evaluation.

7.6.9.2 Initiation Circuit

The two of four low RWST level coincident with two out of four high sump level is the trip signal, which in coincidence with the "SI" signal, provides the initiation function which would automatically open the containment sump isolation valves.

7.6.9.3 Logic

The logic function derived from the RWST level sensors and the "SI" signal are depicted on Figure 7.6-6, Sheet 1.

7.6.9.4 Bypass

The manual reset logic function is shown on Figure 7.6-6, Sheet 2 and its purpose and action is described above in Section 7.6.9.1. As noted, the "SI" signal is retained by latching it and is not removed by action of the main safety injection reset that is used by the operator per emergency procedures to remove the "SI" signal to other equipment prior to realignment for switchover to the recirculation mode following a postulated LOCA.

7.6.9.5 Interlocks

The trip signal logic consists of four RWST water level transmitters, each of which provides a level signal to one of the four RWST level channel comparators and four sump level transmitters, each of which provides a level signal to one of the four sump level channel comparators. The RWST and containment sump level channel comparators are:

(1) normally de-energized.

(2) de-energized on loss of power.

(3) energized on reaching setpoint.

Each set (one sump level and one RWST level) of level channel comparator is assigned to a separate instrumentation and control power supply. A trip signal is provided from both Train A and Train B SSPS cabinets to the corresponding sump isolation valves logic, should two of the four water level channel comparators receive a RWST level signal lower than the Lo level setpoint, and two of the four sump water level channel comparators receive a signal higher than the setpoint following the generation of an "SI" signal.

Valve FCV 63-72 (8811A) is interlocked with RWST/RHR suction valve FCV 74-3 (8700A) such that FCV 63-72 (8811A) cannot be opened manually unless FCV 74-3 (8700A) is closed. Valve FCV 63-73 (8811B) is interlocked with RWST/RHR suction valve FCV 74-21 (8700B) such that FCV 63-73 (8811B) cannot be opened manually unless FCV 74-21 (8700B) is closed. (The above assumes no SI signal is present.)

Note that in the case of these "SI" recirculation sump isolation valves, the protective action is independent of the position of the interlocking valves. The sump valve is opened automatically by the trip signal (see Figure 7.6-6, Sheet 2) and the control from

the RWST/RHR suction valve positions is bypassed. The valve position interlocking is used only during on-line testing of the "SI" recirculation sump isolation valves or manual switchover.

7.6.9.6 Sequence

This circuit is energized directly from the SSPS output cabinet and is not sequenced following an accident that requires its functioning.

7.6.9.7 Redundancy

The function of this semi-automatic switchover is available from both Train A and Train B down to the actuated equipment. The function including the actuated equipment is, therefore, redundant and train separation and independence is maintained from sensor to actuated equipment.

7.6.9.8 Diversity

Diversity of components and equipment between the redundant trains is not required to protect against systematic failures, such as, multiple failures resulting from a credible single event. The associated components are environmentally and seismically qualified in accordance with the procedures described in Section 3.10 and 3.11. It is noted that there is functional diversity provided in that manual operation capability is provided as a back up to the semi-automatic mode.

7.6.9.9 Actuated Devices

The actuated devices are the two motor control center starters, one for each of the motor operated sump valves, 8811A and 8811B.

REFERENCES

(1) Deleted by Amendment 81.

(2) The Institute of Electrical and Electronic Engineers, Inc., "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations," IEEE Standard 279-1971.

(3) The Institute of Electrical and Electronic Engineers, Inc., "IEEE Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems," IEEE Standard 338, 1971.

(4) Calculation WBN-RAG3-003, Probabilistic Analysis showing the effects of deleting the Residual Heat Removal (RHR) Auto Closure Interlock (ACI).

(5) Westinghouse Nuclear Safety Evaluation Check List (SECL), SECL 91-287, Revision 1, Wiring Modifications to Implement Residual Heat Removal System Automatic Closure Interlock Deletion and Add Control Room Alarm.

(6) Watts Bar Nuclear Plant Design Criteria Number WB-DC-30-31, "Loose Parts Monitoring System."

(7) Plant Technical Instruction (TI) - 34 Series (Implementing Instructions for the Loose Parts Monitoring System) includes TI-34.01, TI-34.02, TI-34.03, TI-34.04, and TI-34.05.

(8) Technical Requirements Manual Section TR 3.3.6, "Loose-Part Detection System."

THIS PAGE INTENTIONALLY BLANK

Figure 7.6-1 Deleted by Amendment 65

Figure 7.6-2 Deleted by Amendment 65

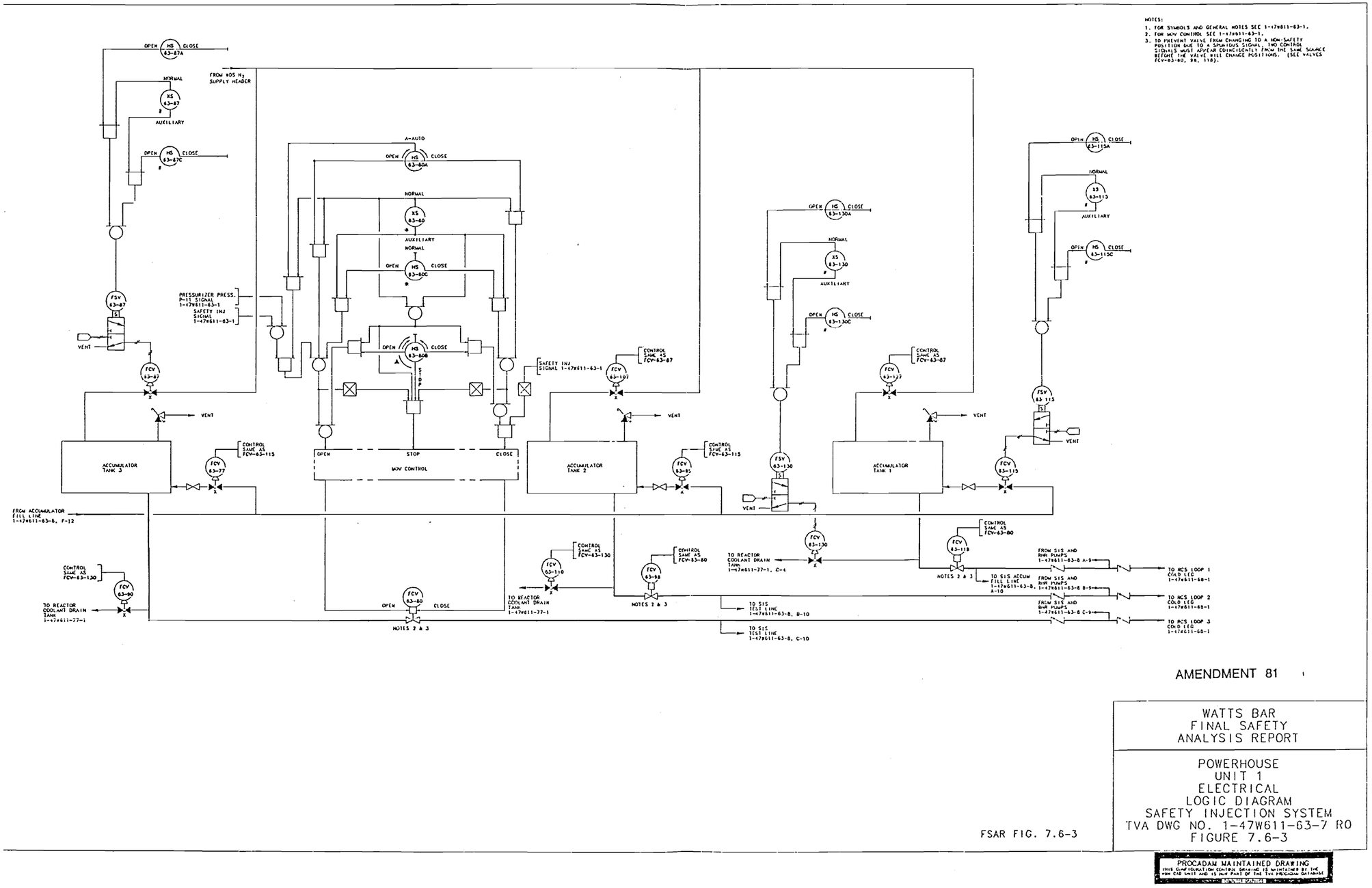


Figure 7.6-3 Powerhouse Unit 1 Electrical Logic Diagram for Safety Injection System

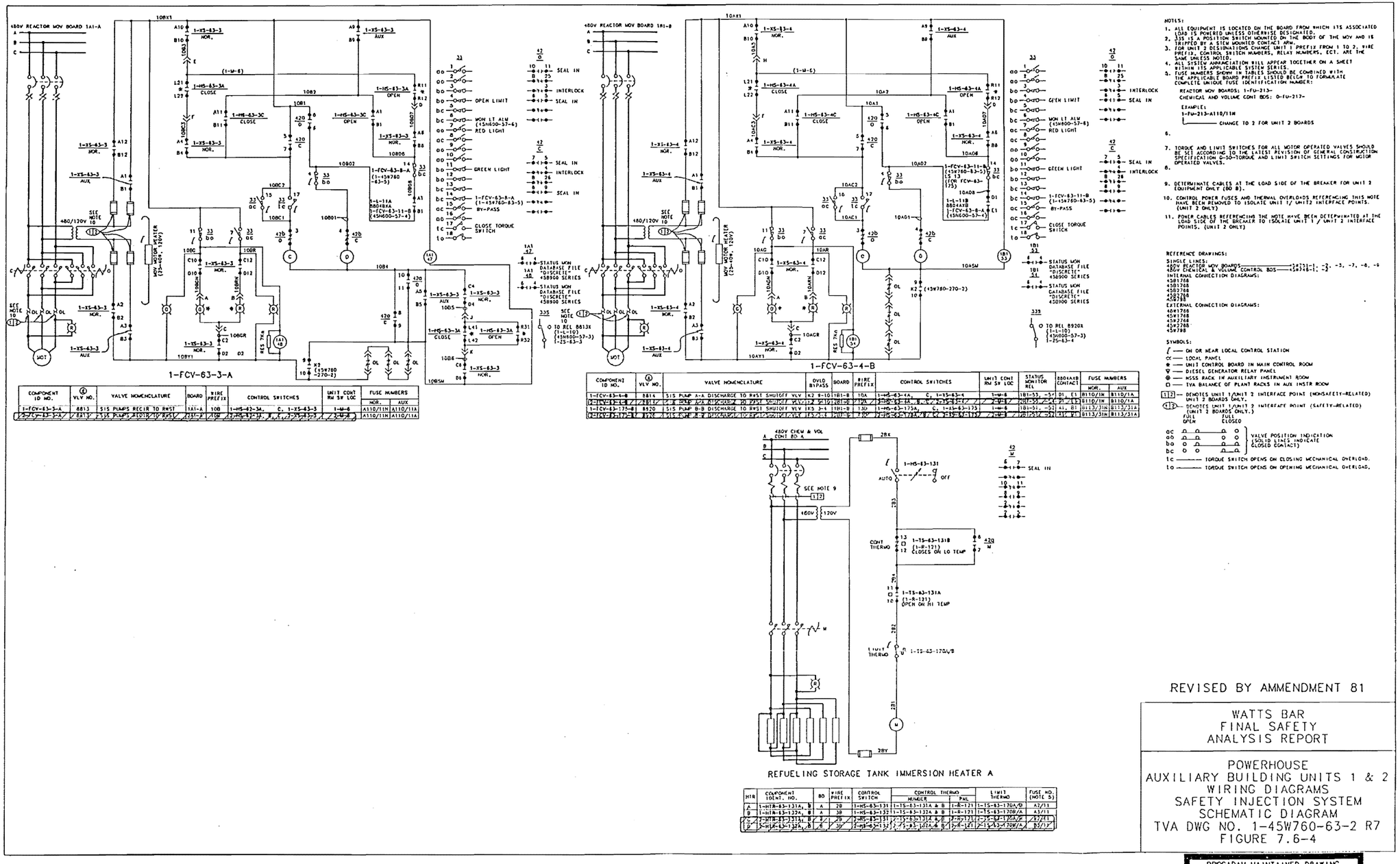


Figure 7.6-4 Powerhouse Auxiliary Building Units 1& 2 Wiring Diagrams for Safety Injection System

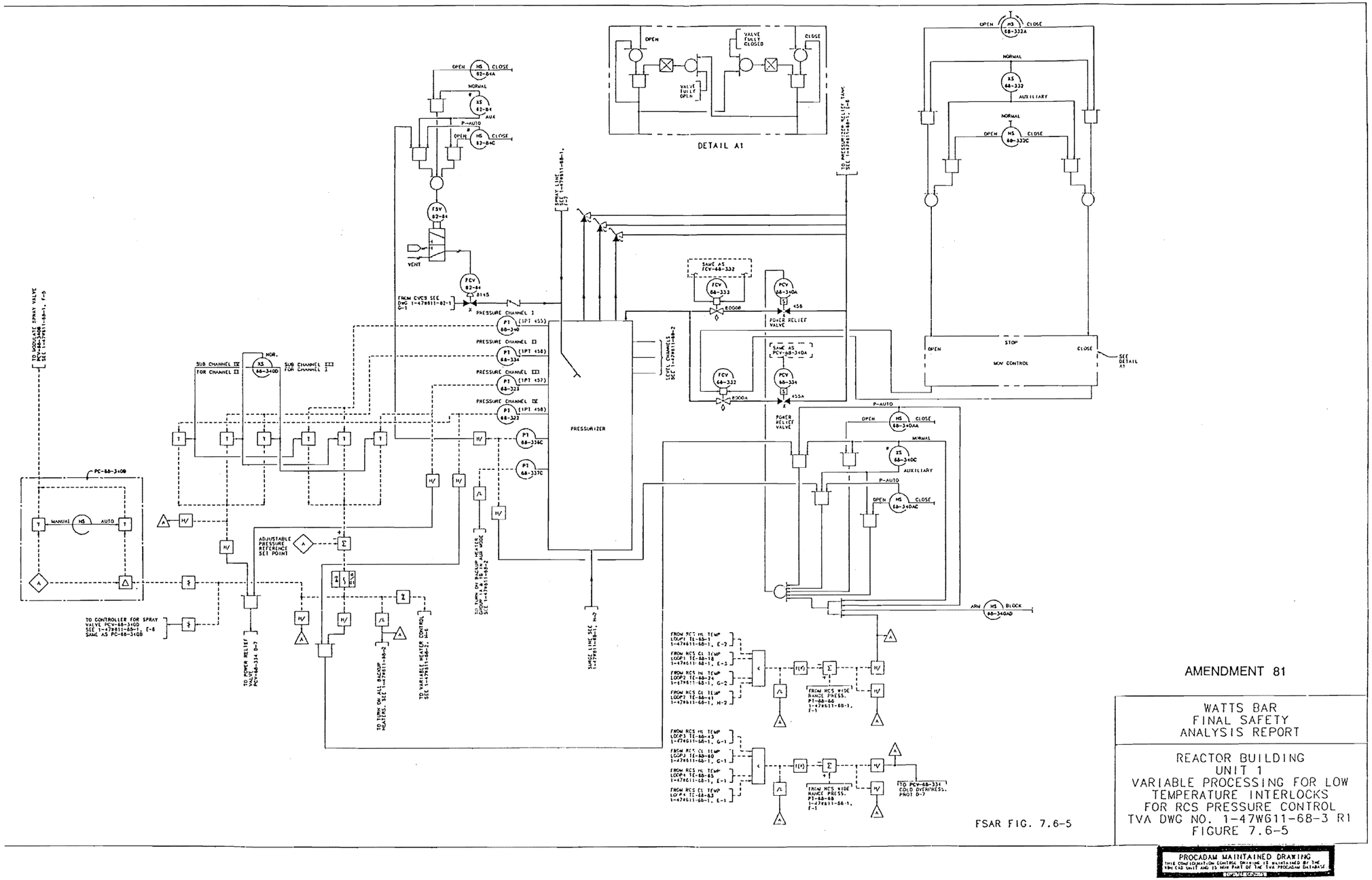


Figure 7.6-5 Reactor Building Unit 1 Variable Processing for Low Temperature Interlocks for RCS Pressure Control

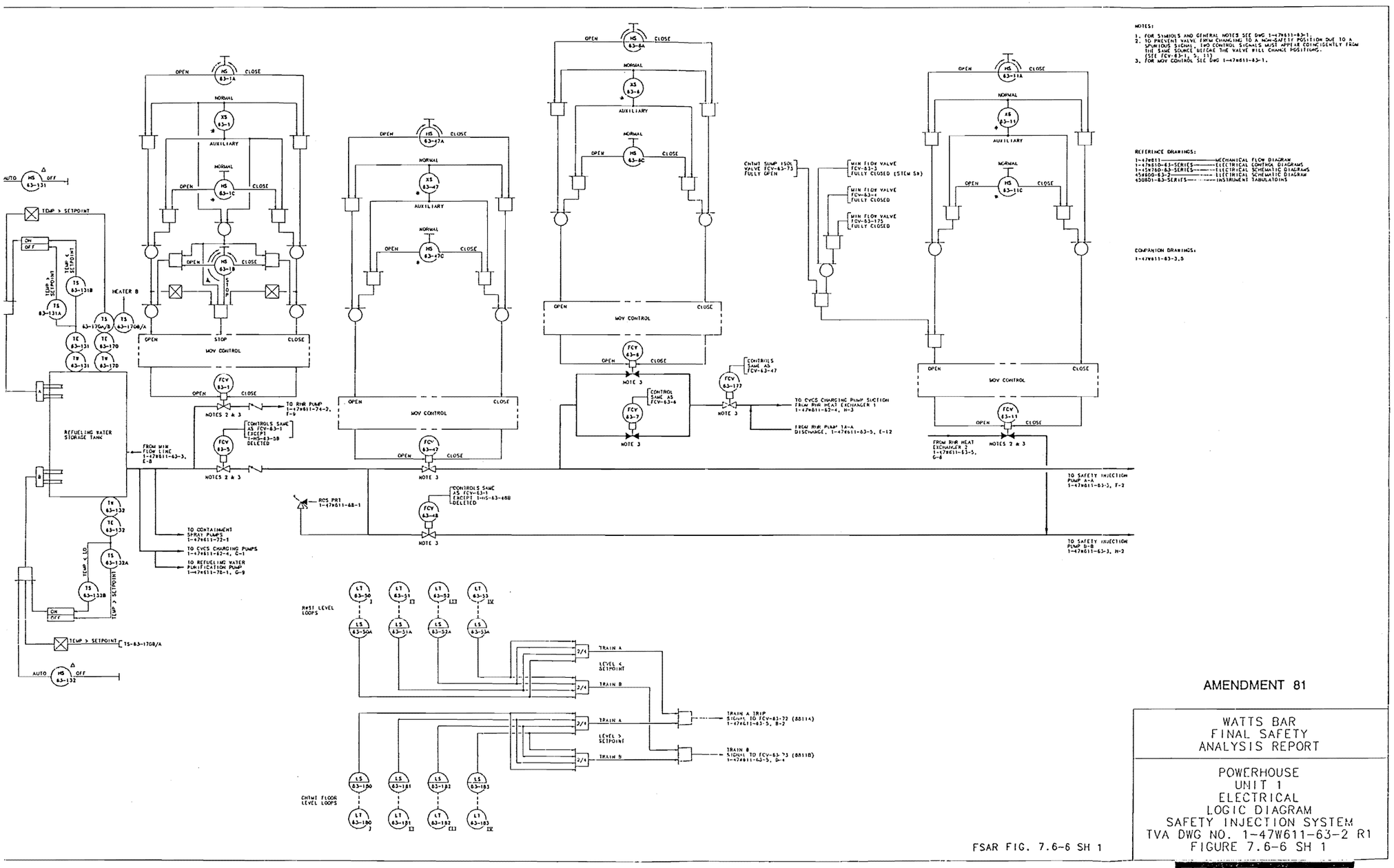


Figure 7.6-6-SH-1 Powerhouse Unit 1 Electrical Logic Diagram for Safety Injection System

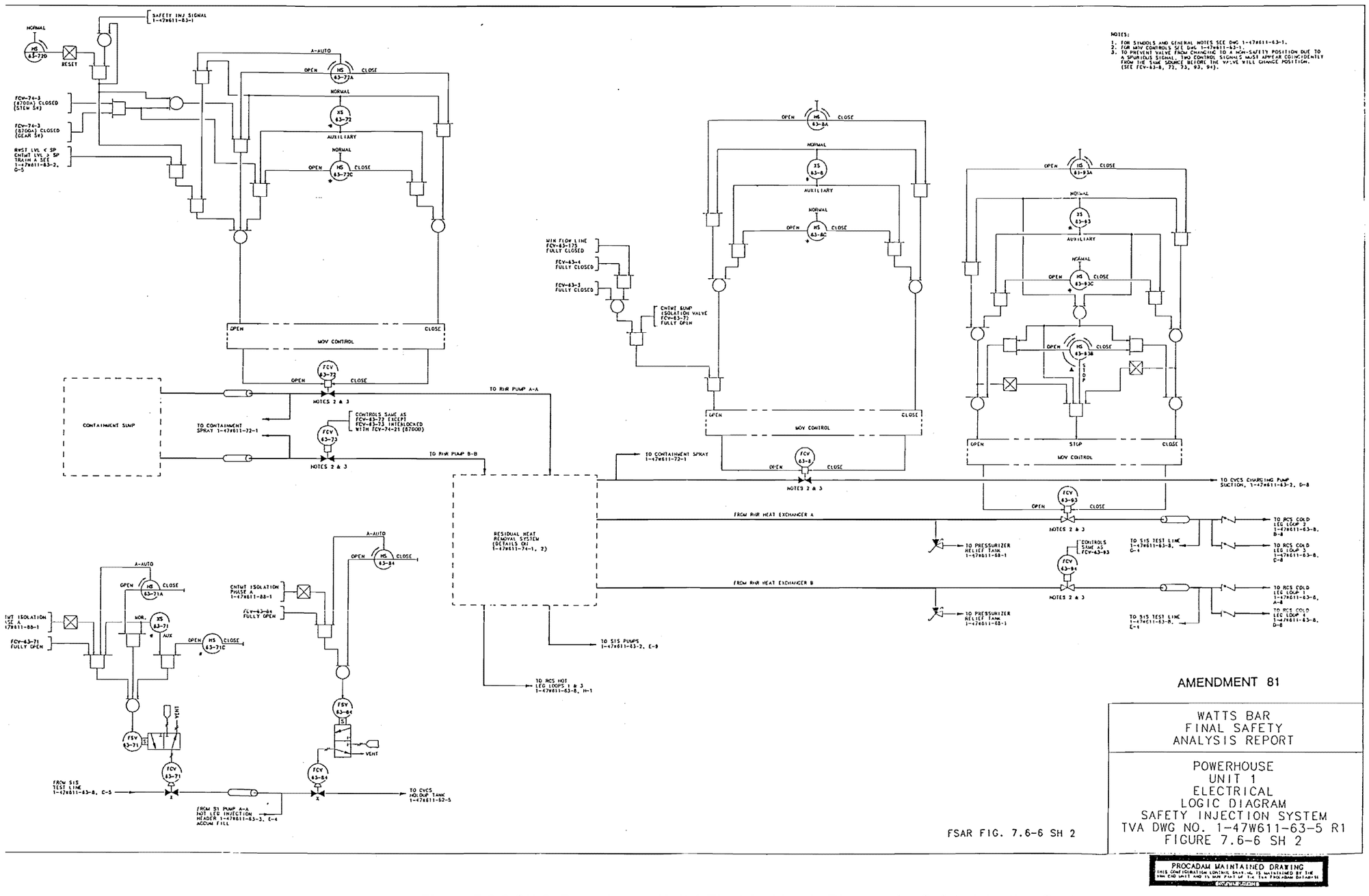


Figure 7.6-6-SH-2 Powerhouse Unit 1 Electrical Logic Diagram for Safety Injection System

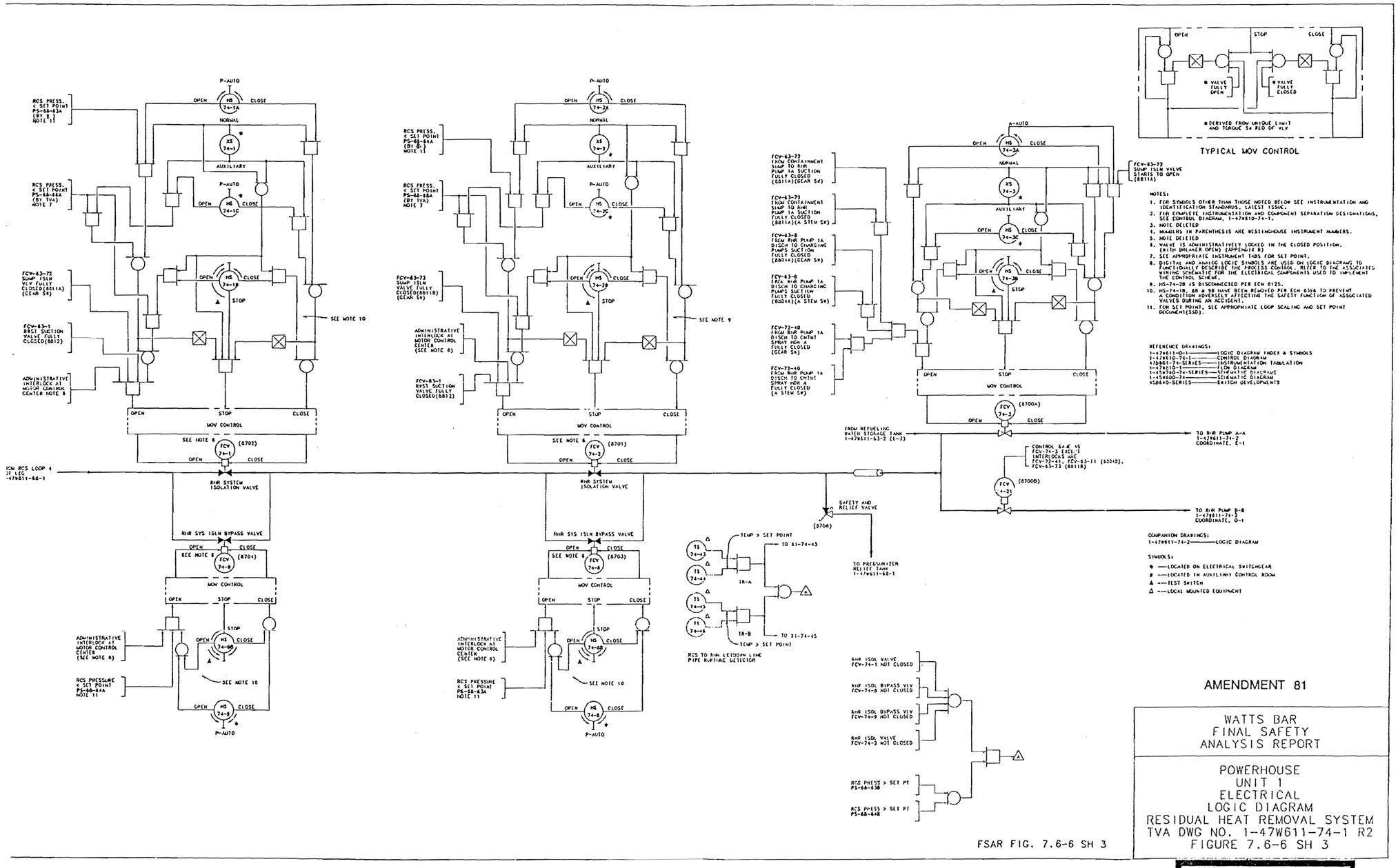
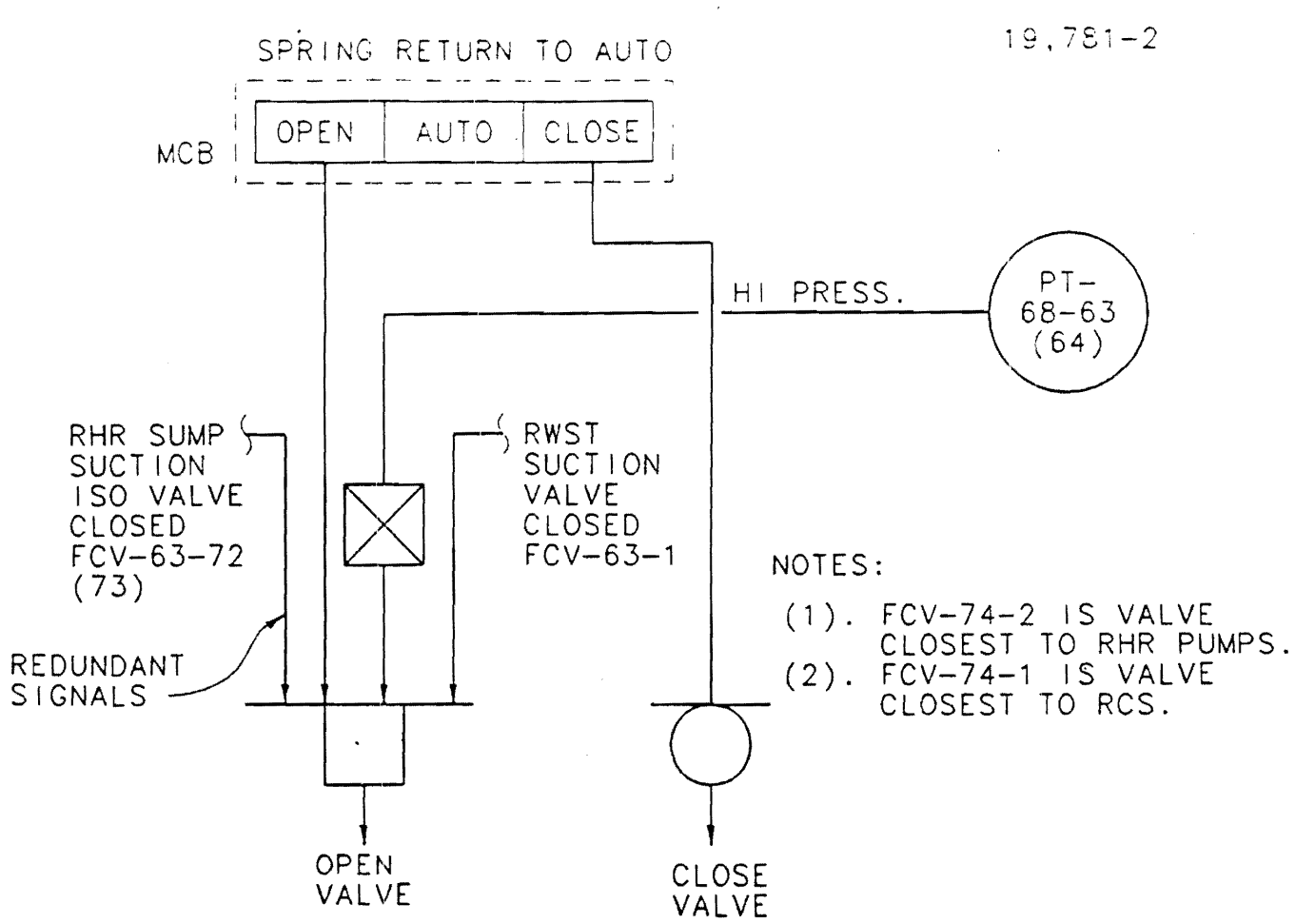


Figure 7.6-6-SH-3 Powerhouse Electrical Logic Diagram Residual Heat Removal System

PROCADAM MAINTAINED DRAWING
THIS CONFIGURATION CONTROL DRAWING IS MAINTAINED BY WBN CAD UNIT AND IS NOW PART OF THE TVA CADAM DATA BASE
Copyright 1992 TVA



(LIMIT SWITCH)

INTER-LOCKED WITH \ VALVE	FCV-74-1	FCV-74-2
RWST SUCTION VALVE	FCV-63-1 (LIMIT SWITCH)	FCV-63-1 (LIMIT SWITCH)
RHR SUMP SUCTION ISOLATION VALVE	FCV-63-72 (LIMIT SWITCH)	FCV-63-73 (LIMIT SWITCH)
RCS PRESSURE	PT-68-63	PT-68-64
POWER TRAIN	A	B

AMENDMENT 89

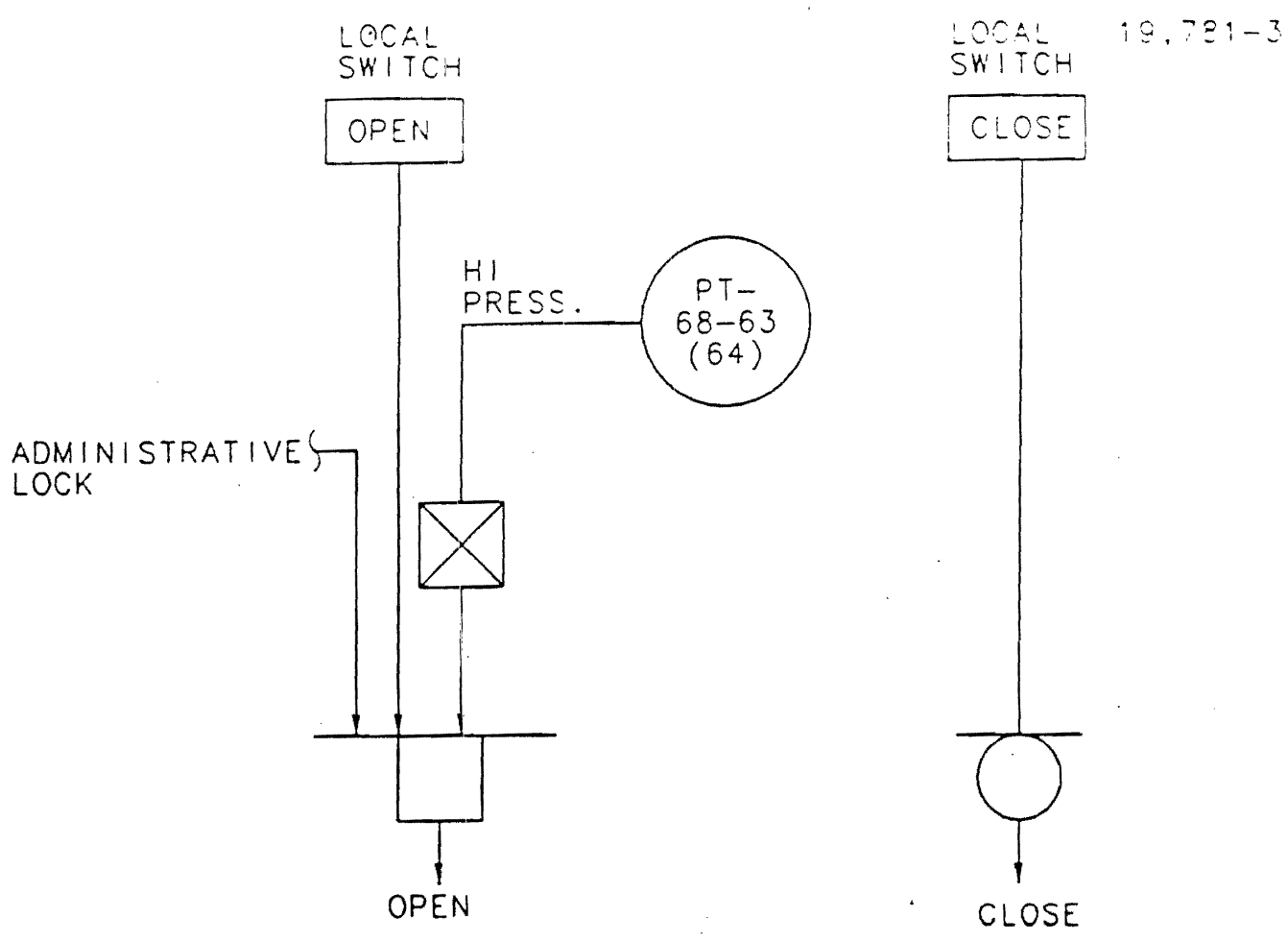
WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

RHR SUCTION ISOLATION
VALVE INTERLOCKS

FIGURE 7.6-7 (SHEET 1)

Figure 7.6-7-SH-1 RHR Suction Isolation Valve Interlocks

PROCADAM MAINTAINED DRAWING
THIS CONFIGURATION CONTROL DRAWING IS MAINTAINED
WBN CAD UNIT AND IS NOW PART OF THE TVA CADAM DA



INTER-LOCKED WITH \ VALVE	FCV-74-8	FCV-74-9
RCS PRESSURE	PT-68-63	PT-68-64
ADMINISTRATIVE LOCK	✓	✓
POWER TRAIN	A	B

NOTES:

(1). FCV-74-8 IS THE BYPASS VALVE FOR FCV-74-2.

(2). FCV-74-9 IS THE BYPASS VALVE FOR FCV-74-1.

AMENDMENT 89

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

RHR BYPASS VALVE LOGIC
FCV--74-8
(FCV--74-9)

FIGURE 7.6--7 (SHEET 2)

Figure 7.6-7-SH-2 RHR Bypass Valve Logic FCV-74-8 T (FCV-7 4-9)

7.7 CONTROL SYSTEMS

The general design objectives of the Plant Control Systems are:

(1) To establish and maintain power equilibrium between primary and secondary system during steady state unit operation;

(2) To constrain operational transients so as to preclude unit trip and re-establish steady state unit operation;

(3) To provide the reactor operator with monitoring instrumentation that indicates all required input and output control parameters of the systems and provides the operator the capability of assuming manual control of the system.

(4) To reduce the likelihood of failure to shutdown the reactor following anticipated transients and to mitigate the consequences of an Anticipated Transient Without Scram (ATWS) event.

7.7.1 Description

7.7.1.1 Control Rod Drive Reactor Control System

The control rod drive reactor control system consists of an automatic system designed to maintain a programmed average temperature in the reactor coolant system by regulating the core reactivity. During steady-state operation the reactor control system maintains reactor coolant average temperature within

± 3.5 °F of the reference temperature (see Reference 10).

This control system is designed to automatically control the reactor in the power range between 15 and 100% of rated power for the following design transients:

- ± 10% step change in load

- 5% per minute ramp loading and unloading

- 50% step load decrease (with the use of automatically initiated and controlled steam dump)

The reactor control signal consists of an error signal used to direct rod speed and position to automatically control reactor power. The two channels used to generate the total error signal are the deviation of the actual auctioneered (highest) primary coolant temperature (T_{avg}) from the programmed average temperature (T_{ref}) and the mismatch between turbine load and nuclear power (see Figure 7.7-1).

7.7.1.1.1 Reactor Control Input Signals

Average Temperature Channel - One average temperature measurement per reactor coolant loop is provided. This measurement is obtained by averaging the hot leg temperature (T_h) measured at the inlet of the steam generator and the cold leg

temperature (T_c) measured at the discharge side of the reactor coolant pump of the associated loop. All four average temperatures are passed into an auctioneering unit which generates the highest of the four-loop average temperature (T_{avg}) signals. (See Section 7.2.1.1.4 for detailed discussion of T_{avg} calculation and equations used to derive T_{avg}). This auctioneered T_{avg} signal is sent to a lead/lag unit which increases the effect of the signal. A second lag is provided to filter out signal noise. The above described signal:

$$T_{avg} \frac{(1 + t_3 s)}{(1 + t_4 s)(1 + t_5 s)} \text{ where } t = \text{time constant (typical)}$$

is then compared with a reference temperature (T_{ref}) signal. (The reference temperature is a function of turbine load, as described previously). Because the steam pressure in the impulse chamber of the high pressure turbine is linear with respect to the turbine load, this pressure signal is used to generate the reference average coolant temperature (T_{ref}). The reference temperature signal is passed through a lag before it is compared with the compensated T_{avg} signal. The resultant error signal is then:

$$T_{ref} \frac{1}{(1 + t_2 s)} - T_{avg} \frac{(1 + t_3 s)}{(1 + t_4 s)(1 + t_5 s)}$$

Power Mismatch Channel - This channel provides fast response to a change in load (by means of the turbine load feed-forward signal) as well as control stability (by means of the nuclear power feedback signal) in cases where the moderator coefficient is zero or is only slightly negative. Turbine load (Q_{tu}) and nuclear power (Q_n) provide input to this channel. Turbine load is represented by the impulse chamber pressure of the high pressure turbine, while the nuclear power signals are passed into an auctioneering unit which generates the highest of the four nuclear power signals.

This deviation between Q_{tu} and Q_n feeds a rate/lag (impulse) unit, thus creating the error signal:

$$(Q_{tu} - Q_n)\frac{t_1 s}{(1 + t_1 s)}$$

Because the T_{avg} channel provides fine control during steady-state operation, the power mismatch channel must not produce a steady-state error signal. This is accomplished by the derivative action in the numerator of the transfer function which causes the output of this unit to go to zero during steady-state operation although the nuclear power and turbine load may not match exactly. A nonlinear gain unit, K_1, placed at the output of the impulse unit, varies the effect of this channel with larger load changes having a correspondingly larger effect. Also, since reactivity changes at lower power levels have a smaller effect on the rate of change of the nuclear power level than reactivity changes at high power levels, a variable-gain unit, K_2, is provided at the output of the power mismatch channel.

The variable gain unit imposes a high gain on the power mismatch error signal at lower power levels and a low gain at high power levels. This variable gain enables the mismatch channel to provide adequate control at low power levels as well as stable operation at high power levels.

7.7.1.1.2 Rod Speed Control Program

Rod Speed Program - The total error signal (T_E) sent to the rod speed program is the sum of the outputs of the two control channels described above. The rod speed program is a function of the total error signal (T_E).

The dead band and lockup are provided to eliminate continuous rod stepping and bistable chattering. The maximum rod speed and the proportional and minimum rod speed bands are identical for rod withdrawal and rod insertion. The rod speed program produces an analog signal which is translated into actual movement by means of the rod stepping mechanism. The total error signal driving the rod speed program is represented in the following equation:

$$T_E = T_{ref}\frac{1}{(1 + t_s s)} - T_{avg}\frac{(1 + t_3 s)}{(1 + t_4 s)(1 + t_5 s)} + \left[(Q_{tu} - Q_n)\frac{(t_1 s)}{(1 + ts)}K_1 K_2\right]$$

7.7.1.2.1 Rod Control System

The rod control system is composed of equipment required to raise or lower the control rod and shutdown rod banks. Control rod banks can be automatically controlled from input signals generated by the reactor control system or by manual means from the unit control room. Shutdown control rods are controlled by manual means from the unit control room (see Reference 1).

The control scheme used to position the control rods is dependent on reactor power level. Manual control of control rod position is used when the reactor thermal power is between 0% and 15%. Above 15% reactor thermal power, automatic control may be used to position the control rods to maintain the average reactor coolant temperature (T_{avg}) within + 3.5°F of the reference temperature (T_{ref}).

The purpose of the rod control system is to provide the means for energizing the mechanism, thus controlling the rod cluster position. This system consists of two types of rod groups: 1) shutdown and 2) control. Shutdown rods along with soluble boron provides sufficient negative reactivity to ensure the reactor remains subcritical. The shutdown banks are fully withdrawn during normal operation. Control rods are used to control the reactor core reactivity. Shutdown and control rods are raised or lowered by a prescribed set of electromechanical actions by the CRD mechanisms.

The functional control requirements of the rod control systems are as follows:

- All control drive mechanisms within a group step simultaneously.
- Two groups within the same bank step such that the relative position of the groups does not differ by more than one step.
- The control banks are controlled such that withdrawal is sequenced in the order bank A, B, C, and D. The insertion sequence is the opposite of the withdrawal.
- The control bank withdrawal is controlled such that when Bank A reaches a preset position, Bank B will begin to withdraw simultaneously with Bank A. When bank B reaches a preset position, Bank C will begin to withdraw, etc. The reverse sequence will apply during bank insertion.
- Abnormal reactor conditions shall inhibit rod withdrawal. These conditions include 1) power range nuclear overpower, 2) intermediate range overpower, 3) overpower ΔT, and 4) overtemperature ΔT.
- Automatic control mode shall be inhibited when turbine power is less than 15%
- Automatic withdrawal shall be stopped when Bank D rod withdrawal exceeds a preset limit.

The bank overlap feature performs two functions; 1) it automatically selects the proper control bank for movement, and; 2) it overlaps the control banks which are to be moved according to a preset pattern. Bank overlap is required to keep the incremental changes in reactivity relatively constant while the control banks are being moved. Shutdown bank overlap operation is not required.

The bank overlap feature works as follows. Control bank A is withdrawn until it reaches a preset position near the center of the core. At this point, Control Bank B starts moving out in synchronism with Control Bank A. Control Bank A stops when it reaches the top of the core and Control Bank B continues until it reaches a preset position near the center of the core. At this point, Control Bank C moves out in synchronism with

Control Bank B. Control Bank B motion stops at the top of the core and Control Bank C sequencing continues until it nears the center position where Control Bank D engagement occurs. Control Bank C and D are withdrawn together until Control Bank C reaches the top of the core. Control Bank D withdrawal then continues as required for control. In the overlap region, group 1 rods of each of the two overlapped banks are stepping simultaneously; similarly, the group 2 rods of the two overlapped banks are stepped simultaneously.

In the manual mode, control bank stepping speed and shutdown bank stepping speed are preset. In the automatic mode (control banks, only), the rod stepping speed is variable between the limits of 8 to 72 steps per minute. The rod speed program of the reactor control system adjusts rod stepping speed to maintain a programmed average temperature in the reactor coolant system. The time required to complete a single sequencing of the rod mechanism coils is fixed at 780 milliseconds. This is the maximum reliable sequencing speed of the electro-mechanical components of the mechanisms. The time interval between mechanism coil sequencing operations is varied to obtain the desired rod speed.

Two motor-generator (MG) sets are used to supply 260V 3-phase AC power to the rod drive mechanisms. Each MG set is capable of delivering the total power requirements to the rod control system. Both MG sets are normally in operation. The motor is an induction type rated at 460 volt AC, 60 hertz. The motor is sized at 150 hp to drive the generator at a speed of 1750 rpm when the set is delivering rated power of 112 KVA.

7.7.1.2.2 Rod Control System Failures

Credible rod control equipment malfunctions which could potentially cause inadvertent positive reactivity insertions due to inadvertent rod withdrawal, incorrect overlap or malpositioning of the rods are the following (see Reference 5):

(1) Failures in the Manual Rod Controls

The Rod Motion Control Switch is a three position lever switch. The three positions are "In," "Hold," and "Out". These positions are effective when the bank selector switch is in manual. Failure of the rod motion control switch (contacts failing short or activated relay failures) would have the potential, in the worst case, to produce positive reactivity insertion by rod withdrawal when the bank selector switch is in the manual position or in a position which selects one of the banks.

When the bank selector switch is in the automatic position, the rods would obey the automatic commands and failures in the rod motion control switch would have no effect on the rod motion regardless of whether the rod motion control switch is in "In, " "Hold," or " Out".

In the case where the Bank Selector switch is selecting a bank and a failure occurs in the Rod Motion switch that would command the bank "Out" even when the Rod Motion Control switch was in an "In" or "Hold" position the selected bank could inadvertently withdraw. This failure is bounded in the

safety analysis (Chapter 15) by the uncontrolled bank withdrawal from subcritical and at power transients. A reactivity insertion of up to 75 pcm/sec is assumed in the analysis due to rod movement. This value of reactivity insertion rate is consistent with the withdrawal of two banks.

A failure that can cause more than one group of five 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. With a failure in the rod motion control switch, such a case could produce 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, overtemperature ΔT, or overpower ΔT.

A failure of the bank selector switch produces no consequences when the rod motion control 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. Results of switch failures in other control positions are discussed above in conjunction with the rod motion control switch.

(2) Failures in the Overlap and Bank Sequence Program Control

The rod control system design prevents the movement of the groups out of sequence as well as limiting the rate of reactivity insertion. The main feature that performs the function of preventing malpositioning produced by groups out of sequence is included in the block supervisory memory buffer and control. This circuitry accepts and stores the externally generated command signals. In the event of out of sequence input command to the rods while they are in movement, this circuit will inhibit the buffer memory from implementing 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. Any detected failure that affects the ability of the rod control system to properly move the rods is considered urgent. An urgent alarm will be followed by the following actions:

- Automatic rod motion and overlapped rod motion is stopped.
- Automatic de-energizing of the lift coil and reduced current energizing of the stationary gripper coils and movable gripper coils.
- Activation of a lamp (urgent failure) located on the logic and power cabinet front panel.
- Activation of control rod urgent failure annunciation window in the main control room.

The urgent alarm is produced by the following general conditions:

- Regulation failure detector
- Phase failure detector
- Logic error detector
- Multiplexing error detector
- Circuit board interlock failure detector
- Oscillator and slave cycler failure detector.

(a) Logic Cabinet

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 cycler while it is sequencing its mechanisms through a 780 millisecond step. This condition stops the control bank motion automatically and alarms are activated locally and in the control room. It also causes the affected slave cycler to reject further 'GO' pulses until it is reset.

Failures that cause the 780 millisecond stop 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.

The positive reactivity insertion rates for these failure modes, including the 100 steps per minute, are bounded by the analysis assumptions in Chapter 15.

Failures Causing Movement of the Rods Out of Sequence

No single failure was discovered (Reference [5]) 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 Failure Alarm.

(b) 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 the power cabinet is 'fail-preferred' in regard 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. No failure within the power cabinet which could cause erroneous drive mechanism operation will remain undetected. Sufficient alarm monitoring (including 'urgent' alarm) is provided in the design of the power cabinet for fault detection of those failures which could cause erroneous operation of a group of mechanisms. As noted in the foregoing, diverse monitoring systems are available for detection of failures that cause the erroneous operation of an individual control rod drive mechanism.

Conclusion

In summary, no single failure within the rod control system can cause either reactivity insertions or malpositioning of the control rods resulting in core thermal conditions not bounded by analyses contained in Chapter 15.

7.7.1.3 Plant Control Signals for Monitoring and Indicating

7.7.1.3.1 Monitoring Functions Provided by the Nuclear Instrumentation System

The Nuclear Instrumentation System (NIS) is safety-related because signals are sent to the solid state protection system used to generate a reactor trip. Refer to Section 7.2 for discussion of reactor protection features. The NIS is described in References [2] and [11].

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 power imbalance, and radial power 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:

(1) Total current from a power range detector (four such signals from separate detectors); these detectors are vertical and have an active length of 10 feet.

(2) Current from the upper half of each power range detector (four such signals).

(3) Current from the lower half of each power range detector (four such signals).

The following indications are derived from these basic signals:

(1) Indicated nuclear power (four such).

(2) Indicated axial flux imbalance, derived from upper half flux minus lower half flux (four such).

Alarm functions derived are as follows:

(1) Deviation alarm (maximum minus minimum of four detector outputs)

(2) Upper radial tilt alarm (maximum to average of four) on detector upper-half currents.

(3) Lower radial tilt alarm (maximum to average of four) on lower-half currents.

Provision is made to continuously record, on strip charts on the control board, the 8 ion chamber signals, i.e., upper and lower currents for each detector. Nuclear power and axial unbalance is selectable for recording as well. Indicators are provided on the control board for nuclear power and for axial power imbalance.

The axial flux difference imbalance deviation $\Delta\varphi$ alarms are derived from the plant process computer which determines the 1 minute averages of the excore detector outputs to monitor $\Delta\varphi$ in the reactor core and alerts the operator where $\Delta\varphi$ alarm conditions exist.

7.7.1.3.2 Main Control Room Rod Position Indication

Two separate systems are used to indicate rod position information in the main control room. One system measures the actual drive rod position as part of the Rod Position Indicator System (RPIS). The second system counts and displays the pulses for rod movement generated in the logic cabinet.

(1) Rod Position Indication System (RPIS)

The position of each rod (57) [Shutdown and Control banks] is displayed on vertical scale indicators. These indicators receive an analog signal from sensors mounted on the rod drive mechanism. The scale is in units of steps and covers the entire range of travel.

Additionally, a rod bottom indicator light for each rod (57) is energized to indicate a rod is near the fully inserted position.

(2) Rod Position Step Counter

The position demand signal for each rod group (14) is displayed on a 3-digit, add-subtract step counter. The input signal is supplied from the logic cabinet circuitry.

The demand position and rod position indication systems are separate systems;

The demand position indication system is described in detail in Reference [3].

7.7.1.3.3 Control Bank Rod Insertion Monitoring

When the reactor is critical, the normal indication of reactivity status in the core is the position of the control bank in relation to reactor power (as indicated by the reactor coolant system loop ΔT) and coolant average temperature. These parameters are used to calculate insertion limits for the control banks. Two alarms are provided for all control banks.

(1) The "Rod Insertion Limit Lo" annunciation alerts the operator of an approach of one or more control bank rods to the insertion limit. This annunciation precedes the "Lo-Lo" annunciation by a preset number of steps.

(2) The "Rod Insertion Limit Lo-Lo" annunciation alerts the operator that one or more control bank rods are positioned below the insertion limit. Corrective measures are to be taken after verifying that rod insertion limits are violated.

The purpose of the control bank rod insertion monitor is to give warning to the operator of excessive rod insertion. The insertion limit maintains sufficient core reactivity, shutdown margin, following reactor trip and provides a limit on the maximum inserted rod worth in the unlikely event of 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 ΔT between the hot leg and the cold leg, which is a direct function of reactor power, and T_{avg} which is programmed as a function of power. The rod insertion monitor uses parameters for each control rod bank as follows:

$$Z_{LL} = K_1 (T_{avg} - 557°F) + K_2 (\%\Delta T) + K_3 \text{ (see Reference 10)}$$

where:

Z_{LL} = maximum permissible insertion limit (steps withdrawn)

T_{avg} = highest average temperature of all loops (auctioneered)

ΔT = highest ΔT of all loops (auctioneered)

K_1, K_2, K_3 = Constants based on physics calculation

The control bank position (steps withdrawn), Z, is compared to calculated Z_{LL} as follows for alarm:

Low Alarm

$Z_{Low} = Z_{LL} + K_4$

Low-Low Alarm

$Z_{Low\text{-}Low} = Z_{LL} + K_5$

Where:

K_4, K_5 = Constants to allow alarms to occur prior to reaching insertion limit (steps).

Since the highest values of T_{avg} and ΔT are chosen by auctioneering, a conservatively high representation of power is used in the insertion limit calculation.

Actuation of the low alarm alerts the operator of an approach to a reduced shutdown reactivity situation. Administrative procedures require the operator to evaluate the need to add boron through the chemical and volume control system. Actuation of the low-low alarm requires the operator to initiate immediate boration procedures after verifying the rod insertion limits are violated. The value for K_5 is chosen such that the low-low alarm would normally be actuated before the insertion limit is reached. The value for K_4 is chosen to allow the operator to follow normal boration procedures. Figure 7.7-2 shows a block diagram representation of the control rod bank insertion monitor. In addition to the rod insertion monitor for the control banks, an alarm system is provided to warn the operator if any shutdown rod cluster control assembly leaves the fully withdrawn position.

Rod insertion limits are established by:

(1) The allowed rod reactivity insertion at full power consistent with the purposes given above.

(2) The differential reactivity worth of the control rods when moved in normal sequence.

(3) The change in reactivity with power level by relating power level to rod position.

(4) Linearizing the resultant limit curve. Key nuclear parameters used in establishing the limit curve are measured as part of the initial physics testing program and periodic surveillance 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

A rod deviation annunciation is actuated in the main control room when; 1) the deviation between the actual rod position and the bank demand position (control banks rods) exceed a preset value, or 2) the deviation between any two rods within a control bank exceed a preset value.

Figure 7.7-3 is a block diagram of the rod deviation comparator and alarm system.

7.7.1.3.5 Rods At Bottom

A "Rods At Bottom" annunciation is actuated in the main control room when any of the shutdown and control bank rods are near the fully inserted position. The rod bottom bistable monitors the analog rod position signal generated by the RPIS and actuates this alarm when the rods are positioned below the setpoint. (The rod bottom bypass bistable module is used to block this alarm signal for control banks B, C, and D).

7.7.1.3.6 Bypassed and Inoperable Status Indication System (BISI)

Refer to Section 7.5 for description of BISI.

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'.

7.7.1.4.1 Rod Stops

Rod stops are provided to inhibit control rod withdrawal under certain abnormal operating conditions. Refer to Table 7.7-1 for description of each interlock.

7.7.1.4.2 Automatic Turbine Load Runback

Automatic turbine load runback is initiated by an approach to an overpower or overtemperature condition. This will prevent high power operation that might lead to an undesirable condition, which, if reached, will be protected by reactor trip.

Turbine load reference reduction is initiated by either an overtemperature or overpower ΔT signal. Two out of four coincidence logic is used.

A rod stop and turbine runback are initiated when:

$$\Delta T > \Delta T_{rod\ stop}$$

for both the overtemperature and the over power condition.

For either condition in general:

$\Delta T_{rod\ stop} = \Delta T_{setpoint} - B_p$

where:

B_p = a setpoint bias

$\Delta T_{setpoint}$ = the overtemperature ΔT reactor trip value and the overpower ΔT reactor trip value for the two conditions.

The turbine runback will continue to cycle to maintain stability until ΔT is equal to or less than ΔT_{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 remaining (backup) heaters are energized on pressurizer level deviation or when the pressurizer pressure controlled signal demands approximately 100% proportional heater power.

The spray nozzles are located on the top of the pressurizer. Spray is initiated when the pressure controller spray demand signal is above a given setpoint. The spray rate increases proportionally with increasing spray demand signal until it reaches a maximum value.

Steam condensed by the spray reduces the pressurizer pressure. A small continuous spray is normally maintained to reduce thermal stresses and thermal shock and to help maintain uniform water chemistry and temperature in the pressurizer.

Power operated relief valves limit system pressure for large positive pressure transients. In the event of a large load reduction, not exceeding the design plant load rejection capability, the pressurizer power operated relief valves might be actuated for the most adverse conditions, e.g., the most negative Doppler coefficient, and the maximum incremental rod worth. The relief capacity of the power operated relief valves is sized large enough to limit the system pressure to prevent actuation of high pressure reactor trip for the above condition.

A block diagram of the pressurizer pressure control system is shown on Figure 7.7-4. See Reference [9].

7.7.1.6 Pressurizer Water Level Control

The pressurizer operates by maintaining a steam cushion over the reactor coolant. As the density of the reactor coolant adjusts to the various temperatures, the steam water interface moves to absorb the variations with relatively small pressure disturbances.

The water inventory in the reactor coolant system is maintained by the chemical and volume control system. During normal plant operation, the charging flow varies to produce the flow demanded by the pressurizer water level controller. The pressurizer water level is programmed as 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 controlled from the main control room.

A block diagram of the pressurizer water level control system is shown on Figure 7.7-5. See Reference [9].

7.7.1.7 Steam Generator Water Level Control

Each steam generator is equipped with a three element feedwater flow controller which maintains a programmed water level which is a function of nuclear power. The three element feedwater controller regulates the feedwater valve by continuously comparing the feedwater flow signal, the steam generator water level signal, the programmed level and the pressure compensated steam flow signal. In addition, 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 ΔP with a programmed ΔP_{ref} which is a linear function of steam flow. Continued delivery of feedwater to steam generators is required as a sink for the heat stored and generated in the reactor following a reactor trip and turbine trip. An override signal closes the feedwater valves when the average coolant temperature is below a given temperature and the reactor has tripped. Manual override of the feedwater control system is available at all times.

Three steam generator water level signals are provided to the feedwater control system via a control grade Median Signal Selector (MSS). The MSS installed in the control system provides a "median" signal for use by the control system to initiate control system actions based on this signal (Reference [6]). For the evaluation of the compliance of steam generator low-low water level channels to Section 4 (Control and Protection System Interaction) of IEEE Standard 279-1971, refer to Section 7.2.

A block diagram of the steam generator water level control system is shown in Figures 7.7-6 and 7.7-7. See Reference [8].

7.7.1.8 Steam Dump Control

The steam dump system has 40% steam dump capacity to the condenser (i.e., 40% of rated full load steam flow can be passed at full load steam pressure when all of the steam dump valves are discharging steam). This allows the NSSS to withstand an external load step reduction of up to 50% of plant rated electrical load (10% NSSS load step capability plus 40% steam dump) without reactor trip or safety valve actuation.

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.

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 valve corresponding to a 10% step load decrease.

A block diagram of the steam dump control system is shown Figure 7.7-8. See Reference [7].

7.7.1.8.1 Load Rejection Steam Dump Controller

This circuit prevents a large increase in reactor coolant temperature following a large, sudden load decrease. The error signal is a difference between the lead/lag compensated auctioneered T_{avg} and the 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, the load rejection steam dump controller is defeated and the plant trip steam dump controller becomes active. The demand signal is the error signal between the lead/lag compensated auctioneered T_{avg} and the no load reference T_{avg}. When the error signal exceeds a predetermined setpoint the dump valves are tripped open in a prescribed sequence. As the error signal reduces in magnitude indicating that the reactor coolant system T_{avg} is being reduced toward the reference no-load value, the dump valves are modulated by the plant trip controller to regulate the rate of removal of decay heat and thus gradually establish the equilibrium hot shutdown condition.

Following a plant trip, only sufficient steam-dump capacity is necessary to maintain steam pressure below the steam-generator relief-valve setpoint (approximately 40% capacity to the condenser). The error signal determines whether a group is to be tripped open or modulated open. The valves are modulated when the error is below the trip-open setpoints.

7.7.1.8.3 Steam Header Pressure Controller

Residual heat removal is maintained by the steam generator pressure controller (manually selected), which controls the amount of steam flow to the condensers. This controller operates a portion of the same steam dump valves to the condensers, which are used during the initial transient following turbine-reactor trip or 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. References [4] and [12] provide additional information on the incore instrumentation system.

7.7.1.9.1 Thermocouples

The incore themocouple system is a Post Accident Monitoring (PAM) safety related monitoring system. Refer to Section 7.5.

Chromel-Alumel thermocouples are threaded into guide tubes that penetrate the reactor vessel head through seal assemblies, and terminate at the exit-flow end of the fuel assemblies. The thermocouples are supported in guide tubes in the upper core support assembly.

The thermocouple cables, connectors, reference junction boxes inside the containment, and cables outside the containment up to the Inadequate Core Cooling Monitor (ICCM) cabinets are environmentally qualified and in compliance with 10CFR50.49. The thermocouple cables maintain adequate separation between post-accident monitoring channels I and II (PAM I and PAM II) after exiting the reactor cavity biological shield wall. Thermocouple readings will be monitored by a plasma display screen (separate for PAM I and PAM II channels) in the main control room. Two three-pen recorders and the plant computer are also available.

7.7.1.9.2 Movable Neutron Flux Detector Drive System

The flux mapping system is a quality-related system. The portion of the system that interfaces with the reactor coolant system pressure boundary is safety related.

Miniature fission chamber detectors can be remotely positioned in retractable guide thimbles to provide flux mapping of the core. See Reference [4] for neutron flux detector parameters. The stainless steel detector shell is welded to the leading end of helical wrap drive cable and to stainless steel sheathed coaxial cable. The retractable

thimbles, into which the miniature detectors are driven, are pushed into the reactor core through conduits which extend from the bottom of the reactor vessel down through the concrete shield area and then up to a thimble seal table.

The thimbles are closed at the leading ends, 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, five path rotary transfer assemblies, and ten path rotary transfer assemblies, as shown in Figure 7.7-9. These assemblies are described in Reference [4]. The drive system pushes hollow helical wrap drive cables into the core with the miniature detectors attached to the leading ends of the cables and small diameter sheathed coaxial cables threaded through the hollow centers back to the ends of the drive cables. Each drive assembly consists of a gear motor which pushes a helical wrap drive cable and a detector through a selective thimble path by means of a special drive box and includes a storage device that accommodates the total drive cable length.

Leakage detection of reactor coolant is discussed in Reference [4].

Manual isolation valves (one for each thimble) are provided for closing the thimbles. When closed, each valve forms a 2500 psig barrier. The manual isolation valves are not designed to isolate a thimble while a detector/drive cable is inserted into the thimble. The detector/drive cable must be retracted to a position above the isolation valve prior to closing the valve. A small leak would probably not prevent access to the isolation valves and thus a leaking thimble could be isolated. A large leak might require cold shutdown for access to the isolation valve.

7.7.1.9.3 Control and Readout Description

The control and readout system provides means for inserting the miniature neutron detectors into the reactor core and withdrawing the detectors while plotting neutron flux versus detector position. The thimbles are distributed nearly uniformly over the core with about the same number of thimbles in each quadrant. The control system consists of two sections, one physically mounted with the drive units, and the other contained in the control room. Limit switches in each transfer device provide feedback of path selection operation. Each gear box drives an encoder for position feedback. One five-path operation selector is provided for each drive unit to insert the detector in one of five functional modes of operation. A ten-path rotary transfer assembly is a transfer device that is used to route a detector into any one of up to ten selectable paths. A common path is provided to permit cross calibration of the detectors.

The control room contains the necessary equipment for control, position indication, and flux recording for each detector. Additional panels are provided for such features as drive motor controls, core path selector switches, plotting and gain controls.

A "flux-mapping" consists, briefly, of selecting (by panel switches) flux thimbles in given fuel assemblies at various core quadrant locations. The detectors are driven to the top of the core and stopped automatically. An x-y plot (position versus flux level) is initiated with the slow withdrawal of the detectors through the core from top to a point below the bottom. In a similar manner other core locations are selected and plotted. Each detector provides axial flux distribution data along the center of a fuel assembly.

Various radial positions of detectors are then compared to obtain a flux map for a region of the core.

Operating plant experience has demonstrated the adequacy of the incore instrumentation in meeting the design bases stated.

7.7.1.10 Control Board

A typical control board functional layout is shown on Figure 7.7-10.

The control board layout is based on operator ease in relating the control board devices to the physical plant and in determining at a glance the status of related equipment. This is referred to as providing a functional layout. Within the boundaries of a functional layout, modules are arranged in columns of control functions associated with separation trains defined for the RPS and ESFAS.

Monitor lights are provided in two places on the control board for automatically actuated valves and components for Phase A and B containment isolation and containment vent isolation, with the exception of all sampling and water quality system valves as well as those EGTS valves that are not in the containment annulus vacuum fans flowpath. Indicating circuits are paralleled to red (open) and green (closed) lights located next to the control station and to red and green split lens lights on the Containment Isolation Status Panel (CISP).

EGTS containment isolation valves not in the containment annulus vacuum fans flowpath have red and green position indication lights located on the control board at the control station.

Position indication for the sampling and water quality system containment isolation valves is provided by paralleling indicating circuits to red and green lights at the local control station in the Auxiliary Building and to red and green split-lens lights on the CISP.

For a description of separation of wiring within the control board refer to Section 7.1.

7.7.1.11 Boron Concentration Measurement System

The boron analyzer, as described below, is not used for Unit 1 operations, and is not used in identifying boron concentration in RCS. During full power operations, primary system sampling is conducted once every week to determine boron concentration. Since periodic sampling can effectively measure boron concentration in RCS, the boron analyzer is not relied upon to provide indications of boron concentration. Periodic sampling is described in Section 9.3.2.2.

The boron concentration measurement system is a monitoring system of the boron concentration in the RCS. This system is provided by Combustion Engineering and provides continuous readout in the MCR of boron concentration in the RCS for the reactor operator. This system provides no control function. The boron concentration in the reactor coolant system is measured in the letdown stream of the CVCS. In addition to the continuous readout in the MCR, a strip chart recorder with the boron concentration in the RCS is provided so that trends in the boron concentration can be monitored by the control room operator.

7.7.1.12 Anticipated Transient Without Scram Mitigation System Actuation

Circuitry (AMSAC) (Reference 13)

To meet the ATWS final rule, Watts Bar added equipment diverse from the existing reactor trip system. The existing reactor trip system is composed of the Westinghouse Eagle 21 process protection system, and the Westinghouse Solid State Protection System (SSPS). The AMSAC equipment consists of a freestanding panel which is installed in the Unit 1 auxiliary instrument room of the Control Building. This modification is diverse from sensor output to the final actuation device. The AMSAC is designed to automatically initiate auxiliary feedwater and trip the turbine under conditions indicative of an ATWS event. An ATWS event will be detected when low-low level in three out of four steam generators is coincidental with the turbine at or above 40% load. An AMSAC actuation will ensure the RCS pressure will remain below the pressure that will satisfy the ASME Boiler and Pressure Vessel Code Level C services limit stress criteria.

A turbine trip and startup of all AFW pumps occurs upon generation of an AMSAC signal. The AMSAC signal is generated by low-low water level signals in the steam generators. The AMSAC coincidence logic is 3 out of 4 (3/4) low-low level signals with one channel per steam generator and the turbine at or above 40% load. Load is determined by two pressure transmitters measuring first stage turbine pressure. When 2 of 2 transmitters sense 40% load, AMSAC is armed. Removal of the AMSAC arming signal is delayed for a specified time so that AMSAC will stay armed and be capable of performing its function after turbine trip or power reduction below 40% power. Only one of the three narrow range level channels per steam generator is used for input to AMSAC coincidence logic. AMSAC actuation is required at a setpoint that is less than the existing RPS steam generator low-low level setpoint. The requirement allows the operation of the RPS before AMSAC. AMSAC actuation is delayed for a specified time to further ensure RPS operation prior to AMSAC.

There is no AMSAC interface to the RPS. The four steam generator level signals are from isolation devices in the auxiliary feedwater system. Signals from two dedicated turbine impulse chamber pressure transmitters are used to indicate if the plant is at or above 40% load and then to determine the trip setpoint. The output signals to start the auxiliary feedwater pumps and trip the turbine are from interposing relays.

AMSAC is designed so that once actuated, the completion of mitigating action shall be consistent with the plant turbine trip and auxiliary feedwater circuitry. AMSAC auxiliary feedwater initiation and turbine trip goes to completion after actuation. The output

relays are energized to actuate in order to prevent spurious trips and false status indication on loss of power or logic.

The AMSAC contains a manual test panel and built in self checks to annunciate faults automatically. On-line testing capability for each train is incorporated in the AMSAC system. The blocking switch prevents inadvertent actuation by inhibiting the output relays before enabling the test function. A test status output shall inform the control room that the AMSAC is in the test mode and actuation is bypassed.

AMSAC is powered from 120V ac preferred power which is independent from the RPS power supply.

The AMSAC system, including input comparators, logic processing and actuation output to isolation relays, is non-safety. The QA requirements are given in NRC Generic Letter 85-06, "Quality Assurance Guidance of ATWS Equipment that is not Safety-Related." The AMSAC cabinet is qualified seismic Category I(L).

The TVA Watts Bar AMSAC design generally conforms to the Westinghouse Owners Group (WOG) Topical Report WCAP-10858 P-A, "AMSAC Generic Design Packages".

7.7.2 Analysis

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 indicators for each rod cluster control assembly. A rod deviation alarm alerts the operator of a deviation of one rod cluster control assembly from the other rod assemblies in that bank position. There are also insertion limit monitors with visual and audible annunciation. A rod bottom alarm signal is provided to the control room for each 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 uses input signals including neutron flux, coolant temperature, and turbine load.

The plant control systems will prevent an undesirable condition in the operation of the plant that, if reached, will be protected by reactor trip. The description and analysis of this protection is covered in Section 7.2. Worst case failure modes of the plant control systems are postulated in the analysis of off-design operational transients and accidents covered in Chapter 15, such as, the following:

(1) Uncontrolled rod cluster control assembly withdrawal from a subcritical condition

(2) Uncontrolled rod cluster control assembly withdrawal at power

(3) Rod cluster control assembly misalignment

(4) Loss of external electrical load and/or turbine trip

(5) Loss of all ac power to the station auxiliaries (station blackout)

(6) Excessive heat removal due to feedwater system malfunctions

(7) Excessive load increase incident

(8) Accidental depressurization of the reactor coolant system.

These analyses will show that a reactor trip setpoint is reached in time to protect the health and safety of the public under those postulated incidents and that the resulting coolant temperatures produce a DNBR well above the limiting value. 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 devices contained in the protection channel. As such, a failure in the control circuitry does not adversely affect the protection channel. Test results have demonstrated that short circuits or the application of fault voltages up to 150 volts dc or 120 volts ac on the isolated output portion of the circuit (nonprotection side) will not affect the input (protection) side of the circuit. Cable trays carrying isolation device outputs will contain no cables in excess of these voltages.

Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels are capable of providing the protective action even when degraded by a second random failure. This meets the applicable requirements of Section 4.7 of IEEE Standard 279-1971 and Criterion 24 of the 1971 GDC. Specific control and protection system interactions are discussed in Section 7.2.2.3.

7.7.2.2 Response Considerations of Reactivity

Reactor trip shutdown with control rod insertion 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 Criteria 25.

The control rod drive system is designed to minimize the effects of a single electrical or mechanical failure in the rod control system that 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 would result in activation of the same alarm and the same visual indications.

Each bank of control and shutdown rods in the system is divided into two groups (group 1 and group 2) of up to 4 or 5 mechanisms each. The rods comprising a group operate in parallel through multiplexing thyristors. The two groups in a bank move sequentially such that the first group is always within one step of the second group in the bank. The group 1 and group 2 power circuits are installed in different cabinets as shown in Figure 7.7-11, which also shows that one group is always within one step (5/8 inch) of the other group. A definite schedule of actuation or deactuation of the stationary gripper, moveable gripper, and lift coils of a mechanism is required to withdraw the rod cluster control assembly attached to the mechanism. Since the stationary gripper, moveable 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 7.7-12 is provided for the following discussion associated with design features that minimize the effects of a single electrical failure that could cause the accidental withdrawal of a single rod cluster control assembly from the partially inserted bank at full power operation.

The Figure 7.7-12 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 address the lift coil circuits. 1) Due to the method of wiring the pulse transformers which fire the lift coil multiplex thyristors, three of the four thyristors in a rod group could remain turned off when required to fire, if for example the gate signal lead failed open at point X_1. Upon "up" demand, one rod in group 1 and 4 rods in group 2 would withdraw. A second failure at point X_2 in the group 2 circuit is required to withdraw one rod cluster control assembly; 2) Timing circuit failures will affect the four mechanisms of a group or the eight mechanisms of the bank and will not cause a single rod withdrawal; 3) More than two simultaneous component failures are required (other than the open wire failures) to allow withdrawal of a single rod.

The identified multiple failure involving the least number of components consists of open circuit failure of the proper two out of sixteen wires connected to the gate of the lift coil thyristors. The probability of open wire (or terminal) failure is 0.016×10^{-6} per hour by MILHDB217A. These wire failures would have to be accompanied by failure, or disregard, of the indications mentioned above. The probability of this occurrence is therefore too low to have any significance.

Concerning the human element, to erroneously withdraw a single rod cluster control assembly, the operator would have to improperly set the bank selector switch, the lift coil disconnect switches, and the in-hold-out switch. In addition, the three indications would have to be disregarded or ineffective. Such series of errors would require a complete lack of understanding and administrative control. A probability number cannot be assigned to a series of errors such as these.

The rod position indication system provides direct visual displays of each control rod assembly position. The plant computer alarms for deviation of rods from their banks. In addition a rod insertion limit monitor provides an alarm to warn the operator of an approach to an abnormal condition due to dilution. The low-low insertion limit alarm alerts the operator to follow immediate boration procedures. 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 indicators, 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 that bank by a preset limit, 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 system which is independent of the plant computer.

Isolated signals derived from the nuclear instrumentation system are compared with one another to determine if a preset amount of deviation of average power level has occurred. Should such a deviation occur, the comparator output will operate a bistable unit to actuate a control board annunciator. This alarm will alert the operator to a power imbalance caused by a misaligned rod. By use of individual rod position indicators, the operator can determine the deviating control rod and take corrective action. The design of the plant control systems meets the requirements of the 1971 General Design Criteria 23.

The boron system can compensate for all xenon burnout reactivity transients.

The rod system can compensate for xenon burnout reactivity transients over the allowed range of rod travel. Xenon burnout transients of larger magnitude must be accommodated by boration or by reactor trip (which eliminates the burnout).

The boron system is not used to compensate for the reactivity effects of fuel/water temperature changes accompanying power level changes.

The rod system can compensate for the reactivity effects of fuel/water temperature changes accompanying power changes over the full range from full load to no load at the design maximum load uprate.

The boron system can maintain the reactor in the cold shutdown state irrespective of the disposition of the control rods.

7.7.2.3 Step Load Changes Without Steam Dump

The reactor control system is designed to automatically control the reactor, without a trip, following a ± 10% step load change over a 15% to 100% power range. 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 and heaters and power relief valves in the pressurizer.

7.7.2.4 Loading and Unloading

Ramp loading and unloading of 5% per minute can be accommodated 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 increases during loading and causes a continuous insurge to the pressurizer as a result of coolant expansion. The sprays limit the resulting pressure increase. Conversely, as the coolant average temperature is decreasing during unloading, there is a continuous outsurge from the pressurizer resulting from coolant contraction. The pressurizer heaters limit the resulting system pressure decrease. The pressurizer water level is programmed such that the water level is above the setpoint for heater cut out during the loading and unloading transients. The primary concern during loading is to limit the overshoot in nuclear power and to provide sufficient margin in the overtemperature ΔT setpoint.

The automatic load controls are designed to adjust the unit generation to match load requirements within the limits of the unit capability and licensed rating.

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 full load steam pressure.

The steam dump flow drops proportionally as the control rods act to reduce the average coolant temperature. The artificial load is therefore removed as the coolant average temperature is restored to its programmed equilibrium value.

The dump valves are modulated in accordance with the error signal developed by the difference between the reactor coolant average temperature and reactor coolant reference temperature. The required number of steam dump valves can be tripped quickly to stroke full open or modulate, depending upon the magnitude of the temperature error signal resulting from loss of load.

7.7.2.6 Turbine-Generator Trip With Reactor Trip

Whenever the turbine-generator trips at an operating power-level above 50% power, the reactor also trips. The unit is operated with a programmed average temperature as a function of load, with the full load average temperature significantly greater than the equivalent saturation pressure of the safety valve setpoint. The thermal capacity of the 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 impulse pressure. Actuation of the steam dump is rapid to prevent actuation of the steam generator safety valves. With the dump valves open, the average coolant temperature starts to reduce quickly to the no load setpoint. A direct feedback of temperature acts to proportionally close the valves to minimize the total amount of steam which is bypassed.

Following the reactor trip, the feedwater flow is cut off when the average coolant temperature decreases below a given temperature or when the steam generator water level reaches a given high level.

Additional feedwater makeup is then controlled manually to restore and maintain steam generator water level while assuring that the reactor coolant temperature is at the desired value. Residual heat removal is maintained by the steam header pressure controller (manually selected) which controls the amount of steam flow to the condensers. This controller operates a portion of the same steam dump valves to the condensers which are used during the initial transient following turbine and reactor trip.

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 low level safety injection setpoint. If 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 prevent the average coolant temperature from falling below the programmed no load temperature following the trip to ensure adequate shutdown margin.

7.7.3 Deleted by Amendment 81

REFERENCES

(1) Blanchard, A. E. and Katz, D. N., "Solid State Rod Control System, Full Length," WCAP-9012-L, March, 1970 (Proprietary) and WCAP-7778, December, 1971 (Non-Proprietary).

(2) Lipchak, J. B. and Stokes, R. A., "Nuclear Instrumentation System", WCAP-8255, January, 1974. (Applicable to Power Range NIS Only.)

(3) Blanchard, A. E., "Rod Position Monitoring", WCAP-7571, March, 1971.

(4) Loving, J. J., "Incore Instrumentation Flux-Mapping System and Thermocouples", WCAP-7607, July, 1971.

(5) Shopsky, W. E., "Failure Mode and Effects Analysis (FMEA) of the Solid State Full Length Rod Control System", WCAP-8976, August 1977.

(6) Mermigos, J. F., "Median Signal Selector for Foxboro Series Process Instrumentation Application to Deletion of Low Feedwater Flow Reactor Trip," WCAP-12417 October 1989 (Westinghouse Proprietary Class 2); WCAP-12418 October 1989 (Westinghouse Proprietary Class 3).

(7) System Description Document Number N3-1-4002, "Main Steam System."

(8) System Description Document Number N3-3A-4002, "Main Feedwater, Feedwater Control, and Injection Water."

(9) System Description Document Number N3-68-4001, "Reactor Coolant System."

(10) System Description Document Number N3-85-4003, "Control Rod Drive System."

(11) System Description Document Number N3-92-4003, "Neutron Monitoring System."

(12) System Description Document Number N3-94-4003, "Incore Instrumentation System."

(13) Design Criteria Number WB-DC-40-57, "Anticipated Transients without Scram Mitigation System Actuation Circuitry (AMSAC)."

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 ΔT above setpoint	Blocks automatic and manual control rod withdrawal
		Actuates turbine runback via load reference
		Defeats remote load dispatching
C-4	2/4 Overpower ΔT above setpoint	Blocks automatic and manual control rod withdrawal
		Actuates turbine runback via load reference
		Defeats remote load dispatching
C-5	1/1 Turbine impulse chamber pressure below setpoint	Blocks automatic control rod withdrawal Defeats remote load dispatching
C-7	1/1 Time derivation (absolute value) of turbine impulse chamber pressure (decrease only) above setpoint	Makes steam dump valves available for either tripping or modulation
C-9	Any condenser pressure above setpoint, or All circulation water pump breakers open	Blocks steam dump to condenser
C-11	1/1 Control Bank D rod position above setpoint	Blocks automatic rod withdrawal

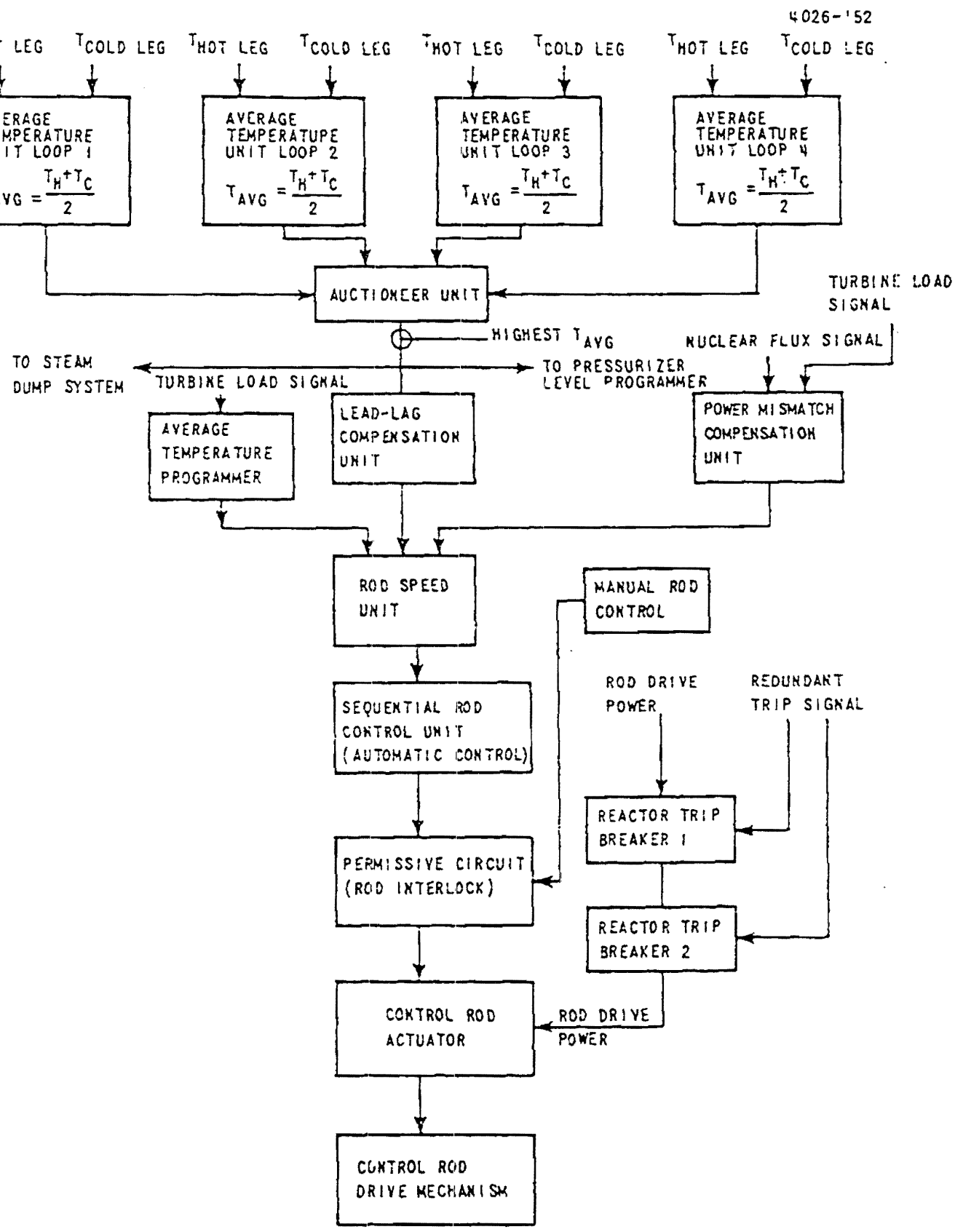
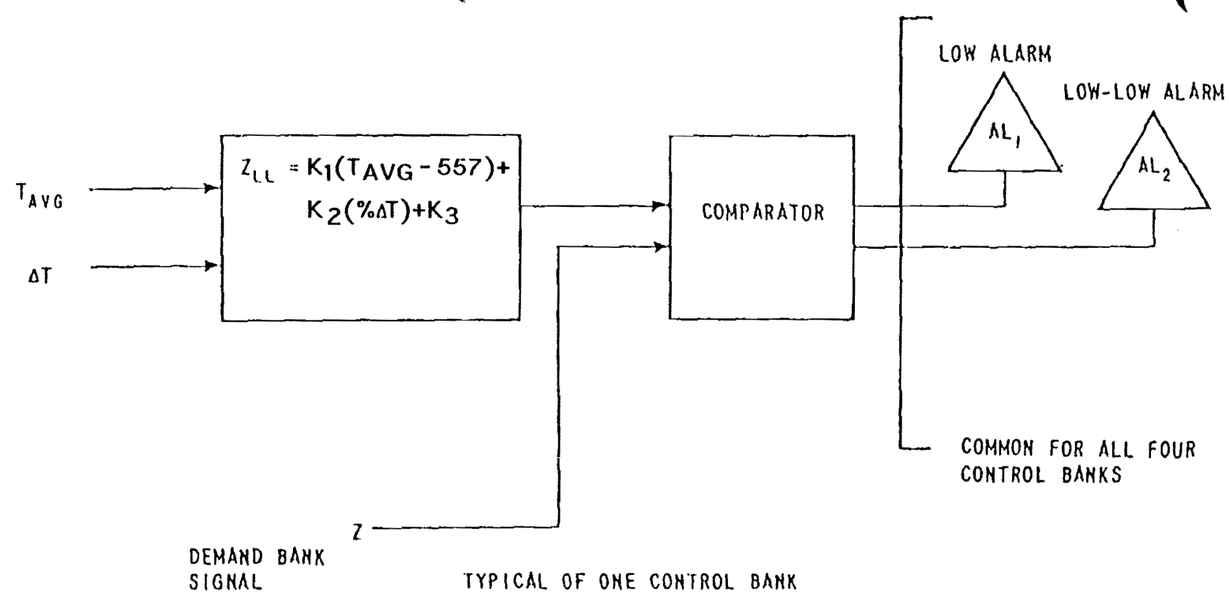


Figure 7.7-1 Simplified Block Diagram of Reactor Control System

SCANNED DOCUMENT
THIS IS A SCANNED DOCUMENT MAINTAINED ON THE LBNP OPTISRAPHICS SCANNER DATABASE



NOTE: 1 ANALOG CIRCUITRY IS USED FOR THE COMPARATOR NETWORK
2 COMPARISON IS DONE FOR ALL CONTROL BANKS

4026-150

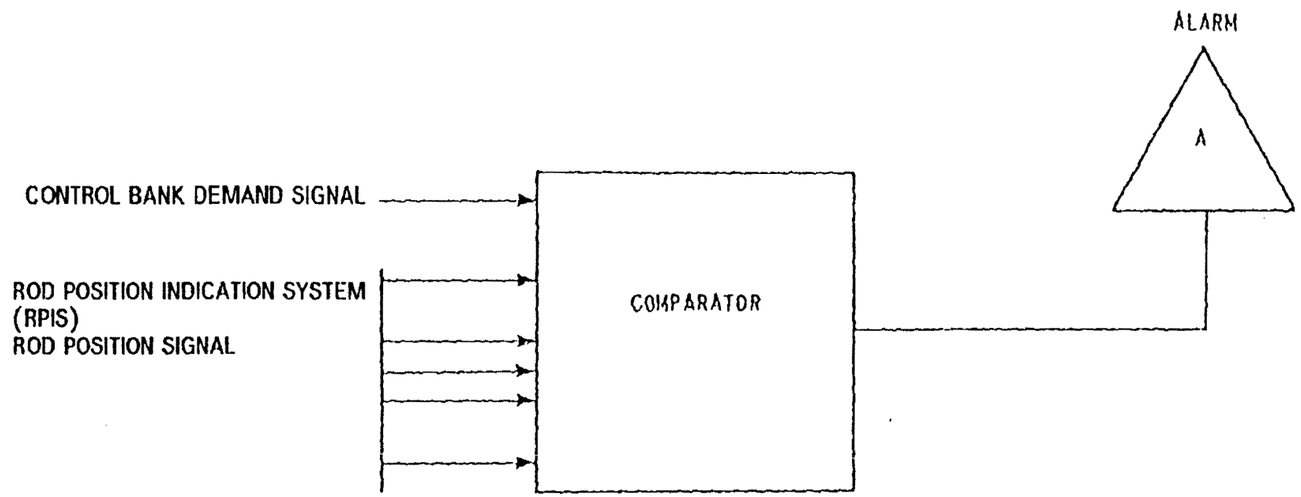
AMENDMENT 81

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

CONTROL BLANK ROD
INSERTION MONITOR
FIGURE 7.7-2

Figure 7.7-2 Control Bank Rod Insertion Monitor

SCANNED DOCUMENT
THIS IS A SCANNED DOCUMENT MAINTAINED ON THE LEAP OPTICAL-DISK SCANNER DATABASE



NOTE
1. DIGITAL OR ANALOG SIGNALS MAY BE USED FOR THE COMPARATOR COMPUTER INPUTS
2. THE COMPARATOR WILL ACTUATE THE DEVIATION ALARM IF; 1) THE DEVIATION BETWEEN THE ACTUAL ROD POSITION AND THE CONTROL BANK DEMAND POSITION EXCEEDS A PRESET VALUE, OR, 2) THE DEVIATION BETWEEN ANY TWO RODS WITHIN A CONTROL BANK EXCEEDS A PRESET VALUE.
3. COMPARISON IS INDIVIDUALLY DONE FOR ALL CONTROL BANKS

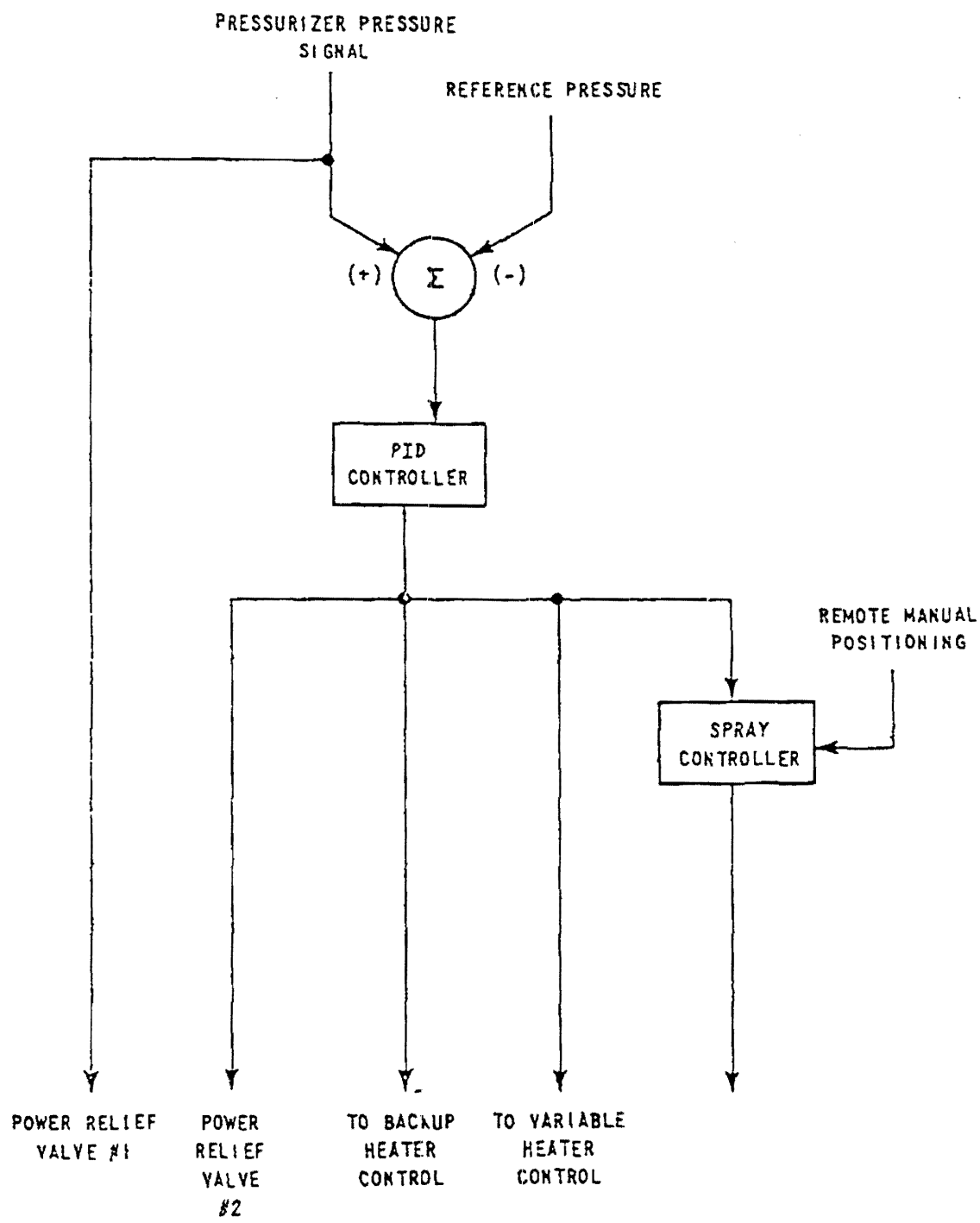
4026-149

AMENDMENT 81

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

ROD DEVIATION COMPARATOR
FIGURE 7.7-3

Figure 7.7-3 Rod Deviation Comparator



AMENDMENT 81

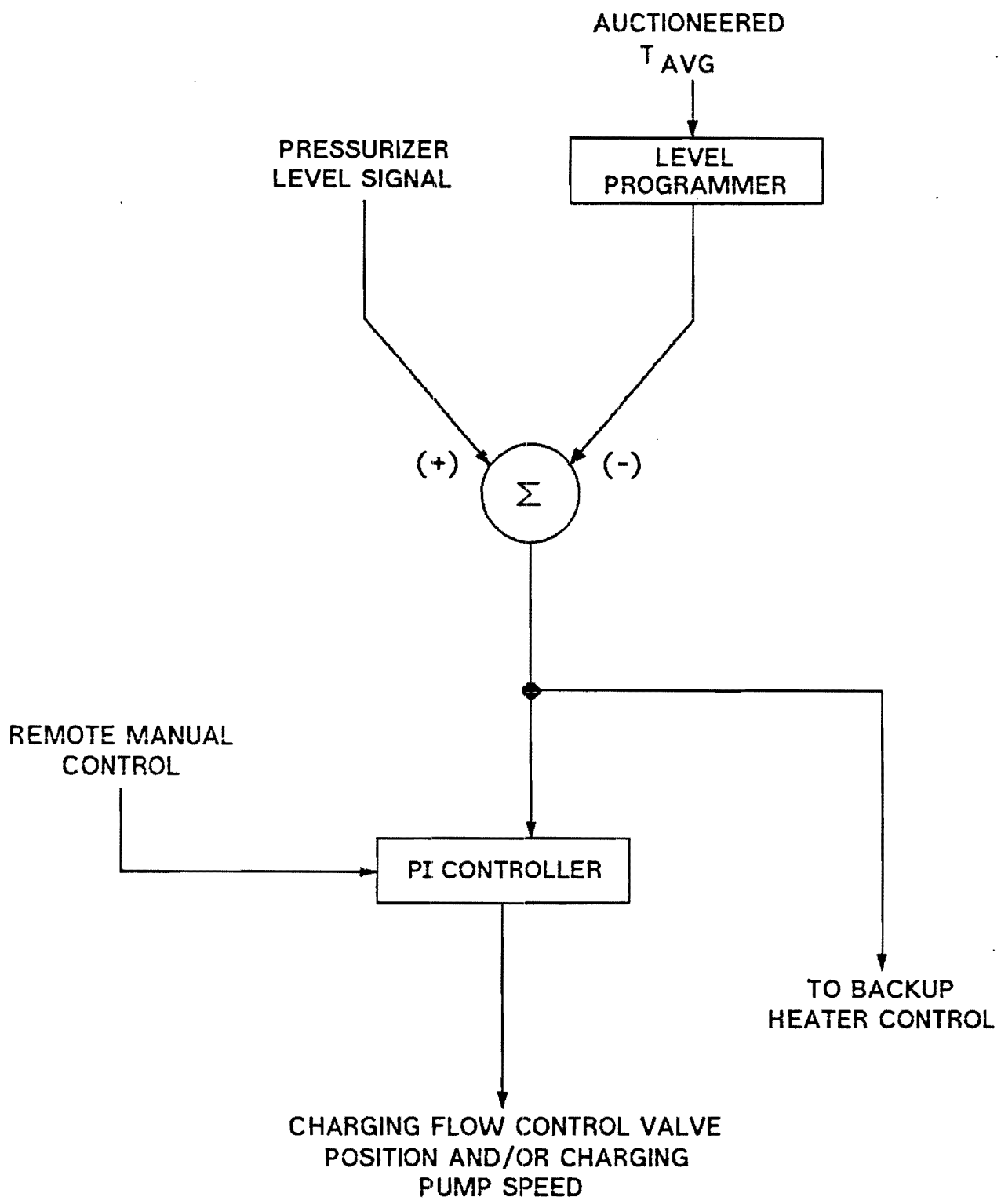
WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

BLOCK DIAGRAM OF PRESSURIZER PRESSURE CONTROL SYSTEM

FIGURE 7.7-4

SCANNED DOCUMENT
THIS IS A SCANNED DOCUMENT MAINTAINED ON THE WBNP OPTIGRAPHICS SCANNER DATABASE

Figure 7.7-4 Block Diagram of Pressurizer Pressure Control System



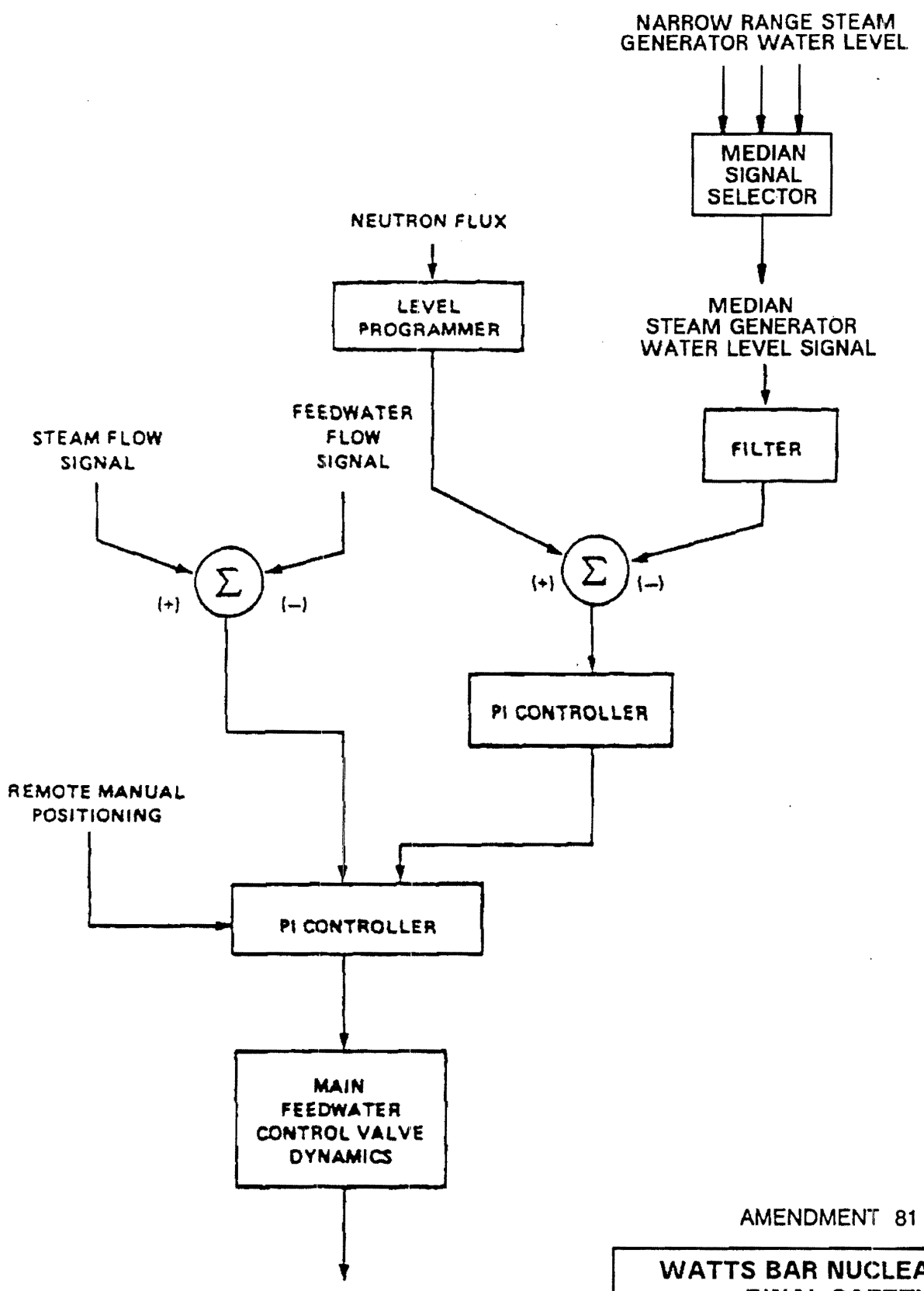
AMENDMENT 81

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

BLOCK DIAGRAM OF PRESSURIZER
LEVEL CONTROL SYSTEM
FIGURE 7.7-5

SCANNED DOCUMENT
THIS IS A SCANNED DOCUMENT MAINTAINED ON
THE WBNP OPTIGRAPHICS SCANNER DATABASE

Figure 7.7-5 Block Diagram of Pressurizer Level Control System



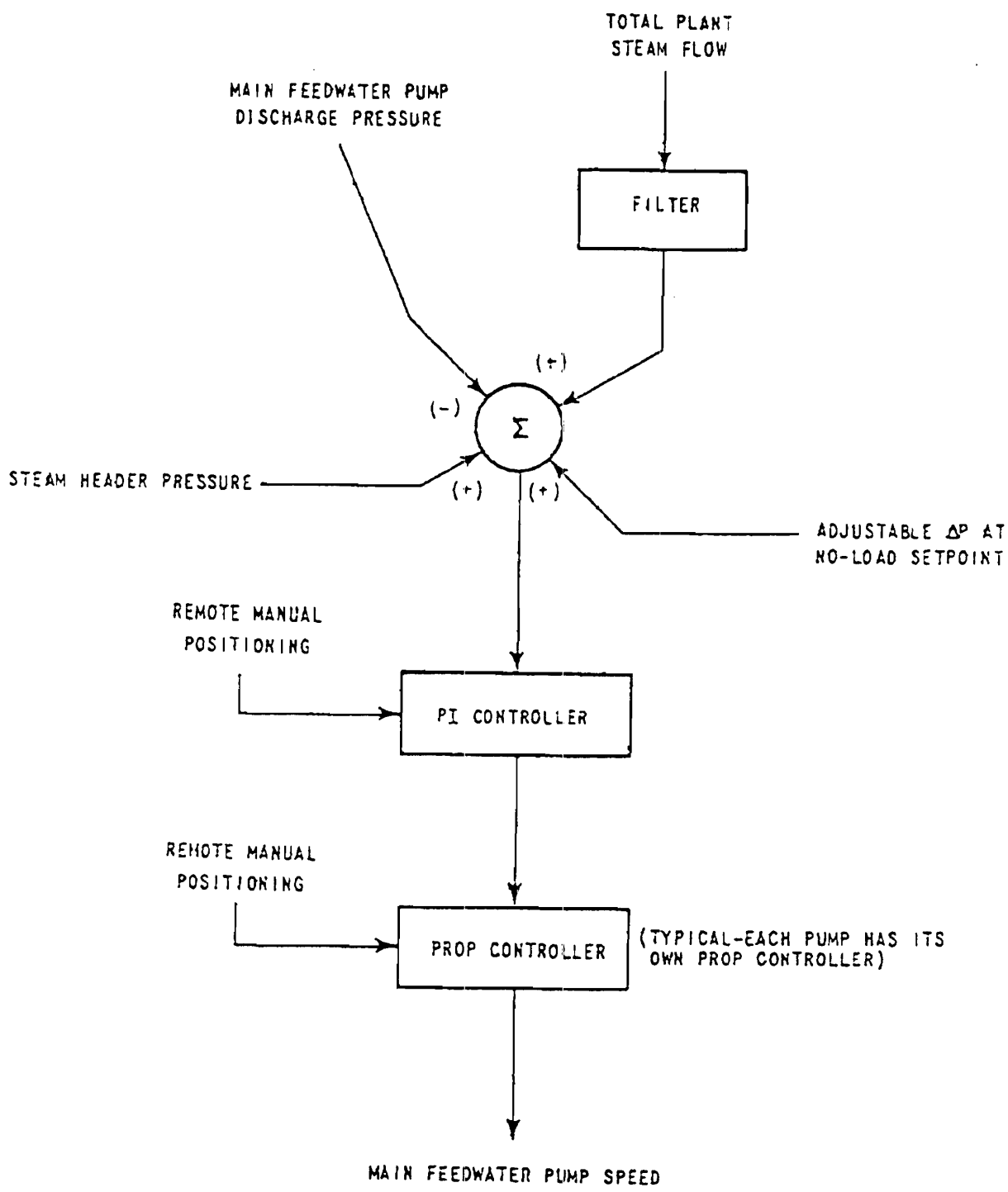
AMENDMENT 81

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

BLOCK DIAGRAM OF
STEAM GENERATOR
WATER LEVEL CONTROL SYSTEM
FIGURE 7.7-6

SCANNED DOCUMENT
THIS IS A SCANNED DOCUMENT MAINTAINED ON THE WBNP OPTIGRAPHICS SCANNER DATABASE

Figure 7.7-6 Block Diagram of Steam Generator Water Level Control System



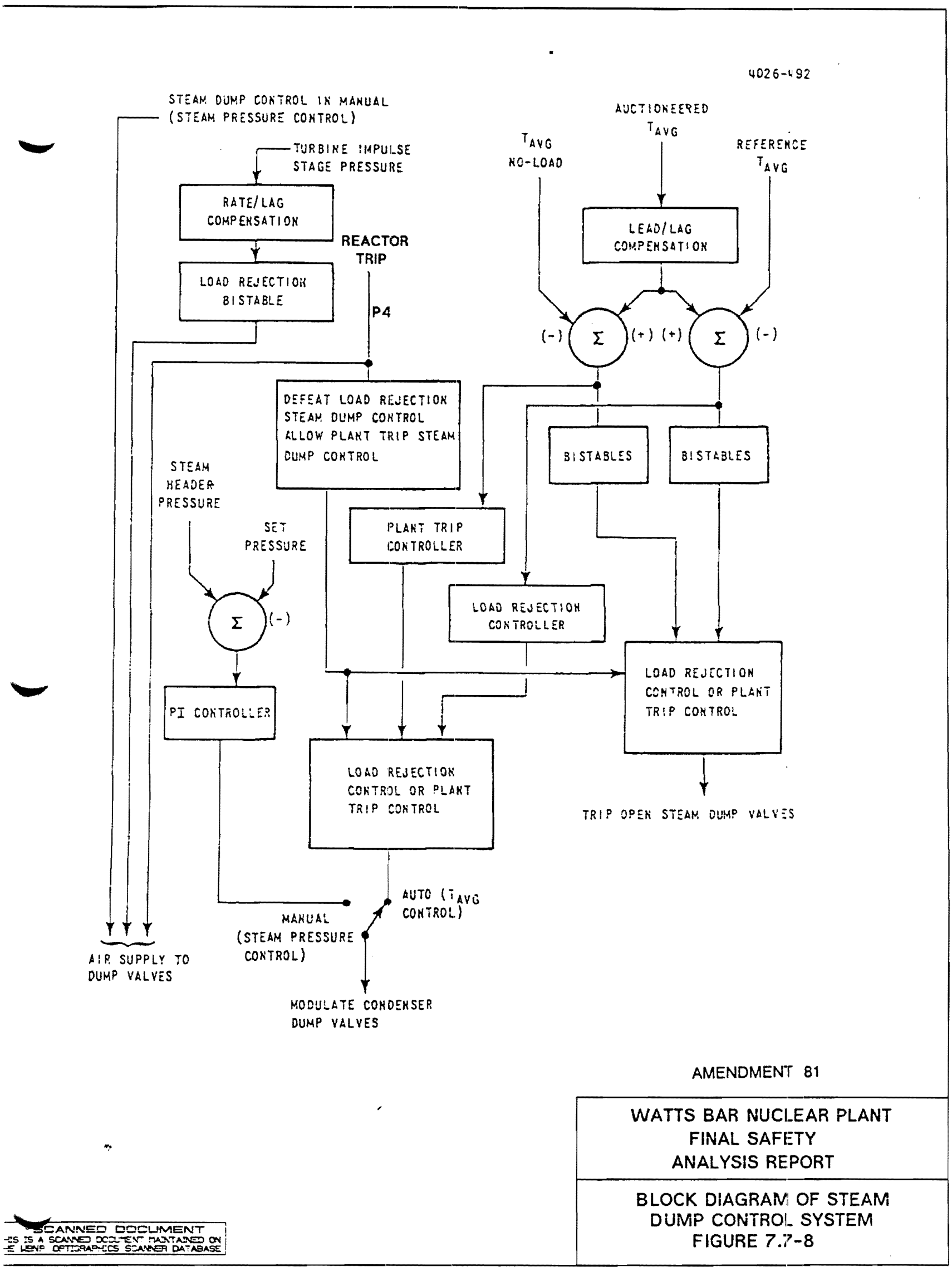
AMENDMENT 81

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

BLOCK DIAGRAM OF MAIN FEEDWATER PUMP SPEED CONTROL SYSTEM
FIGURE 7.7-7

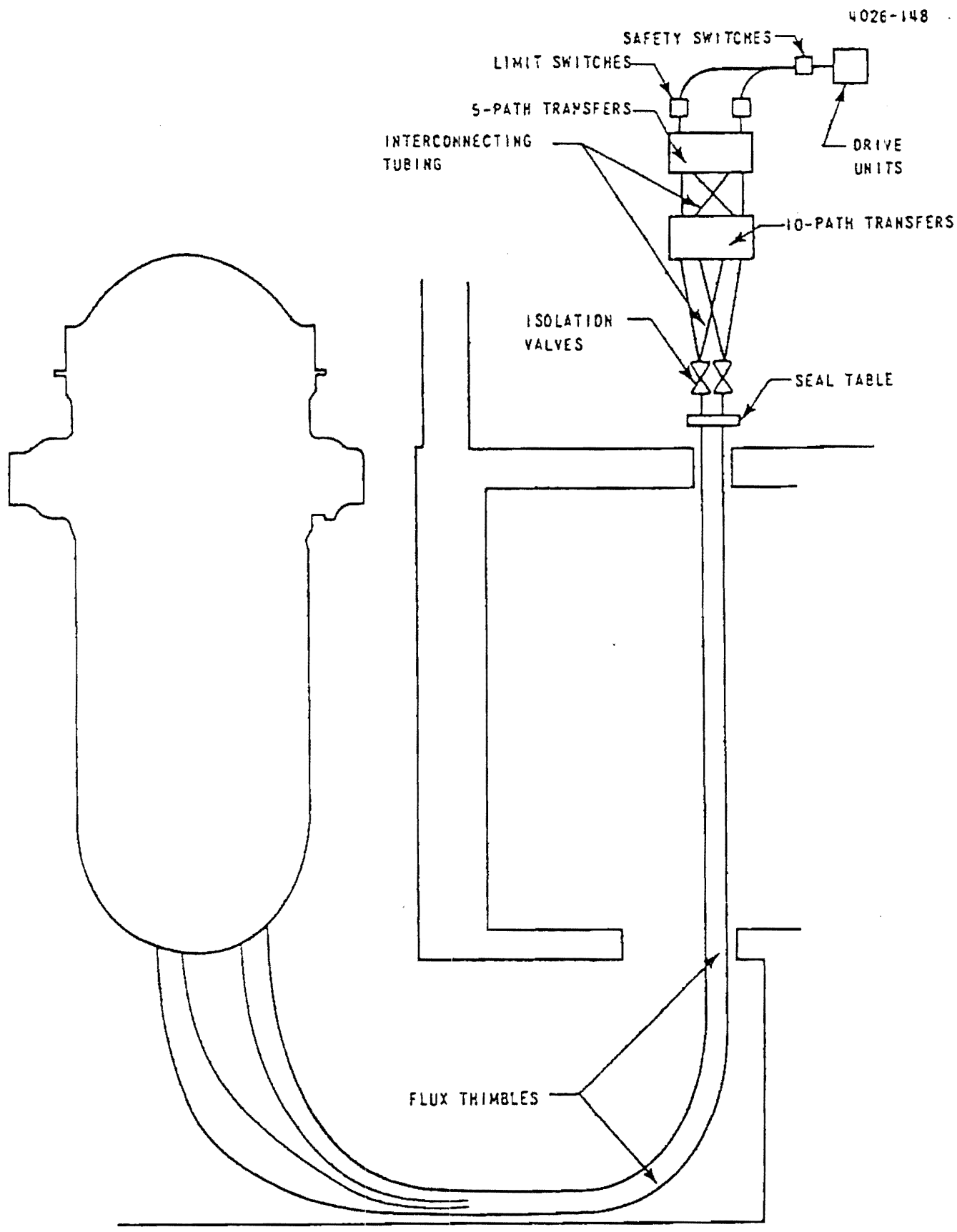
SCANNED DOCUMENT
THIS IS A SCANNED DOCUMENT MAINTAINED ON THE WBNP OPTIGRAPHICS SCANNER DATABASE

Figure 7.7-7 Block Diagram of Main Feedwater Pump Speed Control System



SCANNED DOCUMENT
THIS IS A SCANNED DOCUMENT MAINTAINED ON
THE WBNP OPTIGRAPHICS SCANNER DATABASE

Figure 7.7-8 Block Diagram of Steam Dump Control System



AMENDMENT 81

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

BASIC FLUX-MAPPING SYSTEM
FIGURE 7.7-9

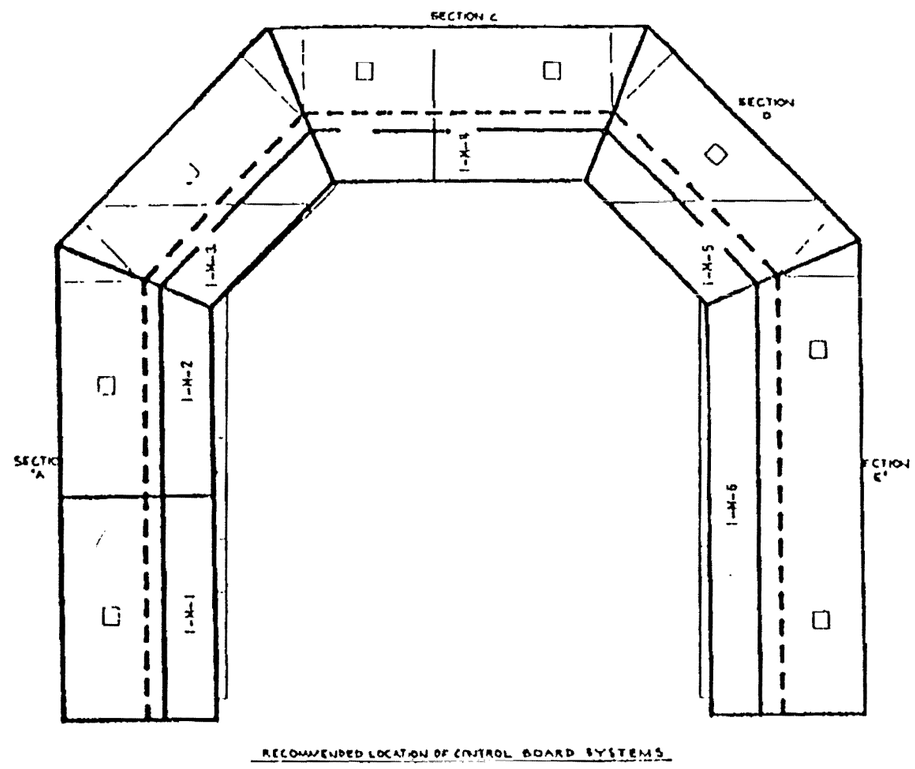
SCANNED DOCUMENT
THIS IS A SCANNED DOCUMENT MAINTAINED ON
THE WBNP OPTIGRAPHICS SCANNER DATABASE

Figure 7.7-9 Basic Flux-Mapping System

SCANNED DOCUMENT
THIS IS A SCANNED DOCUMENT MAINTAINED ON
THE LBNP OPTICAL DISK SCANNER DATABASE

CONTROL PANEL NOMENCLATURE

UNIT 1 PANEL NO.	UNIT 2 PANEL NO.	
1-M-1	2-M-1	GENERATOR & AUXILIARY POWER
1-M-2	2-M-2	TURBINE CONTROL
1-M-3	2-M-3	FEEDWATER, STEAM & CONDENSATE
1-M-4	2-M-4	REACTOR CONTROL
1-M-5	2-M-5	REACTOR COOLANT SYATEM & AUXILIARY STEAM
1-M-6	2-M-6	ENGINEERED SAFEGUARDS SYSTEMS & AUX. SYSTEMS



NOTES

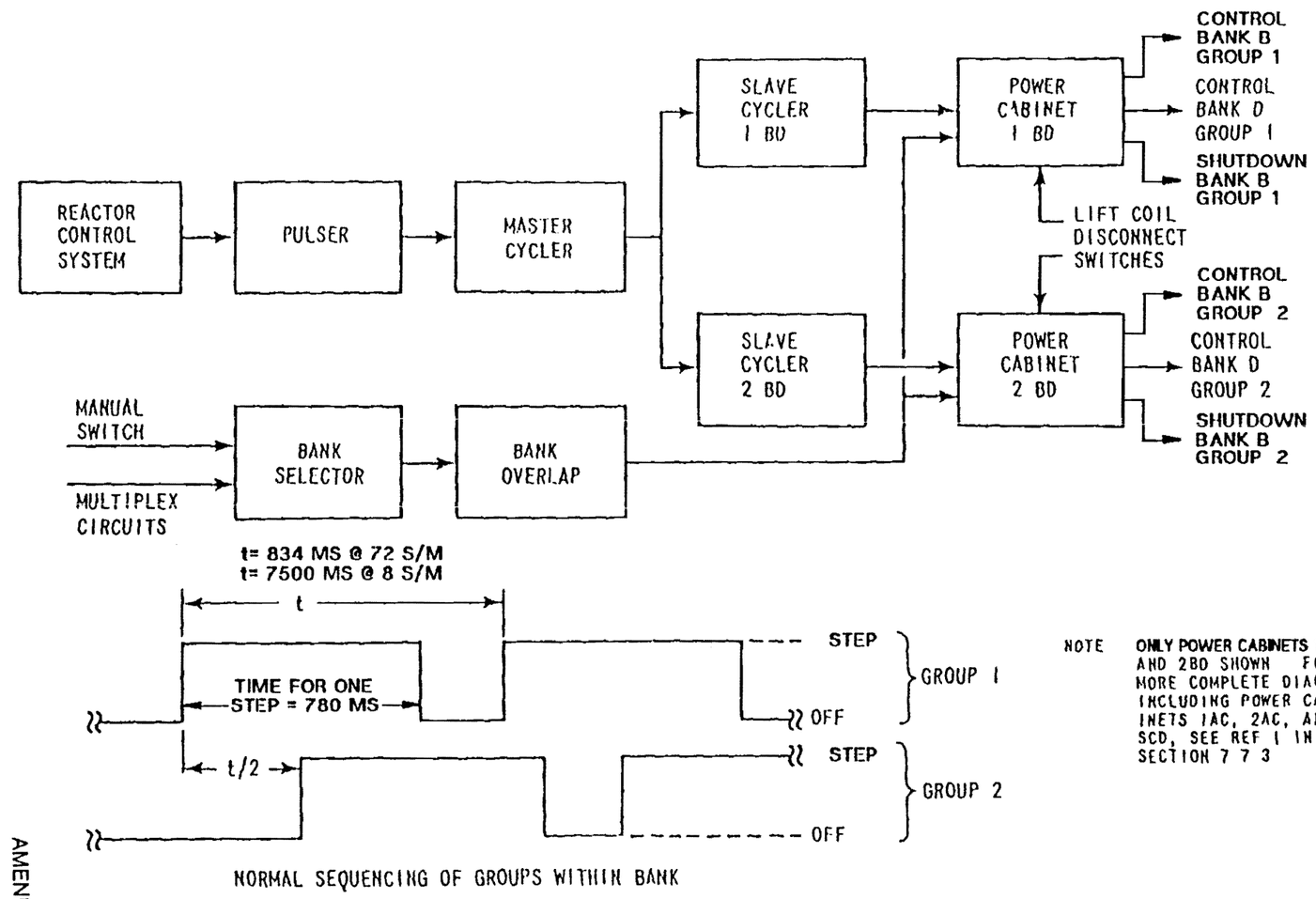
1. SYSTEMS ARE RELATED TO EACH OTHER TO OPTIMIZE OVERALL PLANT OPERATION WITH SECTION "C" ACTING AS MAIN FOCAL POINT.
2. THIS DRAWING CAN BE USED WITH THE STANDARD INTERCONNECTION WIRING DIAGRAMS TO FACILITATE CABLE TRAY LAYOUT.

AMENDMENT 81

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

TYPICAL LOCATION OF
CONTROL BOARD SYSTEMS
FIGURE 7.7-10

Figure 7.7-10 Typical Location of Control Board Systems



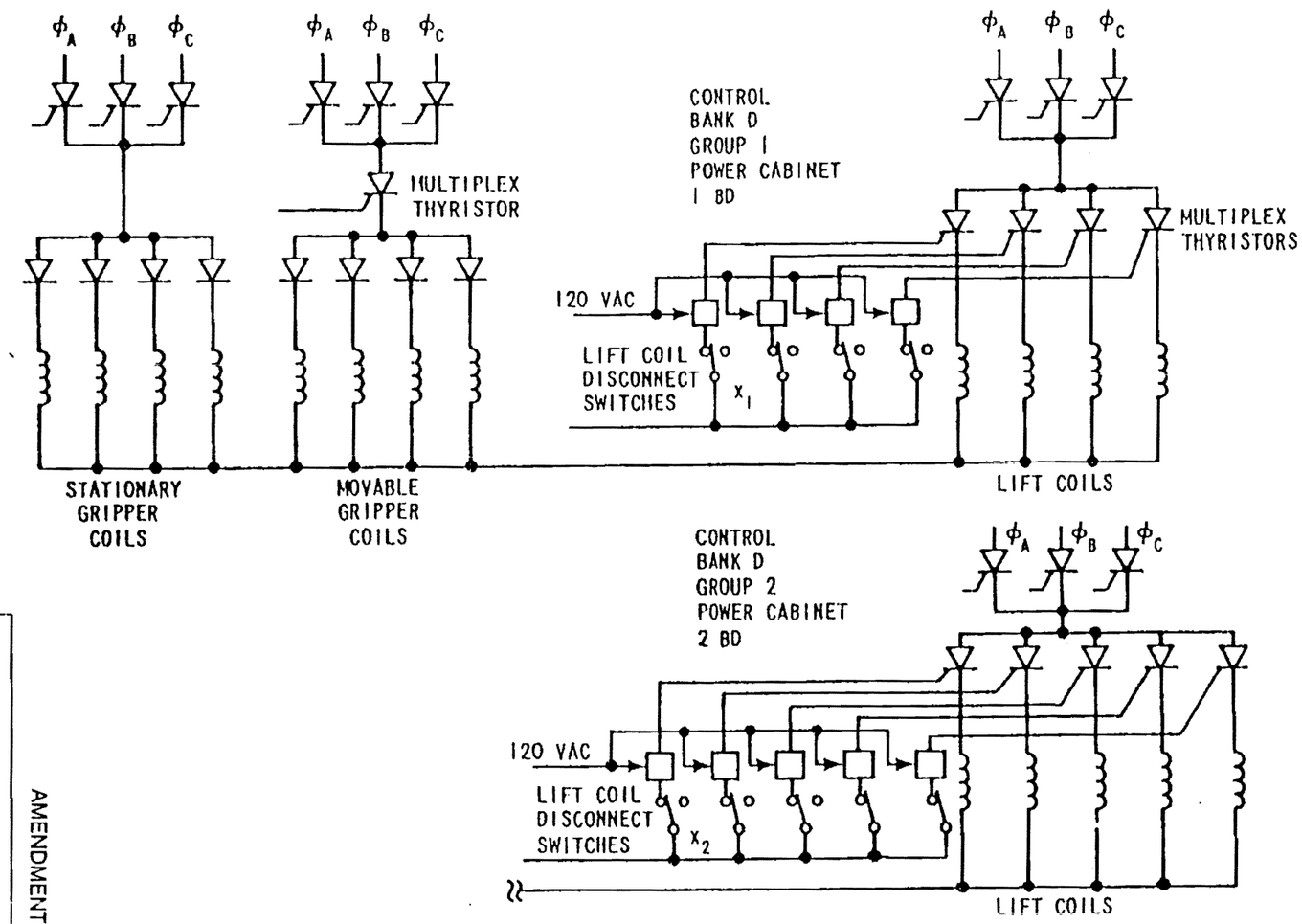
SCANNED DOCUMENT
IS A SCANNED DOCUMENT MAINTAINED ON LEGIBLE OPTISCAN-EOS SCANNER DATABASE

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

AMENDMENT 81

SIMPLIFIED BLOCK DIAGRAM
ROD CONTROL SYSTEM
FIGURE 7.7-11

Figure 7.7-11 Simplified Block Diagram Rod Control System



SCANNED DOCUMENT
THIS IS A SCANNED DOCUMENT MAINTAINED ON
THE WBNP OPTICAPHCOS SCANNER DATABASE.

AMENDMENT 81

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

CONTROL BANK D
PARTIAL SIMPLIFIED SCHEMATIC DIAGRAM
POWER CABINETS 1BD & 2BD
FIGURE 7.7-12

Figure 7.7-12 Control Bank D Partial Simplified Schematic Diagram Power Cabinets 1BD and 2BD

7A INSTRUMENTATION IDENTIFICATIONS AND SYMBOLS

A standard set of instrumentation symbols and identifications is provided in this appendix to aid in the interpretation of the control and logic diagrams in figures reproduced from TVA drawings in this FSAR. A figure made from a TVA drawing can be identified by the words "TVA DWG" followed by a series of numbers in the title block of the figure.

The identification and symbols include the following designation:

(1) Instrument identification letters.

(2) Process system numbers.

(3) Flow and control diagram symbols.

(4) Basic instrumentation and radiation symbols.

(5) Basic digital logic symbols.

7A.1 IDENTIFICATION SYSTEM

Each instrument is identified by a series of letters and numbers to designate the function, the process system, and the control loop.

7A.1.1 FUNCTIONAL IDENTIFICATION

The functional identification of an instrument consists of letters from Figure 7A-I and generally includes one uppercase first letter covering the measured or initiating variable, and one or more uppercase succeeding letters covering the function of the individual instruments. The exceptions to this rule are as follows:

(1) The use of chemical symbols (e.g. pH, Cu, Na) as a first letter entity to better identify some of the measured variables.

(2) The use of An and Px in the succeeding letters to identify analyzer and power supply, respectively.

7A.1.1.1 Principal Function

The functional identification of an instrument is made according to the principal function and not according to the construction. Thus, a differential pressure transmitter used for flow measurement is identified as an FT, not a PdT. A pressure indicator and a pressure switch connected to the output of a pneumatic level transmitter is identified as LI and LS, respectively. (Note: An instrument identified may also have secondary purposes, e.g., a signal originating from a pressure transmitter that is proportional to pressure may also be used as an inferred measurement of temperature.)

7A.1.1.2 Measured Variable

In an instrument loop the first letter of the functional identification indicates the measured (initiating), not the inferred variable and the manipulated variable. Thus a control valve varying flow according to the dictates of a level controller is an LCV, not an FCV. Also, if two or more measured variable signals are combined to control a particular variable the instrument processing the combined signals is identified in accordance with the controlled variable (e.g., cascade control).

7A.1.1.3 Readout or Passive Functions

The one or more succeeding letters of the functional identification designates one or more readout or passive functions, or output functions, or both. The readout or passive functional letters, such as R for recording and I for indicating, follow the first letter in sequence. The output functional letters, such as C for control and S for switch, follow these in sequence except that output letter C (control) shall precede output letter V (valve) and 0 (operator), e.g., HCV, a hand-actuated control valve. However, if these are not readout or passive functional letters, then the output functional letters follow the first letter in sequence.

7A.1.1.4 Modifying Letters

Modifying letters may modify either a first letter or the succeeding letters, as applicable. However, modifying letters, if used, are interposed so that they are placed immediately following the letter they modify except S for solenoid precedes output letter V (valve)., e.g., FSV designates a solenoid-actuated flow valve.

7A.1.1.5 Tagging Symbols

An instrument tagging designation on a control diagram may be drawn with as many circular tagging symbols as there are measured variables or outputs. Thus, a recorder charting temperature and flow may be identified by two tangent circles where possible, one inscribed TR-3-31 and the other FR-3-31. The instrument then would be designated T/FR-3-31.

7A.1.1.6 Special Identifying Letters

The measured variable letter X (special) has been included in Figure 7A-l to cover unlisted variables that are used to a limited extent. It may also be used for an instrument function. Therefore, the letter may have any number of meanings as a first letter and any number of meanings as a succeeding letter.

Any first letter, if used in combination with the modifying letter, e.g., d (differential), represents, as shown on Figure 7A-1 for pressure differential, a new and separate measured variable, and the combination shall be treated as a first-letter entity. Thus, instruments PdI and PI measure two different variables, namely, differential pressure and pressure.

7A.1.1.7 Pilot Lights

A pilot light that serves only as position indication, power available, or alarm is not always identified. A pilot light that is part of an instrument loop, if numbered, is

identified by a first letter Z or X (zone, position, or special) followed by a succeeding letter I or A (I - indicating.; A - alarm).

7A.1.2 SYSTEM IDENTIFICATION

The system identification of an instrument uses a number assigned to the process system of which the instrument is a part. Each process system, e.g. feedwater, extraction steam, reactor coolant system, has been assigned a system identification number.

7A.1.2.1 Identification Numbers

The system identification numbers are listed in Figure 7A-2. The system identification number follows the "succeeding letters" or the functional identification letters and is separated from them by a hyphen.

7A.1.2.1.1 Instruments Common to Multiple Process Systems

If an instrument is common to two or more process systems, it is assigned to the one for which it is performing its principal function.

7A.1.3 LOOP IDENTIFICATION

The control loop identification of an instrument generally uses a number assigned to the control loop of which the instrument is a part. There may be one or many instrument control loops in a process system. However, each control loop has a unique number.

7A.1.3.1 Instruments Common to Multiple Control Loops

If an instrument is common to two or more control loops, it is assigned to the loop for which it is performing its principal function.

7A.1.3.2 Multiple Instruments with a Common Function

If a given loop has more than one instrument with the same functional identification, a suffix letter or number is appended to the loop number, e.g., FCV-3-10A, FCV-3-1OB.

7A.2 SYMBOLS

The symbols used to depict the instrumentation on flow, control, and logic diagrams and other drawings are illustrated in the following figures:

Figure 7A-3 - Flow and Control Diagram Symbols

Figure 7A-4 - Basic Instrumentation and Radiation Symbols

Figure 7A-5 - Application of Basic Instrumentation Symbols

Figure 7A-6 - Digital Logic Symbols

The flow diagram symbols for valves, valve operators, and miscellaneous devices most frequently used by TVA are shown in Figure 7A-3.

7A.2.1 INSTRUMENT SYMBOL

The circular symbol shown in Figure 7A-4 is the basic instrumentation symbol. It is used to depict the instrument proper and most other instrumentation items. Also, it is used as a "flag" to enclose identifications and point out items such as valves, which have their own pictorial symbols. Typical applications of the instrumentation symbols are shown in Figure 7A-5.

REFERENCES

None.

INSTRUMENT IDENTIFICATION COMBINATION OF LETTERS FOR BFN, SQN & WBN

MEASURED VARIABLE \ INSTRUMENT FUNCTION	SYMBOL	CONTROLLING: RECORDING	CONTROLLING: INDICATING	CONTROLLING: NONINDICATING	CONTROLLING: CONTROL VALVE	CONTROLLING: SOLENOID VALVE	CONTROLLING: CONTROL OPERATOR	CONTROLLING: VALVE	MEASURING: RECORDING	MEASURING: INDICATING	MEASURING: SIGHT GLASS	MEASURING: PRIMARY ELEMENT	MEASURING: TRANSMITTER	MEASURING: TOTALIZER	MEASURING: MODIFIER	MEASURING: WELL	MEASURING:	MEASURING:	SWITCH: INDICATING	SWITCH: NONINDICATING	SWITCH:	ALARM: ALARM	ALARM:	ALARM:	SPECIALS: DATA LOGGER	SPECIALS: POWER SUPPLY	SPECIALS: INDICATING LIGHT
	SYMBOL	RC	IC	C	CV	SV	CO		R	I	G	E	T	O	H	W			IS	S		A			DL	PS	IL
ANALYZER	AN								AnR	AnI		AnE	AnT		AnH				AnIS	AnS		AnA					
CARBON DIOXIDE	CO_2								CO_2R	CO_2I		CO_2E	CO_2T		CO_2H				CO_2IS	CO_2S		CO_2A					
CONDUCTIVITY	C								CR	CI		CE	CT		CH				CIS	CS		CA					
ELECTRICAL	E	ERC	EIC	EC					ER	EI		EE	ET	EO	EH				EIS	ES		EA					
FLOW	F	FRC	FIC	FC	FCV	FSV	FCO		FR	FI	FG	FE	FT	FO	FH				FIS	FS		FA					
HAND (MANUAL)	H			HC	HCV		HCO	HV												HS							
INTERVAL (TIME)	I			IC					IR	II			IT	IO	IH				IIS	IS		IA					
LEVEL	L	LRC	LIC	LC	LCV	LSV	LCO		LR	LI	LG	LE	LT		LH				LIS	LS		LA					
MOISTURE	M			MC					MR	MI		ME	MT		MH				MIS	MS		MA					
PRESSURE	P	PRC	PIC	PC	PCV	PSV	PCO		PR	PI			PT		PH				PIS	PS		PA					
PRESSURE DIFF	Pd	PdRC	PdIC	PdC	PdCV	PdSV	PdCO		PdR	PdI			PdT		PdH				PdIS	PdS		PdA					
RADIATION	R								RR	RI		RE	RT		RH				RIS	RS		RA					
SPEED	S	SRC	SIC	SC	SCV		SCO		SR	SI		SE	ST		SH				SIS	SS		SA					
SPECIAL	X	XRC	XIC	XC	XCV		XCO	XV	XR	XI		XE	XT		XH	XW			XIS	XS		XA					
TEMPERATURE	T	TRC	TIC	TC	TCV		TCO		TR	TI		TE	TT		TH	TW			TIS	TS		TA					
VIBRATION	V								VR	VI		VE	VT		VH				VIS	VS		VA					
WEIGHT	W								WR	WI		WE	WT		WH				WIS	WS		WA					
ZONE (POSITION)	Z									ZI			ZT		ZH				ZIS	ZS		ZA					
SAMPLE	Sa											SaE															
HYDROGEN	H_2								H_2R	H_2I		H_2E	H_2T		H_2H				H_2IS	H_2S		H_2A					
OXYGEN	O_2								O_2R	O_2I		O_2E	O_2T		O_2H				O_2IS	O_2S		O_2A					
IND LIGHT																											IL
ROOT VALVE								RTV																			

THIS TABLE IS TYPICAL. REFER TO GENERAL DRAWING G-M-A-3D0617-1A LATEST REVISION

AMENDMENT 81

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

INSTRUMENTATION SYMBOLS
AND TABULATION
FROM TVA DS E18.3.3
FIGURE 7A-1

SCANNED DOCUMENT
TVA 38 (12-1-88)
TVA 38 (12-1-88) SCANNED DOCUMENT

Figure 7A-1 Instrumentation Symbols and Tabulation from TVA DS E18.3.3

CODE	SYSTEM	CODE	SYSTEM	CODE	SYSTEM
0	INDEX, NP STYLES, MIMICS, MISC EQUIP., & LOCAL PANELS	34		67	ESSENTIAL RAW COOLING WATER SYSTEM
1	MAIN STEAM SYSTEM	35	GENERATOR COOLING SYSTEMS	68	REACTOR COOLANT SYSTEM
2	CONDENSATE SYSTEM	36	PW SECONDARY TREATMENT SYSTEM	69	
3	MAIN AND AUXILIARY FEEDWATER SYSTEM	37	GLAND SEAL WATER SYSTEM	70	COMPONENT COOLING SYSTEM
4		38	INSULATING OIL SYSTEM	71	
5	EXTRACTION STEAM SYSTEMS	39	CO_2 STORAGE, FIRE PROTECTION & PURGING SYSTEM	72	CONTAINMENT SPRAY SYSTEM
6	HEATER DRAINS & VENTS SYSTEM	40	STATION DRAINAGE SYSTEM	73	
7	TURBINE EXTRACTION TRAPS & DRAINS SYSTEM	41	LAYUP WATER TREATMENT SYSTEM	74	RESIDUAL HEAT REMOVAL SYSTEM
8	MISCELLANEOUS TURBINE CONNECTIONS	42	CHEMICAL CLEANING SYSTEM	75	
9	MISCELLANEOUS TURBINE VENTS SYSTEM	43	SAMPLING & WATER QUALITY SYSTEM	76	VOLUME REDUCTION SYSTEM
10		44	BUILDING HEATING SYSTEM	77	WASTE DISPOSAL SYSTEM
11		45		78	SPENT FUEL PIT COOLING SYSTEM
12	AUXILIARY BOILER SYSTEM	46	FEEDWATER CONTROL SYSTEM	79	
13	FIRE DETECTION SYSTEM	47	TURBOGENERATOR CONTROL SYSTEM	80	PRIMARY CONTAINMENT COOLING SYSTEM
14	CONDENSATE DEMINERALIZER SYSTEM	48		81	PRIMARY MAKEUP WATER SYSTEM
15	STEAM GEN. BLOWDOWN SYSTEM	49	BREATHING AIR SYSTEM	82	STANDBY DIESEL GENERATOR SYSTEM
16		50	HYPERCHLORITE SYSTEM	83	HYDROGEN RECOMBINATION SYSTEMS
17		51		84	FLOOD MODE BORATION MAKEUP SYSTEM
18	FUEL OIL SYSTEM	52	SYSTEM TEST FACILITY (INSTRUMENTATION)	85	CONTROL ROD DRIVE SYSTEM
19		53		86	
20	CENTRAL LUBRICATING OIL SYSTEM	54	INJECTION WATER SYSTEM	87	UPPER HEAD INJECTION SYSTEM
21		55	ANNUNCIATOR & SEQUENTIAL EVENTS RECORDING SYSTEM	88	CONTAINMENT ISOLATION SYSTEM
22		56	TEMPERATURE MONITORING SYSTEM	89	
23		57	ASSOCIATED ELECTRICAL SYSTEMS	90	RADIATION MONITORING SYSTEM
24	RAW COOLING WATER SYSTEM	58	GENERATOR BUS COOLING SYSTEM	91	
25	RAW SERVICE WATER SYSTEM	59	DEMIN WATER & CASK DECON SYS	92	NEUTRON MONITORING SYSTEM
26	HIGH-PRESSURE FIRE-PROTECTION SYSTEM	60		93	
27	CONDENSER CIRCULATING WATER SYSTEM	61	ICE CONDENSER SYSTEM	94	IN-CORE FLUX DETECTORS
28	WATER-TREATMENT SYSTEM	62	CHEMICAL & VOLUME CONTROL SYSTEM	95	
29	POTABLE (TREATED) WATER DISTRIBUTION SYSTEM	63	SAFETY INJECTION SYSTEM	96	
30	VENTILATING SYSTEM	64		97	
31	AIR CONDITIONING (COOLING-HEATING) SYSTEM	65	EMERGENCY GAS TREATMENT SYSTEM	98	
32	CONTROL AIR SYSTEM	66		99	REACTOR PROTECTION SYSTEM
33	SERVICE AIR SYSTEM				

AMENDMENT 81

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

MECHANICAL SYSTEM
IDENTIFICATION NUMBERS
TVA DWG. NO. 85M430B617-2D R6
FIGURE 7A-2

SCANNED DOCUMENT
THIS IS A SCANNED DOCUMENT MAINTAINED ON THE WBNP OPTIGRAPHICS SCANNER DATABASE

Figure 7A-2 Mechanical System Identification Numbers

Figure 7A-3 Mechanical Flow and Control Diagram Symbols

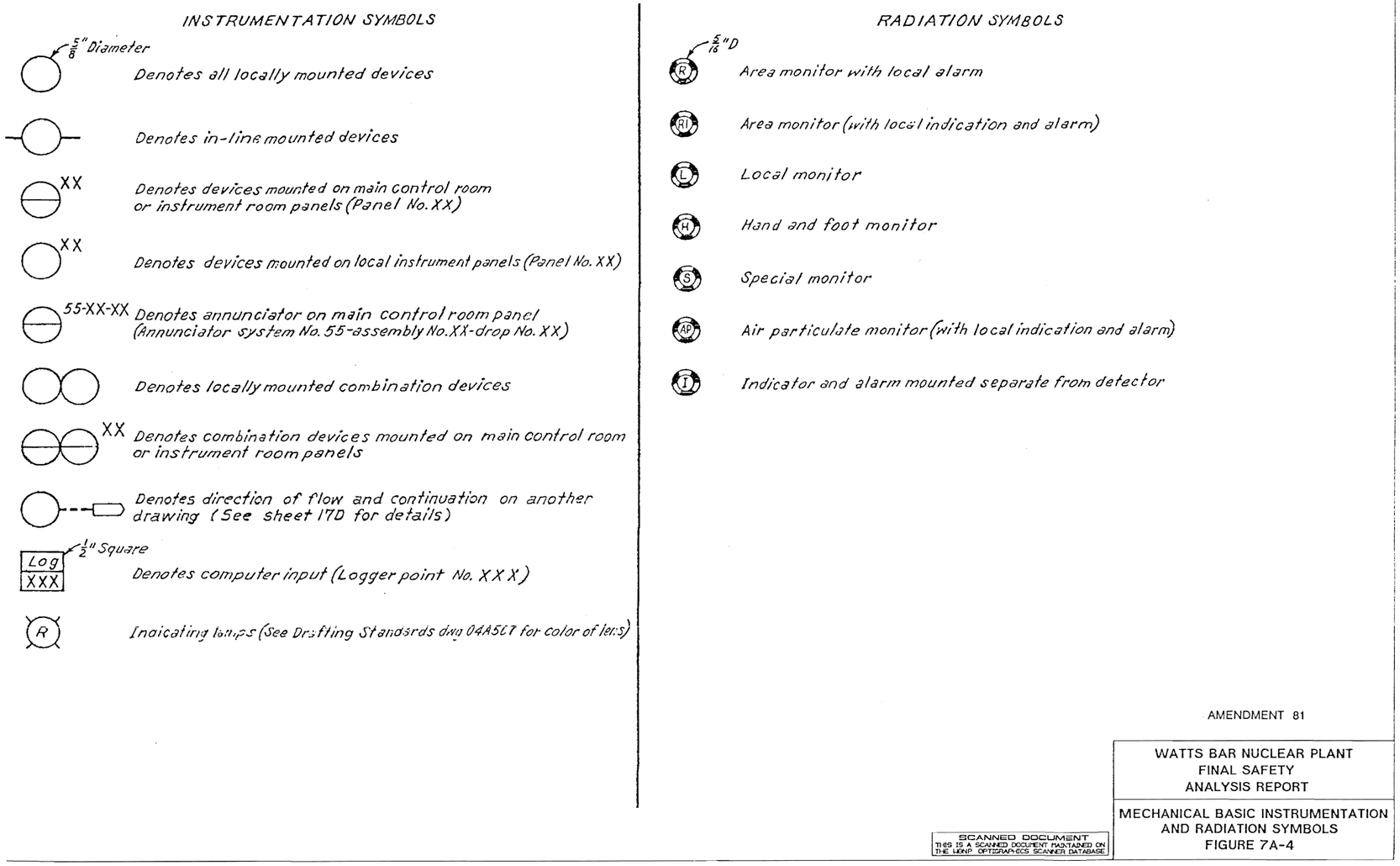


Figure 7A-4 Mechanical Basic Instrumentation and Radiation Symbols

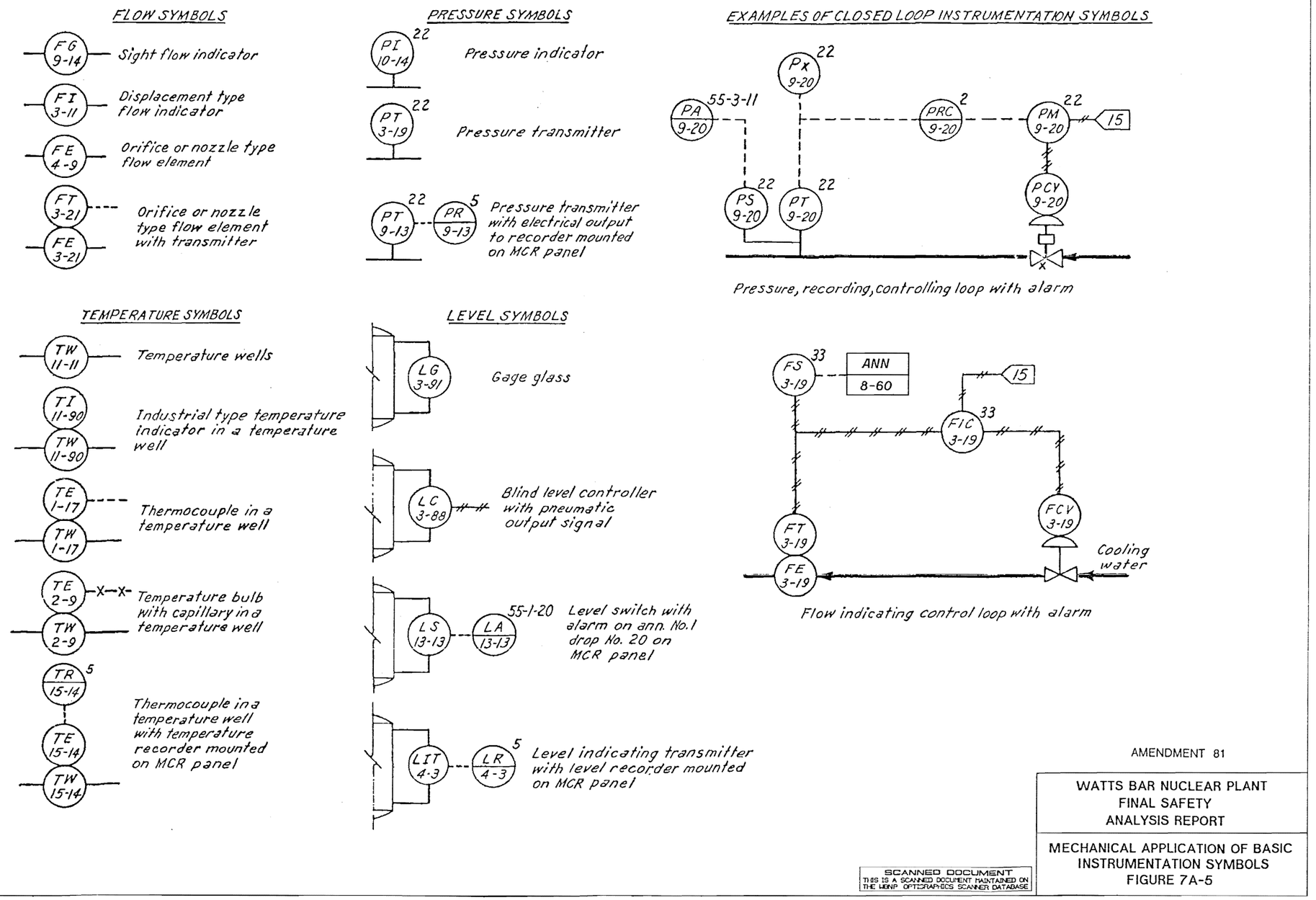


Figure 7A-5 Mechanical Application of Basic Instrumentation Symbols

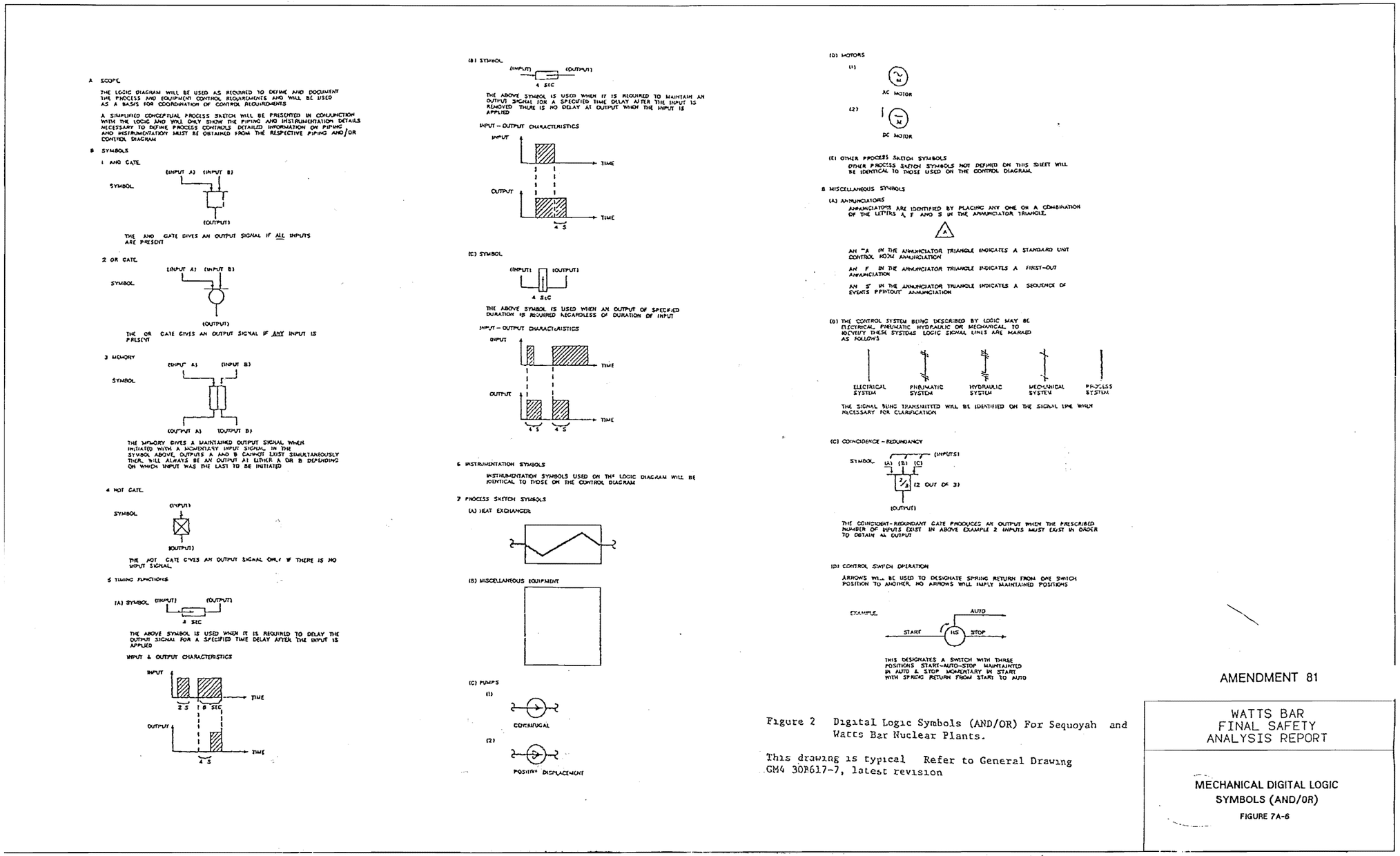


Figure 2 Digital Logic Symbols (AND/OR) For Sequoyah and Watts Bar Nuclear Plants.

This drawing is typical Refer to General Drawing GM4 30R617-7, latest revision

Figure 7A-6 Mechanical Digital Logic Symbols (and/or)