7.0 INSTRUMENTATION AND CONTROLS 1

7.1.0 INTRODUCTION 1

7.1.1 IDENTIFICATION OF SAFETY-RELATED SYSTEMS 3

7.1.1.1 Protection Systems 3

7.1.1.2 Engineered Safety Feature System (ESF System) 3

7.1.1.3 ESF Supporting Systems 4

7.1.1.4 Safe Shutdown Systems 5

7.1.1.5 Display Instrumentation for Safety-Related Systems 5

7.1.1.6 All Other Systems Required for Safety 6

7.1.1.7 Instrumentation and Control System Designers 6

7.1.1.8 Plant Comparison 6

7.1.2 IDENTIFICATION OF SAFETY CRITERIA 7

7.1.2.1 Design Bases 7

7.1.2.2 Independence of Redundant Safety-Related Systems 11

7.1.2.3 Physical Identification of Safety-Related Equipment 14

7.1.2.4 Conformance to Criteria 15

7.1.2.5 Conformance to Regulatory Guide 1.22 15

7.1.2.6 Conformance to Regulatory Guide 1.47 19

7.1.2.7 Conformance to Regulatory Guide 1.53 and IEEE Standard 379-1972 19

7.1.2.8 Conformance to Regulatory Guide 1.63 20

7.1.2.9 Conformance to IEEE Standard 317-1972 20

7.1.2.10 Conformance to IEEE Standard 336-1971 20

7.1.2.11 Conformance to Regulatory Guide 1.68 20

7.1.2.12 Conformance to Regulatory Guide 1.68.3 20

7.1.2.13 Conformance to Regulatory Guide 1.89 20

7.1.2.14 Conformance to Regulatory Guide 1.97 20

7.1.2.15 Conformance to Regulatory Guide 1.100 20

7.1.2.16 Conformance to Regulatory Guide 1.105 21

7.1.2.17 Conformance to Regulatory Guide 1.118 21

7.1.2.18 Conformance to IEEE Standard 338-1971 21

REFERENCES: SECTION 7.1 22

7.2 REACTOR TRIP SYSTEM....23
7.2.1 DESCRIPTION....23
7.2.1.1 System Description....23
7.2.1.2 Design Basis Information....36
7.2.1.3 Final Systems Drawing....38
7.2.2 ANALYSES....39
7.2.2.1 Failure Mode and Effects Analyses....39
7.2.2.2 Evaluation of Design Limits....39
7.2.2.3 Specific Control and Protection Interactions....49
7.2.2.4 Additional Postulated Accidents....52
7.2.3 TESTS AND INSPECTIONS....52
REFERENCES: SECTION 7.2....53
7.3 ENGINEERED SAFETY FEATURES SYSTEM....53
7.3.1 DESCRIPTION....54
7.3.1.1 Engineered Safety Features Actuation System Description....54
7.3.1.2 Independent ESF Actuation Systems....58
7.3.1.3 Automatically Actuated ESF Systems....58
7.3.1.4 Manually Initiated ESF Systems....68
7.3.1.5 Automatic and Manually Controlled ESF Support Systems....69
7.3.1.6 Design Basis Information....89
7.3.1.7 Final System Diagrams....93
7.3.2 ANALYSIS....93
7.3.2.1 Failure Modes and Effects Analyses (FMEA) (IEEE-352)....93
7.3.2.2 Compliance With Standards and Design Criteria....93
7.3.2.3 Further Considerations....108
7.3.2.4 Summary....109
REFERENCES: SECTION 7.3....111
7.4 SYSTEMS REQUIRED FOR SAFE SHUTDOWN....111
7.4.1 DESCRIPTION....112
7.4.1.1 Systems & Equipment Used for Modes of Shutdown....112

7.4.1.2 Instrumentation and Control Systems 114
7.4.1.3 Auxiliary Feedwater System....114
7.4.1.4 Boric Acid Transfer System (Part of CVCS) 118
7.4.1.5 Reactor Coolant Inventory - Charging Pumps 120
7.4.1.6 Reactor Coolant Inventory - Letdown Orifice Isolation Valves 121
7.4.1.7 Steam generator safety and power operated relief valves....123
7.4.1.8 Residual Heat Removal System (RHRS) 125
7.4.1.9 Primary Coolant Pressure Control (Pressurizer Heaters and Spray) 126
7.4.1.10 Supporting Systems For Safe Shutdown....128

7.4.2 ANALYSIS 130
7.4.2.1 General....130
7.4.2.2 Consideration of Selected Plant Contingencies....134

7.5 SAFETY-RELATED DISPLAY INSTRUMENTATION 136

7.5.1 DESCRIPTION 136
7.5.1.1 Plant Process Display Instrumentation (PPDI) 137
7.5.1.2 Reactor Trip System Monitoring....137
7.5.1.3 Engineered Safety Features (ESF) System Monitoring 137
7.5.1.4 ESF Support Systems....139
7.5.1.5 Auxiliary Control Panel Instrumentation 141
7.5.1.6 RCCA Position Indication System 142
7.5.1.7 Safe Shutdown System....142
7.5.1.8 Post-Accident Monitoring Instrumentation....142
7.5.1.9 Bypassed and Inoperable Status Indication (IEEE 279 Section 4.13, RG 1.47, and ICSB-BTP-21) 144
7.5.1.10 Control Panels, Annunciators, Monitoring Light Boxes, Status Light Boxes, Service Water Leak Detection 145

7.5.2 ANALYSIS 148
7.5.2.1 Plant Process Display and Post-Accident Monitoring Instrumentation....148
7.5.2.2 Reactor Trip System Monitoring....152
7.5.2.3 ESF Systems and ESF Supporting Systems....153
7.5.2.4 Auxiliary Control Panel Instrumentation 153
7.5.2.5 Safe Shutdown Monitoring System 153

7.5.2.6 Bypassed and Inoperable Status Indication (IEEE 279, Section 4.13 and RG 1.47)....153
7.5.2.7 Control Panel (Main Control Board)....153

REFERENCES: SECTION 7.5....153

7.6 ALL OTHER INSTRUMENTATION SYSTEMS REQUIRED FOR SAFETY....154

7.6.1 DESCRIPTION....154
7.6.1.1 Interlock Residual Heat Removal System Isolation Valves....154
7.6.1.2 Accumulator Isolation Valves Interlock....154
7.6.1.3 Refueling Interlocks....155
7.6.1.4 Cold Water Slug Injection....156
7.6.1.5 Spent Fuel Pool Cooling and Cleanup System....156
7.6.1.6 ECCS Leak Detection....156
7.6.1.7 Fire Protection and Detection Systems....156
7.6.1.8 Radiation Monitoring System....156
7.6.1.9 Instrumentation and Control Power Supply System....156
7.6.1.10 RHR Recirculation System Sump Isolation Valves Interlock....157
7.6.1.11 Interlocks for RCS Pressure Control During Low Temperature Operation....157

7.6.2 ANALYSIS....159
7.6.2.1 Residual Heat Removal System Isolation Valves Interlock....159
7.6.2.2 Spent Fuel Pool Cooling and Cleanup System....160
7.6.2.3 Instrumentation and Control Power Supply System....162
7.6.2.4 RHR Recirculation System Isolation Sump Valves Interlock....163
7.6.2.5 RCS Pressure Control During Low Temperature Operation....164

REFERENCES: SECTION 7.6....165

7.7 CONTROL SYSTEMS NOT REQUIRED FOR SAFETY....165

7.7.1 DESCRIPTION....165
7.7.1.1 Reactor Control Rod System....168
7.7.1.2 Rod Control System....169
7.7.1.3 Plant Control Signals for Monitoring and Indicating....170
7.7.1.4 Plant Control System Interlocks....174
7.7.1.5 Pressurizer Pressure Control....176
7.7.1.6 Pressurizer Water Level Control....176

7.7.1.7 Steam Generator Water Level Control 177
7.7.1.8 Steam Dump Control 177
7.7.1.9 Incore Instrumentation 178
7.7.1.10 Deleted by Amendment No. 40. 180
7.7.1.11 Safety-related Instrumentation Freeze Protection 180
7.7.2 ANALYSIS 181
7.7.2.1 Separation of Protection and Control System 182
7.7.2.2 Response Considerations of Reactivity 183
7.7.2.3 Step Load Changes Without Steam Dump 186
7.7.2.4 Loading and Unloading 186
7.7.2.5 Load Rejection Furnished by Steam Dump System 187
7.7.2.6 Turbine-Generator Trip With Reactor Trip 187
REFERENCES: SECTION 7.7: 188

7.0 INSTRUMENTATION AND CONTROLS

7.1.0 INTRODUCTION

This chapter presents the plant instrumentation and control systems associated with varying levels of safety by relating the functional performance requirements, design bases, system descriptions, design evaluations, and test and inspections for each system. The information 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." Conformance to applicable criteria and codes, such as the General Design Criteria (10 CFR 50 Appendix A) and the appropriate IEEE Standards, are addressed specifically in the applicable sections.

The primary purpose of the instrumentation and control system is to provide automatic protection and exercise proper control against unsafe and improper reactor operations during steady state and transient power operations (ANS Conditions I, II and III) and to provide initiating signals to mitigate the consequences of faulted conditions (ANS Condition IV). ANS conditions are discussed in Chapter 15.0. Consequently, the information presented in this chapter emphasizes those instrumentation and control systems which are central to assuring that the reactor can be operated to produce power in a manner that ensures no undue risk to the health and safety of the public.

It is shown that the applicable criteria and codes, such as General Design Criteria and IEEE Standards, concerned with the safe generation of nuclear power are met by these systems (see Table 7.1.0-1 for a listing of applicable criteria).

Definitions - Terminology used in this chapter is based on the definitions given in IEEE Standard 279-1971 which is listed in Section 7.1.2. In addition, the following definitions apply:

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

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

Cold Shutdown Condition - When the reactor is subcritical with k_{eff} <0.99, 0 percent thermal power and T_{avg} is ≤200 F.

Hot Shutdown Condition - When the reactor is subcritical, with k_{eff} <0.99, 0 percent thermal power, and 200F <T_{avg} <350F.

Hot Standby - When the reactor is subcritical with k_{eff} <0.99, 0 percent thermal power and T_{avg} ≥ 350F.

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

Phase B Containment Isolation -Closure of remaining process lines not closed by a Phase A containment isolation signal, initiated by containment Hi-3 pressure signal and by manual

initiation of the containment spray actuation signal (process lines do not include engineered safety features lines.)

Reactor Trip System Response Time - The time interval from when the monitored parameter exceeds its trip setpoint at the channel sensor until loss of stationary gripper coil voltage.

Engineered Safety Feature Response Time - Time interval from when the monitored parameter exceeds its ESF actuation setpoint at the channel sensor until the ESF equipment is capable of performing its safety function (i.e., the valves travel to their required positions, pump discharge pressures reach their required values, etc.). Times shall include diesel generator starting and sequence loading delays where applicable.

Reproducibility - This definition is taken from Scientific Apparatus Manufacturers Association (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.

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

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

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

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

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

Trip Accuracy - This definition includes comparator accuracy, channel accuracy, for each input, and rack environmental effects. This is the tolerance expressed in process terms (or percent of span) within which the complete channel should perform its intended trip function. This includes all instrument channel uncertainties, calibration errors, process measurement effects in addition to any harsh environment errors, if appropriate. The term "actuation accuracy" may be used where the word "trip" might cause confusion (for example, when starting pumps and other equipment).

Control Accuracy - This definition includes channel accuracy, accuracy of readout devices (isolator and 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. The control accuracy is defined as the accuracy of the control signal in percent of the span of that signal, including gain changes where the control span is different from the span of the measured variable. Where controllers are involved, the control span is the input span of the controller. No error is included for the time in which the system is in a nonsteady state condition.

7.1.1 IDENTIFICATION OF SAFETY-RELATED SYSTEMS

Safety-related instrumentation and control systems are identified below. The responsibility for design and supply of each system is identified as follows:

a) Ebasco Services, Incorporated. (E)

b) Westinghouse Electric Corporation. (W)

7.1.1.1 Protection Systems

Protection systems, as defined in IEEE-279-1971, include the electrical and mechanical devices and circuitry (from sensors to actuation device input terminals) involved in generating the signals associated with the two protective functions defined below.

The Solid State Protection System (SSPS) (W) consists of:

a) Reactor Protection System (RPS) (W) - The RPS generates signals that actuate reactor trip. This system is part of the Reactor Trip System and is functionally described in Section 7.2. Design bases for the Reactor Trip System are given in Section 7.1.2.1. Figure 7.1.1-1 includes a block diagram of this system.

b) Engineered Safety Features Actuation System (ESFAS) (W) - The ESFAS generates signals that actuate engineered safety features. This system is a part of the Engineered Safety Features System and is described in Section 7.3. Instrumentation and controls associated with interfacing ESF systems are discussed in Section 7.3. Design bases for the Engineered Safety Features Actuation System are given in Section 7.1.2.1.

7.1.1.2 Engineered Safety Feature System (ESF System)

The ESF Systems include the components that perform protective actions after receiving a signal from the ESFAS or the operator.

The ESF systems are:

a) Containment Heat Removal System (E)

b) Containment Isolation System (E)

c) Main Steam Line Isolation System (W)

d) Emergency Core Cooling System (W)

e) Auxiliary Feedwater System (E)

f) Combustible Gas Control System (manually initiated) (E)/(W)

g) Emergency Exhaust System (E)

h) Main Feedwater Isolation System (E)

The instrumentation and controls for ESF systems including design bases are described in Section 7.3.

7.1.1.3 ESF Supporting Systems

The ESF supporting systems include the components that must function to support the operation of the ESF systems. The ESF supporting systems are:

a) Emergency Power System (E)

b) Emergency Service Water System (E)

c) Component Cooling Water System (W)

d) Essential Services Chilled Water System (E)

e) 120V Uninterruptible AC System (E)

f) Safety-related 125V DC Power System (E)

g) Control Room Ventilation System (E)

h) RAB Equipment Cooling System (E)

i) Diesel Generator Building Ventilation System (E)

j) RAB Switchgear Room Ventilation System (E)

k) Diesel Fuel Oil System (E)

l) Spent Fuel Pool Pump Room Ventilation System (E)

m) RAB Electrical Equipment Protection Room Ventilation System (E)

n) Fuel Oil Transfer Pump House Ventilation System (E)

o) Emergency Service Water Intake Structure Ventilation System (E)

p) Containment Vacuum Relief System (E)

The instrumentation and controls for the ESF supporting systems including design bases are described in Section 7.3.

7.1.1.4 Safe Shutdown Systems

The safe shutdown systems include those systems required to establish and maintain the reactor in a safe shutdown condition.

a) Residual Heat Removal System (W)

b) Steam Generator Safety Valves (E)

c) Boric Acid Addition Portions of the Chemical and Volume Control System (W)

d) Auxiliary Feedwater System (E)

The instrumentation and controls for the safe shutdown systems are described in Section 7.4. In addition, the ESF support systems identified in Section 7.1.1.3 are required for safe shutdown.

7.1.1.5 Display Instrumentation for Safety-Related Systems

The following display instrumentation for safety-related systems enables the operator to monitor plant operating conditions. Sufficient information is provided for the operator to perform the required manual safety actions.

a) Plant process display instrumentation (E,W)

b) Reactor trip system monitoring (W)

c) Engineered safety features system monitoring (E,W)

d) RCCA position indication system (W)

e) Safe shutdown system monitoring (E,W)

f) Post-accident monitoring (E,W)

g) ESF support system monitoring (E,W)

h) Auxiliary control panel instrumentation (E)

i) Bypass and inoperable status indication (E)

j) Control board annunciation and light boxes (E,W)

This instrumentation is described in Section 7.5. Section 7.4 summarizes procedures required to achieve and maintain the plant in a hot shutdown condition, or to proceed to cold shutdown.

7.1.1.6 All Other Systems Required for Safety

All other systems required for safety include the interlocks required to prevent overpressurization of the Residual Heat Removal System and the systems, listed below, which provide radiation monitoring or cooling functions:

a) Residual Heat Removal System Interlocks (W)

b) Accumulator Isolation Valve Interlocks (W)

c) Fuel Pool Cooling Subsystem of the Spent Fuel Pool Cooling and Cleanup System (E)

d) ECCS Leak Detection System (E)

e) Diesel Fuel Oil System (E)

f) Safety-related Radiation Monitoring System (E)

g) Reactor Vessel Instrumentation (W)

h) Refueling Interlocks (E)

These systems are described in Section 7.6 with the exception of the Diesel Fuel Oil System which is described in Section 9.5.4, the safety-related Radiation Monitoring System described in Section 11.5, the ECCS leak detection monitoring system described in Section 7.5.1, and the Reactor Vessel Instrumentation (ICC) which is described in Section 7.5.1.

7.1.1.7 Instrumentation and Control System Designers

All systems discussed in Chapter 7.0 have definitive functional requirements developed on the basis of the Westinghouse NSSS design. Figure 7.2.1-1 defines scope interface. Regardless of the suppliers, the functional requirements necessary to assure plant safety and proper control are clearly delineated.

7.1.1.8 Plant Comparison

System functions for all NSSS systems discussed in Chapter 7.0 are similar to those of South Texas Project, Docket No. 50-498. A comparison between SHNPP and South Texas is provided in Table 7.1.1-1.

The ESF Systems that are not part of the NSSS are functionally similar in design to the ESF Systems provided for the Waterford Unit No. 3 (Docket No. 50-382) except that SHNPP does not have a Shield Building Ventilation System. A comparison between SHNPP and Waterford is provided in Table 7.1.1-2.

7.1.2 IDENTIFICATION OF SAFETY CRITERIA

Section 7.1.2.1 gives design bases for the reactor protection and Engineered Safety Features Actuation Systems identified in Section 7.1.1.1. Design bases for other safety and non-safety-related systems are provided in the sections which describe the systems. Considerations for instrument errors are included in the accident analyses presented in Chapter 15.0. Functional requirements, developed on the basis of the results of the accident analyses, that have utilized conservative assumptions and parameters are used in designing these systems and a preoperational testing program verifies the adequacy of the design. Instrument accuracy is given in Sections 7.2, 7.3, and 7.5.

The design bases, criteria, regulatory guides, standards and other documents that are considered in the design of the Ebasco and Westinghouse supplied systems are listed in Table 7.1.0-1. In general, the scope of these documents is given in the document itself. This determines the systems or parts of systems to which the document is applicable. A discussion of compliance with each document for systems in its scope is provided in the referenced sections given in Table 7.1.0-1 for each criterion. However, due to the fact that some documents were issued after design and testing had been completed, the equipment documentation may not meet the format requirements of some standards. Justification for any exceptions taken to each document for systems in its scope is provided in the referenced sections.

The extent to which the recommendations of the regulatory guides listed in Table 7.1.0-1 are followed is described in Section 1.8.

Criteria applied to the physical separation and identification of redundant safety-related electrical and instrumentation and control systems are discussed in Sections 8.3.1.4, 8.3.1.3, 7.1.2.3, and 7.1.2.2.

7.1.2.1 Design Bases

7.1.2.1.1 Reactor Trip System

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

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

a) Minimum departure from nucleate boiling ration (DNBR) shall not be less than limit DNBR as a result of any anticipated transient or malfunction (ANS Condition II events).

b) Power density shall not exceed the rated linear power density for ANS Condition II events. Refer to Chapter 4.0 for fuel design limits.

c) The stress limit of the Reactor Coolant System for the various conditions shall be as specified in Chapter 5.0.

d) Release of radioactive material shall be limited so as not to interrupt or restrict public use of those areas beyond the exclusion radius as a result of any ANS Condition III event.

e) For any ANS Condition IV event, release of radioactive material shall not result in an undue risk to public health and safety.

7.1.2.1.2 Engineered safety features actuation system

The Engineered Safety Features Actuation System acts to limit the consequences of ANS Condition III events (infrequent faults such as primary coolant spillage from a small rupture which exceeds normal charging system makeup and requires actuation of the Safety Injection System).

The Engineered Safety Features Actuation System acts to mitigate ANS Condition IV events (limiting faults which include the potential for significant release of radioactive material).

The design bases for the Engineered Safety Features Actuation System are derived from the design bases given in Chapter 6.0 for the engineered safety features. Design bases requirements of IEEE Standard 279-1971 are addressed in Section 7.3.2.2. General design requirements are given below.

a) Automatic actuation requirements - The primary requirement of the Engineered Safety Features Actuation System is to receive input signals (information) from the various on-going processes within the 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.

b) Manual actuation requirements - The Engineered Safety Features Actuation System must have provisions in the Control Room for manually initiating the functions of the Engineered Safety Features System.

7.1.2.1.3 Emergency power

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

7.1.2.1.4 Interlocks

Interlocks are discussed in Sections 7.2, 7.3, 7.6, and 7.7. The protection (P) interlocks are given on Tables 7.2.1-2 and 7.3.1-4. The safety analyses demonstrate that the protective systems ensure that the NSSS will be put into and maintained in a safe state following a ANS Condition II, III or IV accident commensurate with applicable Technical Specifications and pertinent ANS Criteria. 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 is required to function in accordance with General Design Criteria 20, 21, and 22 and Sections 4.11, 4.12, and 4.13 of IEEE Standard 279-1971. Control interlocks (C) are identified in Table 7.7.1 1. Because control interlocks are not safety-related, they have not been specifically designed to meet the requirements of IEEE Protection System Standards.

7.1.2.1.5 Bypasses

Bypasses are designed to meet the requirements of IEEE Standard 279-1971, Sections 4.1, 4.2, 4.3, 4.4, 4.5, 4.11, 4.12, 4.13, and 4.14. A discussion of bypasses provided is given in Sections 7.2 and 7.3.2.2.13. Routine testing in bypass will only be performed when installed hardware and applicable Technical Specification Action Statements are available to allow testing in bypass without reliance on lifted leads or jumpers (other than to connect test equipment), with the exception of the RWST Low-Low level function as noted in Section 7.3.2.2.13. (Reference 7.1.2-5)

7.1.2.1.6 Equipment protection

The criteria for equipment protection are given in Chapter 3.0. Equipment related to safe operation of the plant is designed, constructed and installed to protect it from damage. This is accomplished by working to accepted standards and criteria aimed at providing reliable instrumentation which is available under varying conditions. As an example, certain equipment is seismically qualified in accordance with IEEE Standard 344-1975. During construction, independence and separation is achieved, as required by IEEE Standard 279-1971, IEEE Standard 384-1974 and Regulatory Guide 1.75, either by barriers, physical separation or demonstration test. This serves to protect against complete destruction of a system by fires, missiles or other natural hazards.

7.1.2.1.7 Diversity

Functional diversity as discussed in Reference 7.1.2-1 has been designed into the system. The extent of diverse system variables has been evaluated for a wide variety of postulated accidents. Generally, two or more diverse protection functions would automatically terminate an accident before unacceptable consequences could occur.

For example, there are automatic reactor trips based upon neutron flux, reactor coolant loop temperature, pressurizer pressure and level, and reactor coolant pump underfrequency and undervoltage, and a safety injection signal. Reactor trip may also be initiated manually.

In response to a loss-of-coolant accident, a safety injection signal can be obtained manually or by automatic initiation from two diverse parameter measurements.

a) Low pressurizer pressure.

b) High containment pressure (Hi-1).

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

a) Low steam pressure.

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

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

7.1.2.1.8 Bistable trip setpoints

There are three values applicable to reactor trip and engineered safety features actuation:

a) Safety limit,

b) Limiting value, and

c) Nominal value.

The safety limit is the value assumed in the accident analysis and is the conservative value. The limiting value is the Technical Specification value and is obtained by applying a safety margin in the conservative direction from the safety limit. The safety margin accounts for instrument error, and process uncertainties such as flow stratification and transport factor effects. The nominal value is the value set into the equipment and is obtained by applying additional allowances for instrument drift from the limiting value. The nominal value allows for the normal expected instrument setpoint drifts such that the Technical Specification limits will not be exceeded under normal operation.

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

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

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

The specific functional requirements for response time, setpoint, and operating span are based on the results and evaluation of safety studies carried out using data pertinent to the SHNPP. This establishes adequate performance requirements under both normal and faulted conditions, includes consideration of process transmitter margins such that even under a highly improbable situation of full power operation at the limits of the operating map (as defined by the high and low pressure reactor trip, ΔT overpower and ΔT overtemperature trip lines [DNB protection] and the steam generator safety valve pressure setpoint) that adequate instrument response is available to ensure plant safety. The safety margin incorporates the instrument error under applicable post-accident environmental conditions, as indicated in studies in Reference 7.2.1-4 and 7.2.1-5.

7.1.2.2 Independence of Redundant Safety-Related Systems

The safety-related systems described in Section 7.1.1.1 are designed to meet the independence and separation requirements of GDC Criterion 22 and Section 4.6 of IEEE Standard 279-1971.

The electrical power supply, instrumentation, and control conductors for redundant circuits of a nuclear plant have physical separation to preserve the redundancy and to ensure that no single credible event will prevent operation of the associated function due to electrical conductor damage. Critical circuits and functions include power, control and analog instrumentation associated with the operation of the Reactor Trip System or Engineered Safety Features Actuation System. Events considered credible and considered in the design include the effects of short circuits, pipe rupture, missiles, and fire.

7.1.2.2.1 General (Include Regulatory Guide 1.75 and IEEE Standard 384-1974)

The physical separation criteria for redundant safety-related system sensors, sensing lines, wireways, cables, and components on racks within NSSS scope meet recommendations contained in Regulatory Guide 1.75 with the following comments:

a) The Westinghouse design of the protection system relies on the provisions of IEEE Standard 384-1974 relative to overcurrent devices to prevent malfunctions in one circuit from causing unacceptable influences on the functioning of the protection system. The protection system uses redundant instrumentation channels and actuation trains and incorporates physical and electrical separation to prevent faults in one channel from degrading any other protection channel.

b) Separation recommendations for redundant instrumentation racks are not the same as those given for the control boards in Regulatory Position C.16 of Regulatory Guide 1.75, Revision 1, because of different functional requirements. Main control boards contain redundant circuits which are required to be physically separated from each other. However, since there are no redundant circuits which share a single compartment of an NSSS protection instrumentation rack, and since these redundant protection instrumentation racks are physically separated from each other, the physical separation requirements specified for the main control board do not apply.

   However, redundant, isolated control signal cables leaving the protection racks are brought into close proximity elsewhere in the plant, such as the control board. It could be postulated that electrical faults, or interference, at these locations might be propagated into all redundant racks and degrade protection circuits because of the close proximity of protection

and control wiring within each rack. Regulatory Guide 1.75 (Regulatory Position C.4) and IEEE Standard 384-1974 (Section 4.5(3)) provide the option to demonstrate by test that the absence of physical separation could not significantly reduce the availability of Class 1E circuits.

Westinghouse test programs have demonstrated that Class 1E protection systems (Nuclear Instrumentation System, Solid State Logic Protection System, Reactor Trip Switchgear and 7300 process control system) are not degraded by non-Class 1E circuits sharing the same enclosure. Conformance to the requirements of IEEE Standard 279-1971 and Regulatory Guide 1.75 has been established and accepted by the NRC based on the following which is applicable to these systems at the Shearon Harris Nuclear Power Plant.

Tests conducted on the as-built designs of the Nuclear Instrumentation System and Solid State Logic Protection System were reported and accepted by the NRC in support of the Diablo Canyon applications (Docket Nos. 50-275 and 50-323). Westinghouse considers these programs as applicable to all plants, including the SHNPP. Westinghouse tests on the 7300 process control system were covered in a report entitled, "7300 Series Process Control System Noise Tests," subsequently reissued as Reference 7.1.2-2. In a letter dated April 20, 1977 (Reference 7.1.2-3) the NRC accepted the report in which the applicability of the SHNPP is established.

c) The physical separation criteria for instrument cabinets within NSSS scope meet the recommendations contained in Section 5.7 of IEEE Standard 384-1974.

7.1.2.2.2 Specific systems

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

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

In the Nuclear Instrumentation System, process systems, and the Solid State Logic Protection System input cabinets where redundant channel instrumentation are physically adjacent, there are no wireways or cable penetrations which would permit a fire resulting from electrical failure in one channel to propagate into redundant channels in the logic racks. Redundant analog channels are separated by locating modules in different cabinets. Since all equipment within any cabinet is associated with a single protection set, there is no requirement for separation of wiring and components within the cabinet.

Two reactor trip breakers are actuated by two separate logic matrices to 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.

a) Reactor Trip System

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

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

b) Engineered Safety Features Actuation System

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

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

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

c) Instrumentation and control power supply system - The separation criteria presented also apply to the power supplies for the load centers and buses distributing power to redundant components and to the control of these power supplies.

d) Control Board - Certain wiring within control boards has been designed and installed to maintain physical independence. Design features include enclosed modular switches, metal wireways (gutters), use of cable rated at 600 volt-200C temperature, non-combustible insulation, and metallic woven braid applied to the outer jacket of non-safety-related wires.

The control board wiring is physically separated from the switch module to the metal wireways (gutters). Field termination connectors are provided and arranged on these wiring bulkheads to provide the interface and continuity between the safety-related field wiring and safety-related control board wiring. Non-safety wiring is also routed separately via wire bundles and carried to separate field termination connector panels. These panels are arranged to provide the interface and continuity between field wiring and non-safety control board wiring.

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

In order to maintain separation between wiring associated with different trains, mutually redundant safety train wiring is not terminated on a single device. For the manual reactor trip, see Section 7.2.1.1.2 and Figure 7.2.1-3. For the engineered safety features manual action circuits see Section 7.3.1.1. For safety-related display instrumentation, see Section 7.5.

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

7.1.2.2.3 Fire protection

Electrical equipment specifications specifies non-combustible or fire retardant material and conducts vendor supplied specification reviews of this equipment which includes assurance that materials are not used which may ignite or explode from an electrical spark, flame, or from heating, or will independently support combustion. These reviews also include assurance of current carrying capacities of all instrument cabinet wiring, which precludes electrical fires resulting from excessive overcurrent (I^2R) losses. For example, wiring used for instrument cabinet construction has teflon or tefzel insulation and is adequately sized based on current carrying capacities set forth by the National Electric Code. In addition, non-combustible paint is used on protection rack or cabinet construction to retard fire or heat propagation from rack-to-rack. Braided sheath material used in the cables is non-combustible.

Details of the Fire Protection System are provided in Section 9.5.1.

7.1.2.3 Physical Identification of Safety-Related Equipment

There are four separate protection sets identifiable with process equipment associated with the Reactor Trip System and Engineered Safeguards Actuation System. A protection set may be comprised of more than a single process equipment cabinet. The color coding of each process equipment rack nameplate coincides with the color code established for the protection set of which it is a part. Redundant channels are separated by locating them in different equipment cabinets. Separation of redundant channels begins at the process sensors and is maintained in the field wiring, containment penetrations and equipment cabinets to the redundant trains in the logic racks. The solid state protection system input cabinets are divided into four isolated compartments, each serving one of the four redundant input channels. Horizontal 1/8 in. thick solid steel barriers, coated with fire retardant paint, separate the compartments. Four 1/8 in. thick solid steel wireways coated with fire retardant paint enter the input cabinets vertically, in its own quadrant. The wireway for a particular compartment is open only 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

Protection Set	Color Coding
II	WHITE with BLACK lettering
III	BLUE with WHITE lettering
IV	YELLOW with BLACK lettering

All non-cabinet mounted protective equipment and components are provided with an identification tag or nameplate. Small electrical components such as relays 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 shall be identified using permanent markings. The purpose of such markings is to facilitate cable routing identification for future modification or additions. Positive permanent identification of cables and/or conductors shall be made at all terminal points. There are also identification nameplates on the input panels of the Solid State Logic Protection System.

7.1.2.4 Conformance to Criteria

A listing of applicable criteria and the sections where conformance is discussed is given in Table 7.1.0-1.

7.1.2.5 Conformance to Regulatory Guide 1.22

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

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

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

a) There is no practicable system design that would permit operation of the equipment without adversely affecting the safety or operability of the plant. See Section 7.3.2.2.10.7 and 10.3.3 for discussions of freedom of motion testing of MSIVs and MFIVs.)

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

c) The equipment can routinely be tested when the reactor is shutdown.

The list of equipment that cannot be tested at full power without possibly damaging equipment or upsetting plant operation is:

a) Manual actuation switches,

b) Turbine trip system,

c) Main steam line isolation valves (close),

d) Main feedwater isolation valves (close),

e) Feedwater control valves (close),

f) Main feedwater pump,

g) Reactor coolant pump component cooling water isolation valves (close),

h) Reactor coolant pump seal water return valves (close), and

i) Additional equipment which cannot be tested at full power without upsetting the plant operation or possibly damaging the equipment:

    1) Deleted by Amendment No. 48

    2) Deleted by Amendment No. 48

    3) Service water to CVCS chillers (close to test)

    4) Deleted by Amendment No. 48

    5) Containment Building instrument air isolation valve (close to test)

    6) Containment spray pump tank suction supply valve (close to test)

    7) Deleted by Amendment No. 51

    8) Main generator trip system

    9) Reactor coolant pump (trip to test)

    10) Non-safety portion of the Steam Dump System

    11) Standby diesel generator breakers (trip to test)

    12) Essential load sequencer system (actuate to test)

    13) Deleted by Amendment No. 51

DISCUSSION

ITEMS i - 1 and 2 - Deleted by Amendment No. 48

ITEM i - 3 - The CVCS chillers when isolated would adversely affect the CVCS system capability.

ITEM i - 4 - Deleted by Amendment No. 48

ITEM i - 5 - Isolation of instrument air would affect non-safety equipment relying on air for operation. Also containment isolation valves inside the Containment may close as a result of loss of air pressure.

ITEM i - 6 - The containment spray pump of the tested train would not have any suction.

ITEM i - 7 - Deleted by Amendment No. 51

ITEM i - 8 - Generator trip would cause plant upset condition similar to turbine trip and/or reactor trip.

ITEM i - 9 - The SSPS undervoltage trip of the reactor coolant pumps would trip the reactor.

ITEM i - 10 - Blocking the steam dump system function under normal operation could negate the plant response to sudden load decrease.

ITEM i - 11 - Emergency diesel generator breaker cannot be tested because of effect on the diesel generator protection system.

ITEM i - 12 - Essential load sequencer is not fully tested because it would initiate a plant shutdown in essence. Each individual actuating circuit can be tested up to the output contact. The affected equipment may be tested from the MCB manually.

Item i - 13 - Deleted by Amendment No. 51

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

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

   The analog signals, from which the automatic safety injection signal is derived, is tested at power in the same manner as the other analog signals and as described in Section 7.2.2.2.3. The processing of these signals in the solid state protection system wherein their channel orientation converts to a logic train orientation is tested at power by the built-in semiautomatic test provisions of the solid state protection system. The reactor trip breakers are tested at power as discussed in Section 7.2.2.2.3.

b) Turbine Trip System - The Turbine Trip System cannot be tested at power. Refer to Sections 10.2 and 7.3 for turbine trip system description.

c) Closing the main steam line isolation valves - Main steam isolation valves are routinely tested during refueling outages. Testing of the main steam isolation valves to closure at power is not practical. As the plant power is increased, the coolant average temperature is programmed to increase. If the valves are closed under these elevated temperature conditions, the steam pressure transient would unnecessarily operate the steam generator relief valves and possibly the steam generator safety valves. The steam pressure transient

produced would cause shrinkage in the steam generator level, which would cause the reactor to trip on low-low steam generator water level. Testing during operation would decrease the operating life of the valve. Based on the above identified problems incurred with periodic testing of the main steam line isolation valves at power and since: 1) no practical system design will permit operation of the valves without adversely affecting the safety or operability of the plant, 2) the probability that the protection system will fail to initiate the actuated equipment is acceptably low due to test up to final actuation, and 3) these valves will be routinely tested during refueling outages, the proposed resolution meets the guidelines of Regulatory Position.4 of Regulatory Guide 1.22.

d) Closing the main feedwater isolation valves - The feedwater isolation valves are routinely tested during refueling outages. Periodic testing of these feedwater isolation valves, closing them completely, or partially, at power would induce steam generator water level transients and oscillations which would trip the reactor. These transient conditions would be caused by perturbing the feedwater flow and pressure conditions necessary for proper operation of the steam generator water level control system. Any operation which induces perturbations in the main feedwater flow, whether deliberate or otherwise, generally leads to a reactor trip and should be avoided. Based on these identified problems incurred with periodic testing of the feedwater isolation valves at power and since: 1) no practical system design will permit operation of these valves without adversely affecting the safety or operability of the plant, 2) the probability that the protection system will fail to initiate the activated equipment is acceptably low due to testing up to final actuation, and 3) these valves will be routinely tested during refueling outages, the proposed resolution meets the guidelines of Regulatory Position D.4 of Regulatory Guide 1.22.

e) Closing the feedwater control valves - These valves are routinely tested during refueling outages. To close them at power would adversely affect the operability of the plant. The verification of operability of feedwater control valves at power is assured by confirmation of proper operation of the steam generator water level control system. The actuation function of the slave relays, which provide the closing signal to the feedwater control valve solenoids, is periodically tested at power as discussed in Section 7.3.2.2.10. The operability of the slave relay which actuates the solenoid, which is the actuating device, is verified during this test. Although the closing of these control valves is blocked when the slave relay is tested, all functions are tested to assure that no electrical malfunctions have occurred which could defeat the protective function. The solenoids work on the de-energize-to-actuate principle, so that the feedwater control valves will fail closed upon either the loss of electrical power to the solenoids or loss of air pressure. Based on the above, the testing of the isolating function of feedwater control valves meets the guidelines of Regulatory Position D.4 of Regulatory Guide 1.22.

f) Main feedwater pump trip - Refer to Section 7.3.1 for details of main feedwater isolation. Main feedwater isolation will trip both the isolation valves and feedwater pumps. The isolation valves are safety grade equipment while the feedwater pumps are non-safety grade. The valves are periodically tested (see Section 7.3.2) in conjunction with the Engineered Safety Features Actuation System and manually initiated testing. Therefore, the main feedwater pumps require no on-line periodic testing to trip because isolation valves are tested. These functions are routinely tested during refueling outages.

g) Reactor coolant pump component cooling water isolation valves (close) - Component cooling water supply and return containment isolation valves are routinely tested during

refueling outages. Testing of these valves while the reactor coolant pumps are operating introduces an unnecessary risk of costly damage to the reactor coolant pumps. Loss of component cooling water to these pumps is to economic consideration only, as the reactor coolant pumps are not required to perform any safety-related function.

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

Also, since the component cooling water flow rates and temperatures, during both plant power operation and plant refueling, are approximately the same, periodic tests of these valves during a refueling outage would duplicate accident conditions. The possibility of failure of containment isolation is remote because an additional failure of the Component Cooling Water System (CCWS) in addition to failure of both CCWS isolation valves would have to occur to open a path through the Containment.

Based on the above described potential reactor coolant pump damage which could occur as a result of periodic testing of the component cooling water containment isolation valves at power, the duplication of at-power operating conditions during refueling outages, and since: 1) no practical system design will permit operation of these valves without adversely affecting the safety or operability of the plant, 2) the probability that the protection system will fail to initiate the activated equipment is acceptably low due to testing up to final actuation, and 3) these valves will be routinely tested during refueling outages when the reactor coolant pumps are not operating, the proposed resolution meets the guidelines of Regulatory Position D.4 of Regulatory Guide 1.22.

h) Reactor coolant pump seal water return valves (close) - Seal water return line isolation valves are routinely tested during refueling outages. Closure of these valves during operation would cause the seal water system relief valve to lift, with the possibility of valve chatter. Valve chatter could damage this relief valve. Testing of these valves at power could cause equipment damage. Therefore, these valves will be tested during scheduled refueling outages. As above, additional containment penetrations and containment isolation valves introduce additional unnecessary potential pathways for radioactive release following a postulated accident. Thus, the guidelines of Regulatory position D.4 of Regulatory Guide 1.22 are met.

7.1.2.6 Conformance to Regulatory Guide 1.47

The extent of compliance with Regulatory Guide 1.47 is discussed in Section 1.8.

7.1.2.7 Conformance to Regulatory Guide 1.53 and IEEE Standard 379-1972

The principles described in IEEE Standard 379-1972 were used in the design of the Solid State Logic Protection System. The system complies with the intent of this standard and the additional guidance of Regulatory Guide 1.53 although the formal analyses have not been documented exactly as outlined. Westinghouse has gone beyond the required analyses and has performed a fault tree analysis (Reference 7.1.2-1).

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

7.1.2.8 Conformance to Regulatory Guide 1.63

Design conformance to Regulatory Guide 1.63 for electrical penetration assemblies is discussed in Section 8.3.1.

7.1.2.9 Conformance to IEEE Standard 317-1972

Design conformance to IEEE Standard 317-1972 for electrical penetrations is discussed in Section 8.3.1.

7.1.2.10 Conformance to IEEE Standard 336-1971

Design conformance to IEEE Standard 336-1971 for installation, inspection and testing is discussed in Section 8.3.1. The MCB and SCB conform to IEEE 336-1980.

7.1.2.11 Conformance to Regulatory Guide 1.68

Conformance to Regulatory Guide 1.68 for preoperational and startup testing is discussed in Chapter 14 and Section 1.8.

7.1.2.12 Conformance to Regulatory Guide 1.68.3

Conformance to Regulatory Guide 1.68.3 for preoperational testing of instrument air is discussed in Section 1.8.

7.1.2.13 Conformance to Regulatory Guide 1.89

Conformance to Regulatory Guide 1.89 for the qualification of equipment is discussed in Sections 1.8, 3.10 and 3.11.

7.1.2.14 Conformance to Regulatory Guide 1.97

Conformance to Regulatory Guide 1.97 for post-accident monitoring is discussed in Sections 1.8 and 7.5.

7.1.2.15 Conformance to Regulatory Guide 1.100

Conformance to Regulatory Guide 1.100 for seismic qualification is discussed in Sections 1.8 and 3.10.

7.1.2.16 Conformance to Regulatory Guide 1.105

Conformance to Regulatory Guide 1.105 for instrument spans and setpoints is discussed in Sections 1.8 and 7.3.

7.1.2.17 Conformance to Regulatory Guide 1.118

Conformance to Regulatory Guide 1.118 for periodic testing of electrical power and protection systems is discussed in Section 1.8.

7.1.2.18 Conformance to IEEE Standard 338-1971

The periodic testing of the Reactor Trip System and Engineered Safety Features Actuation System conforms to the requirements of IEEE Standard 338-1971 as detailed in Sections 1.8 (RG 1.118), 8.3.1.2.27, and 13.5.1.3.e) with the following comments:

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

Overall protection systems response times are demonstrated by test and/or verification. Sensors within the Westinghouse scope are demonstrated adequate for this design by vendor testing, in-site tests in operating plants with appropriately similar design, or by suitable type testing. After an initial hydraulic ramp type test prior to installation, an allocated time may be used for certain sensors enveloped by License Amendment No. 112 to Facility Operating License No. NFP-63 for the Shearon Harris Nuclear Power Plant Unit 1. The nuclear instrumentation system detectors are excluded since they exhibit response time characteristics such that delays attributable to them are negligible in the overall channel response time required for safety.

A periodic verification test program for sensors for determining any deterioration of installed sensor's response time has been developed utilizing currently available test equipment. Technical Specifications require periodic verification on at least 18-month intervals.

Each verification shall include at least one logic train such that both logic trains are verified 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 protective function.

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

The performance of the protection system radiation monitors (Containment Vent Isolation Signal), supplied by EBASCO, are checked using two techniques:

1) Circuit checks can be performed at the discretion of the operator as appropriate. These checks are accomplished by activating the checksource pushbutton which activates a test current that verifies the counting circuitry.

2) Specific calibration checks are performed at a frequency specified by the Technical Specifications using an NBS traceable calibration source and known geometry to yield an observed countrate.

   Based on a complete statistical analysis of these countrates, the performance of the monitors can be evaluated. From this information and new information about the background countrate, the expected response function of the monitor can be calculated.

b) The reliability goals specified in Section 4.2 of IEEE Standard 338-1971 and the adequacy of time intervals between failures are documented in the Maintenance Rule Scoping Document for the Reactor Protection and Engineered Safety Features Actuation System.

c) The periodic time interval discussed in Section 4.3 of IEEE Standard 338-1971, and specified in Technical Specifications, is conservatively selected to assure that equipment associated with protection functions has not drifted beyond its minimum performance requirements. If any protection channel appears to be marginal or requires more frequent adjustments due to plant condition changes, the time interval will be decreased to accommodate the situation until the marginal performance is resolved.

d) The test interval discussed in Section 5.2 of IEEE Standard 338-1971, is developed primarily on past operating experience and modified if necessary to assure that system and subsystem protection is reliably provided. Analytic methods for determining reliability are not used to determine test interval.

   Based on the scope definition given in IEEE Standard 338-1971, no other systems described in Chapter 7.0 are required to comply with this standard.

REFERENCES: SECTION 7.1

7.1.2-1 Gangloff, W.C. and Loftus, W.D., "An Evaluation of Solid State Logic Reactor Protection in Anticipated Transients," WCAP-7706-L (Proprietary) and WCAP-7706 (Non-Proprietary), July, 1971.

7.1.2-2 Marasco, F.W. and Siroky, R.M., "Westinghouse 7300 Series Process Control System Noise Tests," WCAP-8892-A, June 1977.

7.1.2-3 Letter dated April 20, 1977 from R.L. Tedesco (NRC) to C. Eicheldinger (Westinghouse).

7.1.2-4 Letter dated December 17, 1996 from Gary Ferrell (Westinghouse) to Arvin Klemp, "Internal Wiring Separation - Reactor Trip Switchgear," 96-CQL-076.

7.1.2-5 Letter dated June 7, 2000 from James Scarola (CP&L) to USNRC, "Revision to Technical Specification 3/4.3.2 - Engineered Safety Features Actuation System Instrumentation Requirements," HNP-00-001.

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 exceeded (or reached). 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 and 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 reaches a setpoint the reactor will be shutdown in order to protect against either gross damage to fuel cladding or loss of system integrity which could lead to release of radioactive fission products into the Containment.

The following systems make up the Reactor Trip System. Refer to References 7.2.1-1, 7.2.1-2 and 7.2.1-3 for additional background information.

1. Process Instrumentation and Control System.

2. Nuclear Instrumentation System.

3. Solid-State Logic Protection System.

4. Reactor Trip Switchgear.

5. Manual Actuation Circuit.

The Reactor Trip System contains sensors, which, when connected with analog circuitry consisting of two to four redundant channels, monitor various plant parameters. The Reactor Trip System also contains digital circuitry, consisting of two redundant logic trains, which receive inputs from the analog protection channels to complete the logic necessary to automatically open the reactor trip breakers.

Each of the two trains, A and B, is capable of opening a separate and independent reactor trip breaker, RTA and RTB, respectively and a bypass breaker, BYB and BYA, 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 7.2.1-1, Sheet 2. During plant power operation, a DC undervoltage coil on each reactor trip breaker holds a trip plunger out against its spring, allowing the power to be available at the rod control power supply cabinets. For reactor trip, a loss of DC voltage to the undervoltage coil, as well as energization of the shunt coil, trips open the breaker. When either of the trip breakers opens, power is interrupted to the

---

*Further information is contained in the TMI appendix.

rod drive power supply, and the control rods fall, by gravity, into the core. The rods cannot be withdrawn until the trip breakers are manually reset. The trip breakers cannot be reset until the abnormal condition which initiated the trip is corrected. Bypass breakers BYA and BYB are provided to permit testing of the trip breakers, as discussed in Section 7.2.2.2.3.10.

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 (ANS Condition II).

2. To limit core damage for infrequent faults (ANS 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 (ANS 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. The turbine trip avoids 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, a proven design, quality components, proven manufacturing methods, quality control and testing are used. In addition to redundant channels and trains, the design approach provides a Reactor Trip System which monitors numerous system variables, therefore providing protection system functional diversity. The extent of this diversity has been evaluated for a wide variety of postulated accidents.

Table 7.2.1-1 provides a list of reactor trips which are described below.

1. Nuclear Overpower Trips - The specific trip functions generated are as follows:

    a. Power range high neutron flux trip - The power range high neutron flux trip circuit trips the reactor when two of the four power range channels reach the trip setpoint.

    There are two bistables (for each of the four power range channels), 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 percent power (P-10). Three out of the four channels below 10 percent automatically reinstates the trip function. Refer to Table 7.2.1-2 for a listing of all protection system interlocks.

b. Intermediate range high neutron flux trip (anticipatory) - 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 percent power (P-10). Three out of the four power range channels below this value automatically reinstates the intermediate range high neutron flux trip. The intermediate range channels (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. This bypass action is annunciated on the main control board. Intermediate range reactor 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 safety analyses (Chapter 15) for this trip. For example, the analysis of uncontrolled RCCA bank withdrawal from low power of subcritical in FSAR section 15.4.1 conservatively relies upon the power range low setpoint (alone). While one of the design bases generally considered in the protection system is the possibility of an earthquake, intermediate range reactor trip is not required to be fully operable during or immediately after a seismic event. The intermediate range reactor trip function is unrelated to a seismic event in that this trip function is anticipatory in nature and is not credited in the Chapter 15 accident analyses. This design functions in a de-energize-to-trip fashion to cause a plant trip if power is interrupted in the trip circuitry. This ensures that the protection system will in no way be degraded by this anticipatory trip because seismic design considerations do not form part of the design bases for intermediate range reactor trip. The anticipatory trips thus meet the redundancy, separation, and single failure criteria of IEEE Standard 279-1971. With a functional check required by procedure after an earthquake (prior to resuming power operation), this trip also fulfills the criteria for exemption from Regulatory Guide 1.29 (presented in FSAR section 1.8) with respect to seismic qualification of operability.

c. Source range high neutron flux trip (anticipatory) - 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 redundant protection during reactor startup and plant shutdown, can be manually bypassed when one of the two intermediate range channels reads above the P-6 setpoint value and is automatically reinstated when both intermediate range channels decrease below the P-6 setpoint value. This trip is also automatically bypassed by two out of four logic from the power range protection interlock (P-10). This trip function can also be reinstated below P-10 by an administrative action requiring manual actuation of two control board mounted switches. Each switch will reinstate the trip function in one of the two protection logic trains. The source range trip point is between the P-6 setpoint (source range cutoff power level) and the maximum source range power level. The channels can be individually bypassed at the nuclear instrumentation racks to permit channel testing during plant shutdown or prior to startup. This bypass action is annunciated on the main control board. Source range reactor 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 safety analyses (Chapter 15) for this trip. For example, while it is listed in FSAR Table 15.0.8-1 as a protective feature that is available to mitigate the

consequences of uncontrolled RCCA bank withdrawal from low power or subcritical, the discussion in FSAR section 15.4.1 explains that this event is precluded from occurring in Modes 3, 4, and 5. The analysis of uncontrolled RCCA bank withdrawal from low power or subcritical in FSAR section 15.4.1 is focused on Mode 2 initial conditions as the worst case and conservatively relies upon the power range low setpoint (alone). Source range has the same seismic qualification design basis as intermediate range (discussed above).

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 mid-power 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 DNBR as discussed in Section 15.4.3.

Figure 7.2.1-1, Sheet 3, shows the logic for all of the nuclear overpower and rate trips.

2. Core Thermal Overpower Trips - The specific trip functions generated are as follows:

   a. Overtemperature ΔT trip - This trip protects the core against low DNBR and trips the reactor on coincidence as listed in Table 7.2.1-1 with one set of temperature measurements per loop. The setpoint for this trip is continuously calculated by analog circuitry for each loop by solving the following equation:

Where:

$$\Delta T \ \frac{(1+\tau_1 S)}{(1+\tau_2 S)} \ \left[\frac{1}{(1+\tau_3 S)}\right] \ \leq \Delta T_0 \left\{K_1 - K_2 \ \frac{(1+\tau_4 S)}{(1+\tau_5 S)} \ \left[T\left[\frac{1}{(1+\tau_6 S)}\right] - T'\right] + \ K_3 \ (P - P') - f_1 \ (\Delta I)\right\}$$

Where:

ΔT = Measured ΔT by thermowell mounted RTD instrumentation;

$\frac{1+\tau_1 S}{1+\tau_2 S}$ = Lead-Lag compensator on measured ΔT ;

τ_1, τ_2 = Time constants utilized in lead-lag compensator for ΔT, τ_1 = 0 sec., τ_2 = 0 sec.;

$\frac{1}{1+\tau_3 S}$ = Lag compensator on measured ΔT ;

τ_3 = Time constants utilized in lag compensator for ΔT, τ_3 = 4 sec.;

ΔT_0 = Indicated ΔT at RATED THERMAL POWER;

K_1 = 1.185;

K_2 = 0.0224/°F;

$\frac{1+\tau_4 S}{1+\tau_5 S}$ = The function generated by the lead-lag compensator for T_{avg} dynamic compensation;

τ_4, τ_5 = Time constants utilized in the lead-lag compensator for T_{avg} , τ_4 = 22 sec., τ_5 4 sec.;

T = Average temperature, °F;

$\frac{1}{1+\tau_6 S}$ = Lag compensator on measured T_{avg} ;

τ_6 = Time constant utilized in the measured T_{avg} lag compensator, τ_6 = 0 sec.;

T' = Reference T_{avg} at RATED THERMAL POWER (≤ 588.8 °F);

K_3 = 0.0012/psig;

P = Pressurizer pressure, psig;

P' = 2235 psig (Nominal RCS operating pressure);

S = Laplace transform operator, sec.$^{-1}$;

and $f_1(\Delta I)$ is a function of the indicated difference between top and bottom detectors of the power-range neutron ion chambers; with gains to be selected based on measured instrument response during plant startup tests such that:

(1) For q_t - q_b between -21.6 percent and +12.0 percent, $f_1(\Delta I) = 0$, where q_t and q_b are percent RATED THERMAL POWER in the top and bottom halves of the core respectively, and $q_t + q_b$ is total THERMAL POWER in percent of RATED THERMAL POWER;

(2) For each percent that magnitude of q_t - q_b exceeds -21.6 percent, the ΔT Trip Setpoint shall be automatically reduced by 1.75 percent of its value at RATED THERMAL POWER; and

(3) For each percent that the magnitude of q_t - q_b exceeds +12.0 percent, the ΔT Trip Setpoint shall be automatically reduced by 1.50 percent of its value at RATED THERMAL POWER.

The channel's maximum Trip Setpoint shall not exceed its computed Trip Setpoint by more than 1.4 percent of ΔT span for ΔT input; 2.0% of ΔT span for T_{avg} INPUT; 0.4% of ΔT span for pressurizer pressure input; and 0.7% of ΔT span for ΔI input.

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

Increases in Δφ beyond a predefined deadband result in a decrease in trip setpoint. Refer to Figure 7.2.1-2.

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

Figure 7.2.1-1, Sheet 5, shows the logic for overtemperature ΔT trip function.

b. Overpower ΔT trip - This trip protects against excessive power (fuel rod rating protection) and trips the reactor on coincidence as listed in Table 7.2.1-1, with one set of temperature measurements per loop. The setpoint for each channel is continuously calculated using the following equation:

$$\Delta T \frac{(1+\tau_1 S)}{(1+\tau_2 S)} \frac{(1)}{(1+\tau_3 S)} \leq \Delta T_0 \left\{ K_4 - K_5 \frac{(\tau_7 S)}{(1+\tau_7 S)} \frac{(1)}{(1+\tau_6 S)} T - K_6 \left[T \frac{(1)}{(1+\tau_6 S)} - T'' \right] - f_2(\Delta I) \right\}$$

ΔT = As defined in Section 7.2.1.1.2.b)1),

Where

$\frac{1+\tau_1 S}{1+\tau_2 S}$ = As defined in Section 7.2.1.1.2.b)1),

τ_1, τ_2 = As defined in Section 7.2.1.1.2.b)1),

$\frac{1}{1+\tau_3 S}$ = As defined in Section 7.2.1.1.2.b)1),

τ_3 = As defined in Section 7.2.1.1.2.b)1),

ΔT_0 = As defined in Section 7.2.1.1.2.b)1),

K_4 = 1.120,

K_5 = 0.02/°F for increasing average temperature and 0 for decreasing average temperature,

$\frac{\tau_7 S}{1+\tau_7 S}$ = The function generated by the rate-lag compensator for T_{avg} dynamic compensation,

τ_7 = Time constants utilized in the rate-lag compensator for T_{avg} , τ_7= 13 sec.,

$\frac{1}{1+\tau_6 S}$ = As defined in Section 7.2.1.1.2.b)1),

τ_6 = As defined in Section 7.2.1.1.2.b)1),

K_6 = 0.002/°F for T > T" and K_6 = 0 for T ≤ T",

T = As defined in Note 1,

T" = Reference T_{avg} at RATED THERMAL POWER, ≤ 588.8°F),

S = As defined in Section 7.2.1.1.2.b)1), and

$f_2(\Delta I)$ = 0 for all ΔI .

The channel's maximum Trip Setpoint shall not exceed its computed Trip Setpoint by more than 1.4 percent of ΔT Span for ΔT input and 0.2% of ΔT span for T_{avg} input.

The source of temperature and flux information is identical to that of the overtemperature ΔT trip and the resultant ΔT setpoint is compared to the same ΔT. Figure 7.2.1-1, Sheet 5, shows the logic for this trip function.

3. Reactor Coolant System Pressurizer Pressure and Water Level Trips - The specific trip functions generated are as follows:

   a. Pressurizer low pressure trip - The purpose of this trip is to protect against low pressure which could lead to DNB. The parameter being sensed is reactor coolant pressure as measured in the pressurizer. Above P-7 the reactor is tripped when the pressurizer pressure measurements (compensated for rate of change) fall below preset limits. This trip is blocked below P-7 to permit startup. The trip logic and interlocks are given in Table 7.2.2-1.

      The trip logic is shown on Figure 7.2.1-1, Sheet 6.

   b. Pressurizer high pressure trip - The purpose of this trip is to protect the Reactor Coolant System against system overpressure.

      The same sensors and transmitters used for the pressurizer low pressure trip are used for the high pressure trip except that separate bistables are used for trip. These bistables trip when uncompensated pressurizer pressure signals exceed preset limits on coincidence as listed in Table 7.2.1-1. There are no interlocks or permissives associated with this trip function.

      The logic for this trip is shown on Figure 7.2.1-1, Sheet 6.

   c. Pressurizer high water level trip - This trip is provided as a backup to the high pressurizer pressure trip and serves to prevent water relief through the pressurizer safety valves. This trip is blocked below P-7 to permit startup. The coincidence logic and interlocks of pressurizer high water level signals are given in Table 7.2.1-1.

      The trip logic for this function is shown on Figure 7.2.1-1, Sheet 6.

4. Reactor Coolant System Low Flow Trips - These trips protect the core from DNB in the event of a loss of coolant flow situation. Figure 7.2.1-1, Sheet 5 shows the logic for these trips. The means of sensing the loss of coolant flow are as follows:

a. Low reactor coolant flow - The parameter sensed is reactor coolant flow. Three flow sensors are installed in each loop. An output signal to the reactor trip logic will be produced if two-out-of-three sensors indicate low flow in a loop. Above the P-7 setpoint a reactor trip will occur if any two loops show low flow. Above the P-8 setpoint a trip will occur if any one loop shows low flow.

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 loss of offsite power or reactor coolant pump breakers opening).

   Two undervoltage relays (one between Phases A and B and one between Phases B and C) are connected at the load side of each reactor coolant pump motor feeder breaker. Each undervoltage relay contact and its associated time delay relay circuit is connected to 125 V DC safety train A and safety train B respectively. The time delay relay contacts will provide trip inputs to the solid state protection input cabinets which trip the reactor in the event of undervoltages at two out of three reactor coolant pump motor feeders. The safety train A and safety train B time delay circuits are connected to SSP input logic train A and logic train B respectively of each solid state protection channel I, II, and III. The coincidence logic and interlocks are shown in Table 7.2.1 1. The time delay relay coil-to-contact isolation combined with each input cable being in its dedicated conduit provide adequate electrical separation between safety train A and solid state protection channel II and between safety train B and solid state protection channels I and III.

c. Reactor coolant pump underfrequency trip - This trip protects against low flow resulting from pump underfrequency, for example a major power grid frequency disturbance. The function of this trip is to trip the reactor for an underfrequency condition greater than approximately 5 Hz/second. The setpoint of the underfrequency relays is adjustable between 54 and 59 Hz.

   Two underfrequency relays (one between Phases A and B and one between Phases B and C) are connected at the load side of each reactor coolant pump motor feeder breaker. Each underfrequency relay contact and its associated time delay relay circuit is connected to 125 V DC safety train A and safety train B respectively. The time delay relay contacts will provide trip inputs to the solid state protection input cabinets which trip the reactor in the event of underfrequencies at two out of three reactor coolant pump motor feeders. The safety train A and safety train B time delay circuits are connected to SSP input logic train A and logic Train B respectively of each solid state protection channel I, II, and III. The coincidence logic and interlocks are shown in Table 7.2.1-1. The time delay relay coil-to-contact isolation combined with each input cable being in its dedicated conduit provide adequate electrical separation between safety train A and solid state protection channel II and between safety train B and solid state protection channels I and III.

5. Steam Generator Trips - The specific trip functions generated are as follows:

   a. Low feedwater flow trip - This trip protects the reactor from a sudden loss of heat sink. The trip is actuated by steam/feedwater flow mismatch (one out of two) in coincidence with low water level (one out of two) in any steam generator.

Low feedwater flow is a non-primary input to the Solid State Protection System; therefore, the input is considered an anticipatory trip and the flow elements associated with it are non-nuclear safety, located in non-seismic Category I piping within the seismically designed Turbine Building. The flow elements and their associated flow transmitters are shown in Figure 10.1.0 3. The flow transmitters are Class 1E located in non-nuclear safety grade instrument cabinets in the seismically designed Non-Class I Turbine Building. The instrument sensing lines are supported in a manner consistent with site seismic supports and independently routed in accordance with the separation criteria specified in IEEE-279-1971.

The low feedwater flow input signal functioning is unrelated to a seismic event in that they are anticipatory to other diverse parameters which cause reactor trip. The low feedwater flow signal is fail safe in that it serves to interrupt power (de-energize-to-trip) to cause reactor trip. The SSPS cabinets which receive the input signals from the low feedwater flow instrument cabinets (anticipatory trip sensors) are seismically qualified. The primary trip that protects the reactor from a loss of heat sink is the low-low steam generator water level trip. The low feedwater flow trip along with other trips that are not required because the trips are not assumed to function in an accident and therefore no credit is taken for them in the accident analysis are listed in Table 7.2.2-1.

Figure 7.2.1-1, Sheet 7, shows the logic for this trip function.

There are no interlocks associated with this trip.

b. Low-low steam generator water level trip - This trip protects the reactor from loss of heat sink in the event of a sustained steam/feedwater flow mismatch of insufficient magnitude to cause a low feedwater flow reactor trip. This trip is actuated on two out of three low-low water level signals occurring in any steam generator.

   The logic is shown on Figure 7.2.1-1, Sheet 7.

6. Reactor Trip on a Turbine Trip (anticipatory) - The reactor trip on a turbine trip is actuated by two out of three logic from trip fluid pressure signals or by all closed signals from the turbine steam stop valves. A turbine trip causes a direct reactor trip above P-7. 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 safety analyses (Chapter 15) for this trip.

   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 emergency trip fluid pressure goes below its setpoint. The logic for this trip is shown in Figure 7.2.1-1, Sheet 15.

   The turbine trip system employs the two channel concept with redundant inputs from each critical parameter. All local trips and remote trips activate both turbine trip channels through four solenoid valves. The four valves are arranged in a series/parallel configuration separating into two channels so that at least one solenoid valve from each channel must be open to cause a trip.

Separate Reactor Trip contacts (two train "A" and two train "B") are wired out to each of the four turbine trip solenoids. Reactor trip contacts from either train (A or B) will trip the turbine.

One of the design bases considered in the protection system is the possibility of an earthquake. With respect to these contacts, their functioning is unrelated to a seismic event in that they are anticipatory to other diverse parameters which cause reactor trip. The contacts are shut during plant operation and open to cause reactor trip when the turbine is tripped. No power is provided to the protection system from the contacts; they merely serve to interrupt power to cause reactor trip. This design functions in a de-energize-to-trip fashion to cause a plant trip if power is interrupted in the trip circuitry. This ensures that the protection system will in no way be degraded by this anticipatory trip because seismic design 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 redundancy, separation, and single failure criteria of IEEE Standard 279-1971. The circuit routing is discussed in Section 8.3.1.2.30. Seismic qualification of the contact sensors is not required.

Circuit analyses have shown that the functional performance of the protection system would not be degraded by credible faults in circuits associated with reactor trip from turbine trip. Contacts of sensors on steam stop valves and trip fluid pressure system are closed during operation to complete the AC supply through the Solid State Protection System input relays. Open circuit or short circuit faults would trip the channel to produce a partial reactor trip.

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 steam.

   Figure 7.2.1-1, Sheet 8, shows the logic for this trip.

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 trip breaker and the train B bypass breaker; the other output actuates the train B trip breaker and the train A bypass 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 7.2.1-1, Sheet 3, shows the manual trip logic. The design conforms to Regulatory Guide 1.62 as shown in Figure 7.2.1-3.

9. General Warning Alarm Reactor Trip - Each of the two trains of the Solid State Protection System is continuously monitored by the General Warning Alarm subsystem. The warning circuits are actuated if undesirable train conditions are set up by improper alignment of train testing systems circuit malfunction or failure, etc., as listed below. A trouble condition in a train is indicated in the control room. However, if any one of the conditions exists in Train A at the same time any one of the conditions exists in Train B, the reactor will be automatically tripped by the General Warning Alarm Reactor Trip system. Potential trouble conditions monitored are:

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

b. Printed circuit card improperly inserted.

c. Input Error Inhibit switch in the INHIBIT position.

d. Output Relay Mode Selector in TEST position.

e. Multiplexing selector switch in INHIBIT position.

f. Train bypass breaker racked in and closed.

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

h. Logic Function test switch not in OFF position.

i. Loss of AC power in the relay cabinets.

j. Master Relay Selector in TEST position.

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 discrete, but overlapping, ranges. Continuation of startup operation or power increase requires a permissive signal from the higher range instrumentation channels before the lower range level trips can be manually blocked by the operator.

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

   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 the permissive (P-10) setpoint, thus ensuring automatic activation to more restrictive trip protection.

   The development of permissives P-6 and P-10 is shown on Figure 7.2.1-1, Sheet 4. All of the permissives are digital; they are derived from analog signals in the nuclear power range and intermediate range channels.

   See Table 7.2.1-2 for the list of protection system interlocks.

2. Blocks of Reactor Trips at Low Power - Interlock P-7 blocks a reactor trip at low power (below approximately 10 percent of full power) on a low reactor coolant flow in more than one loop, reactor coolant pump undervoltage, reactor coolant pump underfrequency, pressurizer low pressure, pressurizer high water level or turbine trip signal. See Figure 7.2.1-1, Sheets 5, 6 and 15, 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 first stage pressure signals below the setpoint (low plant load). See Figure 7.2.1-1, Sheets 4 and 15, for the derivation of P-7.

   The P-8 interlock blocks a reactor trip when the plant is below approximately 50 percent 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 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 7.2.1-1, Sheet 4, for derivation of P-8, and Sheet 5 for applicable logic.

   See Table 7.2.1-2 for the list of protection system blocks.

7.2.1.1.4 Coolant temperature sensor arrangement

The hot and cold leg resistance temperature detectors are inserted into the reactor coolant loop thermowells. The thermowell arrangement permits replacement of defective temperature elements while the plant is at hot shutdown without draining or depressurizing the reactor coolant loops.

Three thermowells with dual element RTDs are installed in sampling scoops in a cross sectional plane of each hot leg at approximately 120° intervals. The sampling scoops were originally part of a bypass manifold arrangement, but were later converted to hold thermowells. Each of the sampling scoops, which extend several inches into the hot leg coolant stream, contain 5 inlet orifices distributed along its length and one exit orifice at the tip. The thermowell extends down to the third inlet orifice.

The measurements from the 3 RTDs are averaged to develop a T_{HOT} reading for the loop. This is necessary since temperature layers in the hot leg result in slightly different measurements at each RTD.

The cold leg reactor coolant flow is well mixed by the reactor coolant pump thereby eliminating any cold leg temperature spatial dependence. Therefore, there is only one thermowell located on the cold leg downstream of the pump. There are no sampling scoops on the cold leg. The thermowell extends about 3.5 inches into the flow stream.

7.2.1.1.5 Pressurizer water level reference leg arrangement

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

7.2.1.1.6 Analog system

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

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

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

Various types of neutron detectors, with appropriate solid-state electronic circuitry, are used to monitor the leakage neutron flux from a completely shutdown condition to 120 percent of full power. The power range channels are capable of recording (via ERFIS) overpower excursions up to 200 percent of full power. The neutron flux covers a wide range between these extremes. Therefore, monitoring with several ranges of instrumentation is necessary. The lowest range ("source" range) covers six decades of leakage neutron flux. The lowest observed count rate depends on the strength of the neutron sources in the core and the core multiplication associated with the shutdown reactivity. This is generally greater than two counts per seconds. The next range ("intermediate" range) covers eight decades. Detectors and instrumentation are chosen to provide overlap between the higher portion of the source range and the lower portion of the intermediate range. The highest range of instrumentation ("power" range) covers approximately two decades of the total instrumentation range. This is a linear range that overlaps with the higher portion of the intermediate range.

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

See References 7.2.1-1 and 7.2.1-2 for additional background information on the Process and Nuclear Instrumentation Systems.

7.2.1.1.7 Solid-state logic protection system

The solid-state logic protection system takes binary inputs (voltage/no voltage) from the process and nuclear instrument channels corresponding to conditions (normal/abnormal) of plant parameters. The system combines these signals in the required logic combination and generates a trip signal (no voltage) to the undervoltage trip attachment and shunt trip auxiliary relay coils of the reactor trip circuit breakers when the necessary combination of signals occur. The system also provides annunciator, status light and computer input signals which indicate the condition of bistable input signals, partial trip and full trip functions and the status of the various blocking, permissive and actuation functions. In addition the system includes means for semi-automatic testing of the logic circuits. Refer to Reference 7.2.1-3 for background information.

7.2.1.1.8 Isolation amplifiers

Control signals are derived from individual protection channels through isolation amplifiers contained in the protection channel, as permitted by IEEE Standard 279-1971.

Analog signals derived from protection channels for nonprotective functions are obtained through isolation amplifiers located in the analog protection racks. By definition, nonprotective functions include those signals used for control, remote process indication, and computer monitoring. Refer to Section 7.1.2.2.1 for further discussions on isolation.

For a discussion of digital non-class 1E to Class 1E inputs, refer to Section 7.3.2.2.6.

7.2.1.1.9 Energy supply and environmental variations

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

7.2.1.1.10 Setpoints

The setpoints that require trip action are given in the Technical Specifications. A detailed discussion on setpoints is found in Section 7.2.1.2.4 and 7.2.2.2.1.

7.2.1.1.11 Seismic Design

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

7.2.1.2 Design Basis Information

The information given below presents the design basis information requested by Section 3 of IEEE Standard 279-1971. Functional logic diagrams are presented in Figure 7.2.1-1, Sheets 1 through 15.

7.2.1.2.1 Generating Station Conditions

The following are the generating station conditions requiring reactor trip:

1. DNBR approaching safety analysis limit (See Section 4.4.2 for DNBR limits)

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

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

7.2.1.2.2 Generating Station Variables

The following are the variables required to be monitored in order to provide reactor trips (see Table 7.2.1-1).

1. Neutron flux.

2. Reactor coolant temperature.

3. Reactor coolant system pressure (pressurizer pressure).

4. Pressurizer water level.

5. Reactor coolant flow.

6. Reactor coolant pump operational status (voltage and frequency).

7. Steam generator feedwater flow.

8. Steam generator water level.

9. Turbine generator operational status (trip fluid pressure and stop valve pressure).

10. Steam flow.

7.2.1.2.3 Spatially dependent variables

The following variable is spatially dependent:

a) Reactor coolant temperature (see Section 7.2.1.1.4 for a discussion of this variable spatial dependence).

7.2.1.2.4 Limits, margins and setpoints

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 accident analyses, described in Chapter 15 demonstrate that the functional requirements as specified for the Reactor Trip System are adequate, even assuming, for conservatism, adverse combinations of instrument errors (refer to Table 15.0.6-2). 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. Refer to Reference 7.2.1-4, 7.2.1-5, 7.2.1-6, and 7.2.1-7 for setpoint methodology for RPS and Engineering Safety Features System.

7.2.1.2.5 Abnormal events

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

a) Earthquakes (see Chapters 2 and 3).

b) Fire (see Section 9.5).

c) Missiles (See Section 3.5)

d) Flood (see Chapters 2 and 3)

e) 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.

7.2.1.2.6 Minimum performance requirements

a) Reactor Trip System response times - Reactor Trip System response time is defined in Section 7.1. Maximum allowable time delays in generating the reactor trip signal are provided in Technical Specifications based upon analysis assumptions. Table 15.0.6-2 provides response times assumed in accident analyses for Reactor Trip System response times. (See Section 7.1.2.18 for a discussion of periodic response time verification capabilities.)

b) Reactor Trip Accuracies - The Reactor Trip System instrumentation trip setpoints along with the corresponding "Allowable" and "Total Allowance" values are specified in Technical Specifications Table 2.2-1. Calculations of record for these Limiting Safety System settings have been prepared in accordance with the company methodology procedure for instrument loop uncertainty analysis and setpoint determination. Protection channel setpoints have been examined to ensure that the calculated total loop uncertainties are bounded by the "Total Allowance" values presented in Technical Specifications. In addition, the NIS Power Range and pressurizer level high channels require As-Found/As-Left tolerances around the actual device in the field setting as specified in PLP-106, Attachment 11, to comply with the TSTF-493 requirements.

7.2.1.3 Final Systems Drawing

Functional block diagrams and control wiring diagrams are provided in Figure 7.2.1-1 and Drawing CAR-2166-B-401.

7.2.2 ANALYSES

7.2.2.1 Failure Mode and Effects Analyses

An analysis of the Reactor Trip System has been performed. Results of this study and a fault tree analysis are presented in Reference 7.2.2 1.

7.2.2.2 Evaluation of Design Limits

While most setpoints used in the Reactor Protection System are fixed, there are variable setpoints, most notably the overtemperature ΔT and overpower ΔT setpoints. All setpoints in the Reactor Trip Systems 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 RCS pressure boundary during ANS 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 analysis (where appropriate) which utilizes this trip is presented below. It should be noted that the selected trip setpoints all provide for margin before protection action is actually required to allow for uncertainties and instrument errors.

Each of the reactor trip system instrumentation and ESF system setpoints (and their allowable tolerances of these setpoints) is determined by the evaluation of the system design calculations. This evaluation establishes the allowable system tolerance of a setpoint which will still result in the ESF system performing its intended function and within the limits of acceptable system performance. The capabilities of the instrument or instrument loop are then evaluated against the allowable system tolerance to ensure that the control system performance will comply with system requirements. The overall instrument or instrument loop accuracies take into account a) instrument accuracy under accident environment b) calibration uncertainty c) setpoint drift. The calculated instrument loop uncertainty is the square root of the sum of the squares of individual instruments uncertainties comprising that loop.

The design meets the requirements of GDC 10 and 20.

7.2.2.2.1 Trip Setpoint Discussion

The accident analysis shows that for a DNBR below the safety analysis limit, a potential for local fuel cladding failure exists. The DNBR existing at any point in the core for a given core design can be determined as a function of the core inlet temperature, power output, operating pressure and flow. Consequently, core safety limits in terms of a DNBR limit for the hot channel can be developed as a function of core ΔT, T_{avg} and pressure for a specified flow. Actual setpoint constants in the equation for this relationship are as given in the Technical Specifications. These values are conservative to allow for instrument errors. The design meets the requirements of GDC 10, 15, 20 and 29.

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 ANS Condition II and III accidents. This is demonstrated by Technical Specifications (with the associated basis statements) and the accident analysis presented in Chapter 15, Table 15.0.6-2 compares the trip setpoints used in the accident analyses to corresponding values in the Technical Specifications. Table 15.0.8-1 correlates reactor trip functions to applicable incidents presented throughout Chapter 15. In addition, the detailed discussion of accidents within each section of Chapter 15 normally includes a discussion of applicable reactor trip functions.

It should be noted that the Reactor Trip System automatically provides core protection during nonstandard operating configuration, i.e., operation with a loop out of service. Although operating with a loop out of service over an extended time is considered to be an unlikely event, no protection system setpoints need to be reset. This is because the nominal value of the power (P-8) interlock setpoint restricts the power such that DNB ratios less than the safety analysis limit will not be realized during any ANS Condition II transients occurring during this mode of operation. This restricted power is considerable below the boundary of permissible values as defined by the core safety limits for operation with a loop out of service. Thus, the P-8 interlock acts essentially as a high nuclear power reactor trip when operating with one loop not in service. By first resetting the coefficient setpoints in the overtemperature ΔT function to more restrictive values as listed in the Technical Specifications, the P-8 setpoint can then be increased to the maximum value consistent with maintaining DNBR above the safety analysis limit for ANS Condition II transients in the one loop shutdown mode. The resetting of the ΔT overtemperature trip and P-8 will be carried out under prescribed administrative procedures, under the direction of authorized supervision, and with the plant conditions prescribed in the Technical Specifications. The design meets the requirements of GDC 21.

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

Analyses of the results of ANS Condition I, II, III and IV events, including considerations of instrumentation installed to mitigate their consequences are presented in Chapter 15. The instrumentation installed to mitigate the consequences of load rejection and turbine trip is given in Section 7.7.

7.2.2.2.2 Reactor Coolant Flow Measurement

The elbow taps used on each loop in the Reactor Coolant System are instrument devices that indicate the status of the reactor coolant flow. The basic function of this device is to provide information as to whether or not a reduction in flow has occurred. The correlation between flow and elbow tap signal is given by the following equation:

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

where ΔP_0 is the pressure differential at the reference flow, w_0, 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 ± 10 percent of full flow and field results have shown the repeatability of the trip point to be with ± 1 percent.

7.2.2.2.3 Evaluation of Compliance to Applicable Codes and Standards

The Reactor Trip System meets the criteria of the general design criteria as indicated. The Reactor Trip System meets the requirements of Section 4 of IEEE Standard 279-1971 as indicated below.

7.2.2.2.3.1 General Functional Requirement

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

7.2.2.2.3.2 Single Failure Criterion

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

7.2.2.2.3.3 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 GDC 1.

7.2.2.2.3.4 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 GDC 4.

7.2.2.2.3.5 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 Section 7.6 and Chapter 8. The environmental variations, throughout which the system will perform is given in Section 3.11.

7.2.2.2.3.6 Independence

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

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 7.1.1-1).

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

7.2.2.2.3.7 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 amplifiers. The isolation amplifiers are classified as part of the protection system and are located in the analog protective racks. Non-protective functions include those signals used for control, remote process indication, and computer monitoring. The isolation amplifiers are designed such that a short circuit, open circuit, or the application of credible fault voltages from within the cabinets on the isolated output portion of the circuit (i.e., the non-protective side of the circuit) will not affect the input (protective) side of the circuit. The signals obtained through the isolation amplifiers are never returned to the protective racks. This design meets the requirements of GDC 24 and paragraph 4.7 of IEEE Standard 279-1971. Refer to Section 7.1.2.2.1 for further discussion of isolation and separation of control and protection.

7.2.2.2.3.8 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.

7.2.2.2.3.9 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 readouts available. Channel checks are discussed in Technical Specifications.

7.2.2.2.3.10 Capability for Testing

The Reactor Trip System is capable of being tested during power operation. Where only parts of the system are tested at any one time, the testing sequence provides the necessary overlap between the parts to assure complete system operation. The testing capabilities are in conformance with Regulatory Guide 1.22 as discussed in Section 7.1.2.5.

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

a) Analog Channel Tests- Analog channel testing is performed at the analog instrumentation rack set by individually introducing dummy input signals into the instrumentation channels and observing the tripping of the appropriate output bistable. Process analog output to the logic circuitry is interrupted during individual channel test by a test switch which, when thrown, de-energizes the associated logic input and inserts a proving lamp in the bistable output. Interruption of the bistable output to the logic circuitry for any cause (test, maintenance purposes, or removed from service) will cause that portion of the logic to be actuated (partial trip) accompanied by a partial trip alarm and channel status light actuation in the control room. Each channel contains those switches, test points, etc., necessary to test the channel. See Reference 7.2.1-1 for additional background information.

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

   1) T_{avg} and ΔT protection channel testing.

   2) Pressurizer pressure protection channel testing.

   3) Pressurizer water level protection channel testing.

   4) Steam/feedwater flow protection channel testing.

   5) Steam generator water level protection channel testing.

   6) Reactor coolant low flow, pump underfrequency, and pump undervoltage protection channels.

   7) Turbine first stage pressure channel testing.

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

   To test a power range channel, a "TEST-OPERATE" switch is provided to require deliberate operator action and operation of which will initiate the "CHANNEL TEST" annunciator in the Control Room. Bistable operation is tested by increasing the test signal to its trip setpoint and verifying bistable relay operation by control board annunciator and trip status lights.

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

   Certain tests which require interrupting or lowering the detector signals will place channel output trips and permissives in a conservative state with respect to plant status by removing the control power fuses or by lifting leads or cable connector.

   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 a plant shutdown

   1) Source range testing.

   2) Intermediate range testing.

   3) Power range testing.

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

   1) Source range testing.

   2) Power range testing.

c) Testing above P-10 permissive power level

   1) Power range testing.

Any deviations noted during the performance of these tests are investigated and corrected in accordance with the established calibration and troubleshooting procedures provided in the plant technical manual for the Nuclear Instrumentation System. Control and protection trip settings are indicated in the setpoint document.

For additional background information on the Nuclear Instrumentation System, see Reference 7.2.1-2.

c) Solid-State Logic Testing - The reactor logic trains of the Reactor Trip System are designed to be capable of complete testing at power. After the individual channel analog testing is complete, the logic matrices are tested from the train A and train B logic rack test panels. This step provides overlap between the analog and logic portions of the test program. During this test, all of the logic inputs are actuated semi-automatically in all combinations of trip and nontrip logic. Trip logic is not maintained sufficiently long enough to permit opening of the reactor trip breakers. The reactor trip undervoltage coils are "pulsed" in order to check continuity. During logic testing of one train, the other train can initiate any required protective functions. Annunciation is provided in the Control Room to indicate when a train is in test (train output bypassed) and when a reactor trip breaker is bypassed. Logic testing can be performed in less than 30 minutes.

A direct reactor trip resulting from undervoltage or underfrequency on the reactor coolant pump buses is provided as discussed in Section 7.2.1 and shown on Figure 7.2.1-1, sheets 2 and 5. 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, discussed in Section 7.1.2.18.

The permissive and block interlocks associated with the Reactor Trip System and Engineered Safety Features Actuation System are given on Tables 7.2.1-2 and 7.3.1-4, respectively 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.

Testing of all protection system interlocks is provided by the logic testing and semi-automatic testing capabilities of the solid-state protection system. In the solid-state protection system the undervoltage trip attachment and shunt trip auxiliary relay coils (reactor trip) and master relays (engineered safeguards actuation) are pulsed for all combinations of trip or actuation logic with and without the interlock signals. For example, reactor trip on low flow (2 out of 3 loops showing 2 out of 3 low flow) is tested to verify operability of the trip above P-7 and nontrip below P-7 (see Figure 7.2.1-1 Sheet 5). Interlock testing may be performed at power.

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

1) Check of input relays - During testing of the Process Instrumentation System and Nuclear Instrumentation System Channels, each channel bistable is placed in a trip mode causing one input relay in train A and one in train B to de-energize. A contact of each relay is connected to a universal logic printed circuit card. This card performs both the reactor trip and monitoring functions. Reactor trip inputs cause status lamps and annunciators in the main control board to operate as shown in Figure 7.2.1-1. Either the train A or train B input relay operation will light the status lamp and annunciator.

Each train contains a multiplexing test switch. This switch (in either train) will be maintained in the A + B position while performing process or nuclear instrumentation system testing. The train whose switch is maintained in the A + B position will be alternated on a monthly basis following Reactor Protection System Actuation Logic and Relay Testing. The A + B position alternately allows information to be transmitted from the two trains to the main control board. A steady status lamp and annunciator indicates that input relays in both trains have been de-energized. A flashing lamp means that the input relays in the two trains did not both de-energize. Contact inputs to the logic protection system such as reactor coolant pump bus underfrequency relays operate input relays which are tested by operating the remote contacts as described above and using the same type of indications as those provided for bistable input relays.

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

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

   The logic test scheme uses pulse techniques to check the coincidence logic. All possible trip and nontrip combinations are checked. Pulses from the tester are applied to the inputs of the universal logic card at the same terminals that connect to the input relay contacts. Thus, there is an overlap between the input relay check and the logic matrix check. Pulses are fed back from the reactor trip breaker undervoltage trip attachment and shunt trip auxiliary relay 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.

d) Testing of Reactor Trip Breakers - Normally, reactor trip breakers 52/RTA and 52/RTB (see Figure 7.2.1-1, Sheet 2) are in service, and bypass breakers 52/BYA and 52/BYB are withdrawn (out of service). In testing the protection logic, pulse techniques are used to avoid tripping the reactor trip breakers thereby eliminating the need to bypass them during this testing. The following procedure describes the method used for testing the trip breakers:

   1) With bypass breaker 52/BYA racked out to the test position, close and trip it via the local pushbuttons to verify its operation.

2) Rack in and close 52/BYA. Manually trip 52/RTA through a protection system logic matrix while at the same time operating the "Auto Shunt Trip Block" pushbutton on the automatic shunt trip panel. This verifies operation of the Undervoltage Trip Attachment (UVTA) when the breaker trips. After reclosing RTA, trip it again by operation of the "Auto Shunt Trip Test" pushbutton on the automatic shunt trip panel. This is to verify tripping of the breaker through the shunt trip device.

3) Reset 52/RTA.

4) Trip and rack out 52/BYA.

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

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

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

The train A and 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 test procedures used to determine reactor trip breaker operability include verification of the proper operation of the associated control room indication.

e) Testing of Reactor Trip Bypass Breakers - The purpose of the bypass breaker is to allow online testing of the main reactor trip breaker. This short period is the only time a bypass breaker may be called upon to provide a protective function. Additionally, protection is still considered to be provided by the opposite train main reactor trip breaker. Considering the relatively low occurrence of a combined event (one main reactor trip breaker in test, opposite main reactor trip breaker failure, and the requirement for a reactor trip), frequent testing of each bypass breaker is not warranted. Therefore, Shearon Harris does not propose to verify the operability of each bypass breaker undervoltage trip attachment prior to placing it in service each time the main reactor trip breakers are to be tested. However, they will be tested prior to startup after each refueling outage.

f) Testing of Control Board Manual Switch - The operability of the control room manual reactor trip switch contacts and wiring will be adequately tested prior to startup after each refueling outage. The test procedure will not involve installing jumpers, lifting leads, or pulling fuses for verifying the manual reactor trip functions.

The complete Reactor Trip System is normally required to be in service. However, to permit online testing of the various protection channels or to permit continued operation in the event of a subsystem instrumentation channel failure, a Technical Specification defining the minimum number of operable channels has been formulated. This Technical Specification also defines the required restriction to operation in the event that the channel operability requirements cannot be met. The Technical Specifications require periodic testing of the undervoltage and shunt trip functions and manual reactor trip switch contacts and wiring.

7.2.2.2.3.11 Channel bypass or removal from operation

The protection system is designed to permit periodic testing of the analog channel portion of the Reactor Trip System during reactor power operation without initiating a protective action unless a trip condition actually exists. This is because of the coincidence logic required for reactor trip. Additional information is given in Section 7.2.2.2.3.10.

7.2.2.2.3.12 Operating bypasses

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

7.2.2.2.3.13 Indication of Bypasses

Bypass indication is discussed in Section 7.3.2.2.13.

7.2.2.2.3.14 Access to Means for Bypassing

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

7.2.2.2.3.15 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 setting are considered part of the protective system and are designed in accordance with the criteria of this section.

7.2.2.2.3.16 Completion of Protective Action

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

7.2.2.2.3.17 Manual Initiation

Switches are provided on the main 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.

7.2.2.2.3.18 Access

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

7.2.2.2.3.19 Identification of Protective Actions

Protective channel identification is discussed in Section 7.1.2.3. Indication is discussed in Section 7.2.2.2.3.20.

7.2.2.2.3.20 Information and Read Out

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

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

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

7.2.2.2.3.21 System Repair

The system is designed to facilitate the recognition, location, replacement, and repair of malfunctioning components or modules. Refer to the discussion in Section 7.2.2.2.3.10.

7.2.2.3 Specific Control and Protection Interactions

7.2.2.3.1 Neutron Flux

Four power range neutron flux channels are provided for overpower protection. If any channel fails in such a way as to produce a low output, that channel is incapable of proper overpower protection. The reference power signal to automatic rod control is supplied as a "high select" of the four flux channels, and if one channel fails high, it could cause rod movement. Two out of four overpower trip logic will ensure an overpower trip if needed even with an independent failure in another channel.

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

7.2.2.3.2 Coolant temperature

The accuracy of the Reactor Coolant System (RCS) primary resistance temperature detectors (RTD) is demonstrated during plant startup. Tests compare the RCS RTDs with one another. The comparisons are done with the Reactor Coolant System in an isothermal condition. The linearity of the ΔT measurements obtained from the hot leg and cold leg loop resistance temperature detectors as a function of plant power is also checked during plant startup tests.

The absolute value of ΔT versus plant power is not important, per se, as far as reactor protection is concerned. Reactor Trip System setpoints are based upon percentages of the indicated ΔT at nominal full power rather than on absolute values of ΔT. This is done to account for loop differences which are inherent. Therefore, the percent ΔT scheme is relative, not absolute, and therefore provides better protective action without the expense of accuracy. For this reason, the linearity of the ΔT signals as a function of power is of importance rather than the absolute values of the ΔT. As part of the plant startup tests, the loop 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 amplifiers such that no feedback effect can perturb the protection channels.

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

7.2.2.3.3 Pressurizer pressure

The pressurizer pressure protection channel signals are used for high and low pressure protection and as inputs to the overtemperature ΔT trip protection function. Pressurizer pressure is sensed by fast response pressure transmitters. Control signals are not derived from protection channels.

A spurious high pressure signal from one control channel can cause decreasing pressure by actuation of either spray or relief valves. Protection is provided in the low pressurizer pressure reactor trip and in the logic for safety injection to ensure low pressure protection.

Overpressure protection is based upon the positive surge of the reactor coolant produced as a result of turbine trip under full load, assuming the core continues to produce full power. The self-actuated safety valves are sized on the basis of steam flow from the pressurizer to accommodate this surge at a setpoint of 2500 psia and an accumulation of 3 percent.

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.

One tap on the pressurizer is shared for one each protection level and pressure transmitter, two control pressure transmitters and one wide range level transmitter. Redundancy is not compromised by having a shared tap since the logic for this trip is two out of three. If the shared tap is plugged, the affected channels will remain static. If the impulse line bursts, the indicated pressure will drop to zero. In either case the fault is easily detectable, and the protective function remains operable.

7.2.2.3.4 Pressurizer water level

Three pressurizer water level channels are used for reactor trip. Isolated signals from these channels are used for pressurizer water level control. A failure in the level control system could fill or empty the pressurizer at a slow rate (on the order of half an hour or more).

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

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

7.2.2.3.5 Steam generator water level and feedwater flow

The basic function of the reactor protection circuits associated with low steam generator water level and low feedwater flow 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 coincidence of steam/feedwater flow mismatch and low steam generator water level or 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. These reactor trips act 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, the following reactor trip circuits are provided for each steam generator to ensure that sufficient initial thermal capacity is available in the steam generator at the start of the transient:

1. A mismatch in steam and feedwater flow coincident with low steam generator water level;

2. A low-low steam generator water level regardless of steam/feedwater flow mismatch.

It is desirable to minimize thermal transients on a steam generator for credible loss of feedwater accidents. Hence, it should be noted that controlled malfunctions caused by a protection system failure affect only one steam generator; the steam generator level signal used in the feedwater control originates separately from that used in the low feedwater reactor trip. The steam generator reference legs are insulated to avoid the heat up concerns resulting from the effects of high temperature in the steam generator water level measurement reference legs after a high energy line break.

A spurious high signal from the feedwater flow channel being used for control would cause a reduction in feedwater flow preventing that channel from ultimately tripping. However, the mismatch between steam demand and feedwater flow produced by this spurious signal will actuate alarms to alert the operator of this situation in time for manual correction. If the condition is allowed to continue and the mismatch is not sufficient to trip the reactor, reactor trip will occur on a low-low water level signal independent of indicated flow.

A spurious low signal from the feedwater flow channel being used for control would cause an increase in feedwater flow. The mismatch between steam flow and feedwater flow produced by the spurious signal would actuate alarms to alert the operator of the situation in time for manual

correction. If the condition continues, a two out of four high-high steam generator water level signal in any loop, independent of the indicated feedwater flow, will cause feedwater isolation and trip the turbine. The turbine trip will result in a subsequent reactor trip if power is above the P-7 setpoint. The high-high steam generator water level trip is an equipment protective trip preventing excessive moisture carryover which could damage the turbine blades.

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

Protection from a control system action due to the failure of a steam generator water level or steam flow impulse line is provided by ensuring that common upper taps are only shared by the same channel instruments. A spurious high steam generator water level signal from the protection channel used for control will tend to close the feedwater valve. However, before a reactor trip would occur, two out of four channels for a steam generator would have to indicate a high water level. A spurious low steam generator water level signal will tend to open the feedwater valve. Again, before a reactor trip would occur, two out of three channels in a loop would have to indicate a low water level. Any slow drift in the water level signal will permit the operator to respond to the level alarms and take corrective action. Automatic protection is also provided in case the spurious low level signal increases feedwater flow sufficiently to cause high level in the steam generator. A turbine trip and feedwater isolation would occur on two out of four high-high steam generator water level in any loop.

7.2.2.4 Additional Postulated Accidents

Loss of plant instrument air or loss of component cooling water is discussed in Sections 9.3.1.3 and 9.2.2 respectively. Load rejection and turbine trip are discussed in further detail in Section 7.7.

The control interlocks, called rod stops, which are provided to prevent abnormal power conditions which could result from excessive control rod withdrawal are discussed in Section 7.7.1.4 and listed on Table 7.7.1-1. 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 Chapter 16) being reached. Before such a limit is reached, protection will be available from the Reactor Trip System. At the power levels of the rod block setpoints, safety limits have not been reached; and, therefore, these rod withdrawal stops do not come under the scope of safety-related 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 discussed in Sections 7.2.2.2.3.10 and 7.1.2.18. The testability of the system is discussed in Section 7.2.2.2.3. The initial test intervals are specified in Chapter 16. Written test procedures and documentation, conforming to the requirements of IEEE Standard 338-1971, will be available for audit by responsible personnel. Periodic testing complies with Regulatory Guide 1.22 as discussed in Sections 7.1.2.5 and 7.2.2.2.3. Response time testing will contain the criteria listed in Section 14.2.12.1.11.

REFERENCES: SECTION 7.2

7.2.1-1 Reid, J. B., "Process Instrumentation for Westinghouse Nuclear Steam Supply Systems," WCAP-7913, January, 1973.

7.2.1-2 Lipchak, J. B., "Nuclear Instrumentation System," WCAP-8255, January, 1974.

7.2.1-3 Katz, D. N., "Solid State Logic Protection System Description," WCAP-7488-L (Proprietary), March, 1971 and WCAP-7672 (Non-Proprietary), May, 1971.

7.2.1-4 Westinghouse Instrument Setpoints, 1364-53067 (historical reference for current Technical Specification operability determination basis).

7.2.1-5 Precautions, Limitation and Setpoints for Nuclear Steam Supply Systems, 1364-53872.

7.2.1-6 Calculation HNP-I/INST-1010, "Evaluation of Tech Spec Related Setpoints, Allowable Values, and Uncertainties Associated With RTS/ESFAS Functions for Steam Generator Replacement (with current 2787 MWT-NSSS Power or Uprate to 2912.4 MWT-NSSS Power)".

7.2.1-7 PLP-106, Technical Specification Equipment List Program and Core Operating Limits Report.

7.2.2-1 Gangloff, W. C. and Loftus, W. D., "An Evaluation of Solid-State Logic Reactor Protection in Anticipated Transients," WCAP-7706-L (Proprietary) and WCAP-7706 (Non-Proprietary), February, 1973.

7.3 ENGINEERED SAFETY FEATURES SYSTEM

The engineered safety features instrumentation measures temperatures, pressures, flows and levels in the Reactor Coolant System, steam and power conversion systems, Containment and auxiliary systems, and actuates and monitors the operation of the engineered safety features equipment. Process variables necessary on a continuous basis for the start-up, operation, and shutdown of the Engineered Safety Features System are controlled, indicated, and/or recorded from the Control Room as required. The quantities and types of process instrumentation provided ensure safe and orderly operation of all systems and processes over the full operating range of the plant.

The Engineered Safety Features (ESF) System directs various ESF equipment to take protective action to mitigate the consequences of a loss-of-coolant accident (LOCA) secondary system rupture, or fuel handling accident. ESF and Support Systems are listed in Table 7.3.1-1, with the organizational responsibility for mechanical design identified. The sensors, analog circuitry, and actuation logic for each ESF system are supplied by Westinghouse Electric Corporation (Westinghouse) with the exception of those for the Fuel Handling Building (FHB) Exhaust System and Combustible Gas Control System, which are furnished by Ebasco. The containment and control room radiation monitors and their logics are also furnished by Ebasco. Ebasco furnishes all final actuation control equipment, including control switches, indicating lights, breakers, and motor controllers. The interfaces between the Westinghouse actuation signals and actuated equipment furnished by Ebasco are shown on Figure 7.3.1-1.

Certain controls and indicators which require a minimum of operator attention, or are only in use intermittently, are located on local control panels near the equipment to be controlled. Monitoring of the alarms of such control systems is provided in the Control Room. Design criteria for redundancy, separation and diversity are similar to those used for the Reactor Protection System as discussed in Section 7.2, except for Combustible Gas Control, which satisfies Reg Guide 1.7 design criteria.

7.3.1 DESCRIPTION

The Engineered Safety Features Actuation System (ESFAS) uses selected plant parameters and determines whether or not predetermined safety setpoints are being exceeded; if they are, it combines the signals into logic matrices sensitive to combinations indicative of primary or secondary system boundary ruptures (ANS Class III or IV faults). Once the logic combination is completed, the system sends actuation signals to the appropriate ESF components. The ESFAS meets the requirements of General Design Criteria 13, 20, 27, 28, and 38. The ESFAS is described in Section 7.3.1.1.

The Combustible Gas Control System, the FHB portion of the Emergency Exhaust Systems, and the Control Room Ventilation Isolation System are independent of the Westinghouse-furnished ESFAS. They have been designed to meet the requirements of GDC 13 and 20 and are described in Section 7.3.1.2.

7.3.1.1 Engineered Safety Features Actuation System Description

The ESFAS functionally consists of the following:

a) Process instrumentation and control (Reference 7.3.1-1)

b) Solid-State Logic Protection System (Reference 7.3.1-2)

c) Engineered safety features test cabinet (Reference 7.3.1-3)

d) Manual actuation circuits

The ESFAS consists of two distinct portions of circuitry: (1) An analog portion consisting of three to four redundant channels per parameter or variable which monitor various plant parameters such as reactor coolant system (RCS) and main steam supply system pressures, temperatures and flows and containment pressures; and (2) a digital portion consisting of two redundant logic trains which receive inputs from the analog protection channels and perform the logic needed to actuate ESF equipment. Each digital train is capable of actuating the ESF equipment required.

The engineered safety features actuation circuitry and hardware layout are designed to maintain channel isolation up to and including the bistable operated logic relay. This design is similar to that of the reactor protection circuitry as discussed in Section 7.2.

The redundant concept is applied to both the analog and digital portions of the system. Separation of redundant analog channels begins at the process sensors and is maintained in the field wiring, containment penetrations, and analog protection racks terminating at the

redundant safeguards logic racks. The design meets the requirements of GDC 20, 21, 22, 23, and 24.

The variables are sensed by the analog circuitry as discussed in Section 7.2. The outputs from the analog channels are combined into actuation logic as shown on Figure 7.3.1-1 sheets 2 through 7. Tables 7.3.1-2 and 7.3.1-3 give additional information pertaining to logic and function.

Redundant manual actuation of ESF trains is provided on the main control board from the following:

a) Safety injection actuation

b) Containment spray actuation (containment isolation - Phase B)

c) Containment isolation - Phase A/containment ventilation isolation

d) Main steam line isolation

Manual actuation from the main control board of containment isolation Phase A is initiated by operation of either one of the redundant momentary containment isolation Phase A controls. Each control consists of two mechanically linked actuation switches. The separate trains are thereby linked by mechanical means in a fashion similar to that shown on Figure 7.3.1-2. Manual actuation of safety injection from the main control board is initiated by one of the redundant controls; and a manual activation of containment spray (containment isolation Phase B) is initiated by either of the two sets of controls. Manual actuation of each of the main steam isolation valves is accomplished in the same manner as the manual actuation of containment isolation Phase A.

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

Refer to Figure 7.3.1-1, Sheet 2 for the interface of the signals that actuate engineered safety features equipment. The interlocks associated with ESFAS are outlined in Table 7.3.1-4. The following terminology is used to identify the various functional signals used to actuate ESF and supporting systems:

a) Safety Injection Actuation Signal (S)

b) Containment Isolation Actuation Signal-Phase A (T)

c) Containment Isolation Actuation Signal-Phase B (P)

d) Containment Spray Actuation Signal (CSAS)

e) Control Room Ventilation Isolation Signal (CRI)

f) Containment Ventilation Isolation Signal (CVIS)

g) Main Feedwater Isolation Signal (MFIS)

h) Main Steam Isolation Signal (MSIS)

7.3.1.1.1 Function Initiation

The specific functions and equipment which are initiated by ESFAS are:

a) A reactor trip, provided one has not already been generated by the Reactor Trip System.

b) Cold leg injection isolation valves, which are opened for injection of borated water by the charging pumps into the cold legs of the RCS.

c) Charging/high-head and RHR/low-head safety injection pumps and associated valving which provide emergency makeup water to the cold legs of the RCS following a LOCA.

d) Containment fan coolers, which serve to cool the Containment and limit the potential for release of fission products from the Containment by reducing the pressure following an accident.

e) Component cooling water pumps and emergency service water pumps

f) Motor-driven auxiliary feedwater pumps

g) Phase A containment isolation, which functions to prevent fission product release, i.e., isolation of all lines not essential to reactor protection.

h) Steam line isolation to prevent the continuous, uncontrolled blowdown of more than one steam generator and thereby uncontrolled RCS cooldown.

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

j) Standby diesel generators to assure backup supply of power to emergency and supporting systems components.

k) Isolation of the control room intake ducts to protect control room personnel from potential airborne radioactivity following a LOCA.

l) Containment spray actuation, which initiates containment spray to reduce containment pressure and temperature following a LOCA or steam line break accident inside the Containment.

m) Phase B containment isolation, which isolates the Containment on high pressure following a LOCA or a steam or feedwater line break within the Containment to limit radioactive releases. (Phase B isolation together with Phase A isolation results in isolation of all but ESF lines penetrating the Containment.)

7.3.1.1.2 Analog circuitry

The process analog sensors and racks for the ESFAS are discussed in Section 7.2 and in Reference 7.3.1-1. Discussed are the parameters to be measured, including pressures, flows,

levels and temperatures. The transmitters, orifices, flow elements, and resistance temperature detectors as well as automatic calculations, signal conditioning, and location and mounting of the devices are also discussed.

Containment pressure is sensed by four physically separated differential pressure transmitters mounted by rigid supports outside of the Containment. They are connected to the Containment atmosphere by a filled, sealed hydraulic transmission system. The distance from penetration to transmitter is kept to a minimum, and separation is maintained. This arrangement, together with the pressure sensors external to the Containment, forms a double barrier and conforms to GDC 56 and Regulatory Guide 111.

The safety injection function is derived from the following logic functions, with the number of channels provided and the number needed to trip as shown in Table 7.3.1-2.

a) Manual actuation

b) Low pressurizer pressure

c) High containment pressure (Hi-1)

d) Low compensated steam line pressure

7.3.1.1.3 Digital circuitry

The ESF logic racks as part of the Solid State Protection System (SSPS) are discussed in detail in Section 7.2. The description includes the considerations and provisions for physical and electrical separation including details, provisions for test points, considerations for the instrument power source, and considerations for accomplishing physical separation. The outputs from the analog channels are combined into actuation logic as shown on Figures 7.3.1-1 Sheet 5 (steam generator, water level, and steam pressure rate), 7.3.1-1 Sheet 2 (ESF actuation), 7.3.1-1 Sheet 6 (feedwater control and isolation), 7.3.1-1 Sheet 3 (auxiliary feedwater), 7.3.1-1 Sheet 4 (steam line isolation), and 7.3.1-1 Sheet 7 (turbine trips, runbacks, and other signals).

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

7.3.1.1.4 Final actuation circuitry

The Solid State Protection System actuates the following equipment:

a) Table 7.3.1-5 lists actuated equipment for safety injection. Typical control logics for actuated equipment are shown on Figures 7.3.1-4, 7.3.1-11 and 7.3.1-15.

b) Table 7.3.1-6 lists actuated equipment for containment spray. Typical control logics for actuated equipment are shown on Figures 7.3.1-3.

c) Table 7.3.1-7 lists actuated equipment for containment isolation - Phase A. Typical control logics are shown on Figures 7.3.1-5 and 7.3.1-6.

d) Table 7.3.1-8 lists actuated equipment for containment isolation - Phase B. Typical control logics are shown on Figures 7.3.1-5 and 7.3.1-6.

e) Table 7.3.1-9 lists actuated equipment for containment ventilation isolation. Typical control logics are shown on Figure 7.3.1-23.

f) Table 7.3.1-10 lists actuated equipment for steam line isolation. A typical control logic is shown on Figure 7.3.1-7.

g) Table 7.3.1-11 lists actuated equipment for feedwater isolation. Typical control logics are shown on Figure 7.3.1-8.

If an accident is assumed to occur coincident with or without a loss of offsite power, the ESF loads will be sequenced into the safety buses so that emergency diesel generators or start-up transformers will not be overloaded, as discussed in Chapter 8. The design meets the requirements of GDC 35.

7.3.1.2 Independent ESF Actuation Systems

The following ESF Actuation Systems are independent of the Westinghouse Solid State Protection System.

a) Fuel Handling Building Emergency Exhaust System. Refer to Section 7.3.1.3.4.

b) Combustible Gas Control System. Refer to Section 7.3.1.4.

c) Control Room Ventilation Isolation System can be actuated independently of the SSPS, but has an "S" signal input. Refer to Section 7.3.1.5.7.

7.3.1.3 Automatically Actuated ESF Systems

7.3.1.3.1 Containment Heat Removal System

7.3.1.3.1.1 Containment Spray System

Refer to Section 6.5.2, Containment Spray System, for the system description, Figure 6.2.2-1 for the system flow diagrams, and Figure 7.3.1-3 for the CSS schematic and logic diagrams.

<u>Initiating Circuits and Logic</u>

The Containment Spray System is automatically energized by the Containment Spray Actuation Signal (CSAS). The CSAS is derived from high-pressure signals, as shown on Figure 7.3.1-1 Sheet 2. The CSAS signal energizes the Containment Spray System (CSS) by starting the containment spray pumps and opening the containment spray isolation valves. The operating mode of the Containment Spray System is automatically changed from injection mode to recirculation mode by transferring the suction of the pump to the containment sump, opening the

valves in the sump recirculation lines and closing the valves from the refueling water storage tank (RWST). This switchover is initiated by a 2-out-of-4 low RWST level signal.

A Containment Isolation (T) signal shuts down the recirculation line from the containment spray pump to the refueling water storage tank by isolation of the containment spray pump recirculation valves. The CSS can also be operated manually from the Control Room.

As described in Section 6.2.2.2, the containment spray actuation signal will initiate the operation of the sodium hydroxide addition system and the two sodium hydroxide system valves will open and admit the chemical to the two separate trains of the Containment Spray System. The valves will close automatically when the level in the tank reaches to the "empty level".

Bypasses, Interlocks and Sequencing

In addition to the automatic transfer of containment spray pump suction from the RWST to the containment sumps, the containment spray pump recirculation valves and the containment spray eductor test valves are automatically closed upon a "T" signal. The manual initiation of both safety trains of the CSS may be accomplished when both control switches on the main control board are activated. Also, once a safety train of the CSS is placed in the recirculation mode for testing, it cannot be automatically or manually placed in injection mode until the recirculation valve is closed and the containment spray pump is stopped.

The containment spray pumps are not directly sequenced onto the emergency buses on the receipt of an "S" signal or loss of offsite power; however, the sequencer panels may actuate them under the following conditions:

a) CSAS generated before the first second of load block 2 has elapsed: The spray pump starts in load block 2, its normal assignment.

b) CSAS generated after the first second of load block 2 has elapsed but before load block 3 is complete: Spray pump start is delayed until the start of load block 4. This delay is within the limits assumed in the containment transient analyses.

c) CSAS generated after load block 3 is complete: The spray pump starts immediately.

Redundancy and Diversity

The system is composed of redundant trains; Train A and Train B. The instrumentation and controls of the components and equipment in Train A are physically and electrically separate and independent of the instrumentation and controls of the components and equipment in Train B. The redundancy and independence provided are adequate to maintain the equipment functional capabilities following the design basis events shown in Table 7.3.1-1.

Actuated Devices

The following devices are actuated in each CSS train by either the SSPS or individual manual component controls of the Containment Spray System.

a) Containment spray pump

b) Containment spray header isolation valve

c) Sump recirculation valves and injection supply valve

d) Containment spray pump recirculation valve

e) Containment spray chemical addition valve

f) Containment spray eductor test valve

Display Instrumentation

The safety-related display instrumentation, which provides the operator with sufficient information to monitor the performance of the Containment Spray System and to perform the required safety functions, is described in Section 7.5.

7.3.1.3.1.2 Containment Cooling System

Refer to Section 6.2.2.2.1 for a description of the Containment Cooling System (CCS), Figure 6.2.2-3 for the system flow diagram, and Figure 7.3.1-4 for the schematic and logic diagrams. The system includes both safety and non-safety subsystems which are used during normal plant operation.

Initiating Circuits and Logic

Controls and instrumentation necessary for remote manual operation of the non-safety fan coil units and the safety-related fan cooler units are located in the Control Room. The safety-related fan coolers can also be remotely controlled from the auxiliary control panels.

For description of mode of operation, refer to Section 6.2.2. The safety fan coolers are two-speed and operate at high speed during normal conditions. In the event of loss of offsite power, one fan of each of the four safety-related fan coolers is automatically started on high speed by the sequencer panels. Upon the initiation of a safety injection signal, one fan of each of the four fan coolers is automatically started on low speed by the sequencer panels. Also upon a safety injection signal, the non-safety fan coil units are automatically tripped.

Bypasses, Interlocks and Sequencing

The non-safety fan coil units are interlocked such that if the operating fan trips due to electrical overload or low flow conditions, the standby unit is automatically started. If one of these abnormal conditions exists for the safety fan coolers, low flow is alarmed and the operator will take appropriate actions.

The discharge dampers associated with each non-safety fan coil unit are automatically opened when the associated unit fan is started, and closed when the associated fans are stopped. During normal operating conditions, the nozzle dampers associated with the safety fan coolers are controlled as described in Section 6.2.2. In the event of a safety injection actuation signal, the nozzle damper is opened automatically when either cooler fan is operated at low speed.

When fan cooler operation is initiated via the sequencer panels, only the selected A or B fan is actuated. The other B or A fan is manually initiated from the MCB or ACP in the manual diesel generator Load Block 9 in the event that a fan was not automatically started in the "low speed" mode in Load Block 2. Refer to Table 8.3.1-2c.

Redundancy and Diversity

The system is composed of redundant safety trains, Train A and Train B, and non-safety trains. The instrumentation and controls of the components and equipment in Train A are physically and electrically separated and independent of the instrumentation and controls of the components and equipment in Train B. There is also complete physical and electrical separation between the safety and non-safety portions of the system.

Display Instrumentation

The safety-related display instrumentation, which provides the operator with sufficient information to monitor the performance of the Containment Cooling System and to perform the required safety functions, is described in Section 7.5. In addition to these instruments, the air outlet temperature of each fan coil unit and fan cooler cooling section is recorded in the Control Room on a multipoint recorder.

7.3.1.3.2 Containment Isolation System, Main Steam Line Isolation System and Main Feedwater Isolation System

Refer to Section 6.2.4 for a description of the Containment Isolation System and to Table 6.2.4-1 for a list of the lines affected by the isolation system. A typical logic for this system is shown on Figures 7.3.1-5 and 7.3.1-6.

The Main Steam Line Isolation System and Main Feedwater Isolation System consist of the aggregate of the following:

1. The Westinghouse supplied SSPS initiating circuits and logic which supply signals to effect main steam line and feedwater line isolations.

2. The Ebasco supplied interposing logic which permits the main steam line isolation valves and feedwater isolation valves to have redundant valve actuation circuits. Additionally, MSIV test capability is permitted by this logic. Refer to Figures 7.3.1-7 and 7.3.1-8.

3. The Ebasco supplied devices actuated by the main steam line isolation signal (MSLI). Refer to Table 7.3.1-10 for a listing of devices actuated by the MSLI, and to section 10.3.2 for a description of Main Steam Supply System.

4. The Ebasco supplied devices actuated by the Main Feedwater Isolation signal (MFIS). Refer to Table 7.3.1-11 for a listing of devices actuated by the MFIS and to Section 10.4.7 for a description of Feedwater System.

Initiating Circuits and Logic

The necessary containment piping and instrument lines are isolated by one or more of the following signals:

1. T and/or P - Containment Isolation Actuation Signal
2. MFIS - Main Feedwater Isolation Signal
3. MSIS - Main Steam Isolation Signal
4. S - Safety Injection Actuation Signal
5. CVI - Containment Ventilation Isolation Signal
6. M - Remote Manual From Control Room

Table 6.2.4-1 identifies the lines to be isolated and the signal that initiates isolation.

Power operated containment isolation valves have limit switches which indicate the status of the valve in the Control Room.

The Main Steam Isolation System is automatically energized by an SSPS supplied signal. Refer to Figure 7.3.1-1 Sheet 2 for events which result in the MSIS.

For the main steam line isolation valves, the MSIS is transmitted through Ebasco supplied logic shown on Figure 7.3.1-7. This logic prevents inadvertent opening of the main steam isolation valve in the presence of the MSIS. Refer to Section 7.7 for a description of control of other valves in the main steam lines.

Four Class 1E radiation monitors are used for the containment ventilation isolation signal (CVIS). Two monitors, RC-3561A and RC-3561C, are for train A and two monitors, RC-3561B and RC-3561D, are for train B. The CVIS is generated by a 2 out of 4 (2/4) logic. To obtain a train A 2/4 logic, the output of train B monitor signals are physically and electrically isolated from the system A and the output of train A monitor signals are isolated from system B for the train B logic. The functional logics are shown on FSAR Figures 7.3.1-1 Sheet 2. For additional information regarding the containment radiation monitors refer to Section 12.3.4.1.8.1.

As shown on Figures 7.2.1-1 Sheet 8 and 7.3.1-1 Sheet 2, Containment Ventilation Isolation Signal (CVIS) is generated by either containment high radiation (2/4 logic) or by the containment isolation Phase A (T) signal. Upon receipt of a high radiation signal, the retentive memory relay in the circuit will energize and generate the CVIS signal. To assure that a "T" signal will not be blocked after resetting the relay, the high radiation signal is a single shot. Although the high radiation condition may still be present after resetting the signal, the single shot feature blocks the radiation input signal to the CVIS output relay. Thus, a "T" signal is still capable of activating the CVIS after it has been reset. The high radiation condition must be corrected before the single shot is itself reset. Resetting of the CVIS signal, by itself, will not change the position of actuated components. The resetting of the retentive memory logic can be done through the CVIS signal reset switch from the Control Room.

The isolation of the Feedwater System can be accomplished manually through the Safety Injection (SI) manual actuation control switch from the Main Control Board. However, individual components of the Feedwater System can be manually isolated at any time from the MCB. Feedwater system can be effectively isolated from the MCB manually (without actuating Manual Safety Injection) by tripping the main feedwater pumps or closing the Steam Generators

Feedwater Isolation Valves FW-V26, FW-V27, and FW-V28. The FWIS & SI signals must be reset prior to the opening of the isolation valves. Separate control switches (Train A and Train B) are provided on the MCB for the resetting of the SI and FWIS signals.

Bypasses, Interlocks and Sequencing

The signals listed above override any manual action. Once initiated, all isolation actions go to completion and require operator action to return to the normal operating condition.

The SHNPP control circuitry for interfacing with automatic containment isolation valves is designed so that the result of resetting the isolation signal is not the automatic re-opening of containment isolation valves. In the event it is necessary to open any containment isolation valve after the isolation signal is reset, the operator must manually do so from the main control room. The re-opening of the isolation valves must be performed by the operator on a valve by valve basis. Each isolation valve has its own control switch located in the main control room to accomplish this. Refer to FSAR Figures 7.3.1-1 (Sheet 2 of 7), 7.3.1-5 (two sheets), 7.3.1-6, 7.3.1-7 and 7.3.1-8 (three sheets) for typical examples of the interface logic.

The main steam line isolation valves have redundant valve actuator circuits which, as shown on Figure 7.3.1-7 prevent inadvertent opening of the valve the presence of an MSIS.

Redundancy and Diversity

The system is composed of redundant trains; Train A and Train B. The instrumentation and controls of the components and equipment in Train A are physically and electrically separate and independent of the instrumentation and controls of the components and equipment in Train B. The redundancy and independence provided are adequate to maintain equipment functional capabilities necessary to isolate the Containment following the design basis events shown in Table 7.3.1-1.

Power for the actuation of two isolation valves in series (inside and outside of Containment) is supplied by redundant, independent power sources without cross-ties. Air operated containment isolation valves are designed to fail in a safe position upon loss of control air. Power for the redundant main steam isolation valve actuator circuits is supplied by separate, independent power sources without cross-ties.

Actuated Devices

Tables 7.3.1-7 and 7.3.1-8, 7.3.1-10, and 7.3.1-11, respectively list the equipment actuated by the Containment Isolation System, Main Steam Isolation System, and Main Feedwater Isolation System. Other actuated devices in the main steam lines are described in Section 7.7.

Display Instrumentation

The safety-related display instrumentation, which provides the operator with sufficient information to monitor the performance of the isolation systems and to perform the required safety functions, is described in Section 7.5.

7.3.1.3.3 Auxiliary Feedwater System

Refer to Section 10.4.9 for a description of the Auxiliary Feedwater System, to Figure 10.1.0-3 for the system flow diagram, and to Figures 7.3.1-9 and 7.3.1-10 for the schematic and logic diagrams. The auxiliary feedwater system instrumentation and controls are designed for automatic operation during emergency situations such as steam line rupture, loss of normal feedwater, and loss of offsite power, and manually as part of the safe shutdown systems.

Initiating Circuits and Logic

The motor driven auxiliary feedwater pumps are automatically started by any one of the following signals.

1. Safety injection signal
2. Low-low water level in any steam generator
3. Loss of power (undervoltage) on the emergency bus
4. Loss of both feedwater pumps
5. AMSAC

The turbine driven auxiliary feedwater pump is automatically started by any one of the following signals:

1. Loss of power (undervoltage) on the emergency bus
2. Low-low water level in two out of three steam generators.
3. AMSAC

The steam inlet valves to the Steam Driven Auxiliary Feedwater Pumps are powered from the safety DC battery system.

Upon any automatic initiation of the auxiliary feedwater pumps (motor or turbine driven), the steam generator blowdown and sampling valves are closed.

Once initiated by an automatic signal, an auxiliary feedwater pump may be stopped or restarted manually by the operator.

A comparison of the differential pressures between all steam generators is made and used in conjunction with the MSIS to determine a steam line break and isolate the faulty steam generator from auxiliary feedwater. Both the steam generator (steamline) pressure mismatch logic and MSIS are results of two out of three logics and are combined in a coincidence Logic to develop a Steam Generator Available Signal (SGAS).

A SGAS will close the auxiliary feedwater regulating and motor-operated isolation valves to the faulty steam generator.

Manual initiation and operation of the Auxiliary Feedwater System is provided in the Control Room. Auxiliary feedwater can be effectively isolated manually (without actuating the Manual Safety Injection) by the operator from the MCB by tripping the pumps or isolating the auxiliary feedwater pump discharge motor operated isolation valves. In addition, manual control switches for the auxiliary feedwater pumps, auxiliary feedwater isolation and regulating valves are provided on the auxiliary control panel (ACP).

Manual auxiliary feedwater flow is provided by opening the auxiliary feedwater isolation valves and controlling the auxiliary feedwater flow, through the auxiliary feedwater regulating valves, by means of manual controls on the main control board (MCB) or ACP. Process indication, alarm and status instrumentation is provided to enable the MCB or ACP operator to evaluate system performance and detect malfunctions.

The auxiliary feedwater regulating valves are automatically driven full open upon any of the following initiating signals:

1. Safety injection signal;
2. Low-low water level in any steam generator;
3. Loss of off-site power;
4. Loss of both main feedwater pumps;
5. AMSAC.

The auxiliary feedwater pumps discharge pressure is maintained by regulating valves at the discharge of the auxiliary feedwater pump such that the valves cannot be operated beyond the pump low pressure setpoint (runout protection).

Bypass and Interlocks

The AFW pumps have an alarm for low pump suction, and a pump trip on low-low pump suction. Also included are low pump discharge pressure alarms.

Pressure switches PS-2250A1 and PS-2250B1, Auxiliary Feedwater Suction Pressure Switches, will trip the AFWP-A&B pumps for low-low pressure in the pumps suction header.

Redundancy is provided by the Auxiliary Feedwater Pumps A&B Discharge Pressure Switches PS-2150A and PS-2150B located in the pumps discharge line to provide alarm in the MCB Annunciator and Auxiliary Control Panel (ACP) Annunciator for low discharge pressure.

Turbine Driven Auxiliary Feedwater Pump Lube Oil low pressure is alarmed in MCB per FCR-I-2826 R/2.

Sequencing

Upon loss of offsite power or during Safety Injection with offsite power available, the motor driven pumps are automatically started and powered from the respective standby diesel generators through the sequencer.

Redundancy

The system contains two motor driven pumps and one turbine driven pump. The motor driven pumps are arranged in two separate trains: Train A and Train B. The instrumentation and controls of the components and equipment in Train A are physically and electrically separate and independent of the instrumentation and controls of the components and equipment in Train B.

The two trains of motor driven auxiliary feedwater pumps and associated auxiliary feedwater valves are powered from one of two redundant emergency buses, SA and SB, with separate and independent circuitry being provided for redundant components. In addition, diversity is provided by AC electric power for the motor driven pump(s) and by steam power for the turbine driven pump.

Display Instrumentation

The safety-related display instrumentation, which provides the operator with sufficient information to monitor the performance of the Auxiliary Feedwater System and to perform the required safety functions, is described in Sections 7.4.1.3 and 7.5.1.3.5.

7.3.1.3.4 Emergency Exhaust Systems

Refer to Section 6.5.1 for a description of the Emergency Exhaust System, to Figures 9.4.2-1 and 9.4.3-2 for the system flow diagrams, and to Figures 7.3.1-11 through 7.3.1-14 for the logic and schematic diagrams.

Initiating Circuits and Logic

The emergency exhaust units in the Reactor Auxiliary Building and Fuel Handling Building can be operated from the Control Room through their control switches for testing to prevent a build-up of moisture in charcoal adsorbers.

See Figure 7.3.1-13 and Section 6.5.1.2 for a detailed description of the fuel handling building emergency exhaust unit.

The conditions and signals that cause automatic initiation of the various exhaust units are as follows:

a) Following a design basis accident (DBA)

The SSPS generated safety injection signal or the Control Room Isolation Signal (CRIS) will cause the following:

1) Reactor auxiliary building (RAB) emergency exhaust fans start (via the load sequencer on a safety injection or directly via train specific logic on a Control Room Isolation)

2) Reactor auxiliary building isolation dampers close, (isolating the NNS portions of the ventilation from the safety portions).

The RAB Emergency Exhaust System has two completely redundant systems which operate similarly.

b) Following a Fuel Handling Accident in the Fuel Handling Building:

On a high radiation signal generated at the fuel handling operating floor, the signal causes the following:

1) FHB emergency exhaust fans start

2) Fuel handling building isolation dampers close to isolate the normal supply and exhaust ventilation subsystems

The FHB Emergency Exhaust System has two completely redundant systems which operate similarly.

The FHB system is completely isolated upon radiation monitoring signal actuation. In addition, the Fuel Handling Building can be effectively isolated manually by actuation of individual isolation components at any time from the Control Room (Auxiliary Equipment Panel). The normal supply for the FHB can be isolated by tripping the operating supply and exhaust fans which in turn shut the isolation dampers. The Spent Fuel Pool Pump Room ventilation can be isolated by tripping the operating supply Fan AH-17. The FHB loading area can be isolated by shutting the isolation dampers D35SA or D36SB and D37SA or D38SB.

The RAB ventilation isolation is part of the component isolation during a manual safety injection actuation. Manual actuation of SI will also include the isolation of the RAB ventilation system. The RAB can be effectively isolated manually (without actuating the manual SI) from the Auxiliary Equipment Panel. The RAB switchgear rooms can be isolated by closing the system Outside Air Intake and exhaust air dampers and aligning the system for full recirculation mode. The Normal Exhaust System can be isolated by tripping the exhaust Fans E17, E18, E19, and E20. The electrical protection room can be isolated by isolation valves at the air intake and exhaust and aligning system for full recirculation mode. Manual reset of the SI from the MCB will automatically reset the RAB ventilation isolation signal.

Bypasses, Interlocks and Sequencing

Electric heating coil SA control circuit is interlocked with the fan SA starter and its built-in air flow and temperature switches. The coil is energized and remains energized when: 1) the fan is started, 2) the flow velocity through the coil has exceeded a predetermined level as established by the coil manufacturer, and 3) the temperature of air leaving the coil remains below a level as established by the coil manufacturer. The coil electric power is modulated by a SCR drive based on the outlet temperature of the charcoal filters. The fan inlet and outlet and filter train inlet valves are interlocked with the fan A-SA starter. The valves are opened when the fan starts. The heater coil SB control circuit and associated valves are similarly interlocked with the B-SB fan starter.

The fan is designed to operate when its inlet vortex damper is closed, or opened partially as controlled by building pressure and flow through the filter train.

Operation of both trains is not required during an accident period. If both trains are running, the operator can place a train in standby by stopping the exhaust fan.

Each train is automatically actuated, the RAB exhaust units by either a Safety Injection Actuation Signal or a Control Room Isolation Signal, and the FHB exhaust units by a high radiation signal in the Fuel Handling Building. For the details of the control logic see Figures 7.3.1-11 through 7.3.1-14.

There is no automatic bypass and sequencing for the dampers. After an automatic closure, a damper can be reopened through its control switch if its actuating signals are not present.

Redundancy and Diversity

The system is composed of redundant Trains A and B. The instrumentation and controls of the components and equipment in Train A are physically and electrically separate and independent of the instrumentation and controls of the components and equipment in Train B. The redundancy and independence provided between safety trains A and B are adequate to maintain equipment functional capabilities following the design basis events shown in Table 7.3.1-1.

Display Instrumentation

The safety-related display instrumentation, which provides the operator with sufficient information to monitor the performance of the Emergency Exhaust Systems and to perform the required safety functions, is described in Section 7.5.

7.3.1.4 Manually Initiated ESF Systems

7.3.1.4.1 Combustible Gas Control System

Refer to Section 6.2.5 for a description of the Combustible Gas Control System. The system consists of two non-safety-related subsystems which operate as follows:

a) A hydrogen analyzing subsystem (grab sample skid) provides the capability to monitor the containment atmosphere, and

b) The containment hydrogen purge subsystem (which is non-safety-related except for the containment isolation function) for providing a controlled purge of the Containment through fission product removal equipment. Refer to Figure 7.3.1-27 for the Instrument Schematic and Logic Diagrams.

Initiating Circuits and Logic

Complete system instrumentation and control are provided in the Control Room and electrical protection room adjacent to the Control Room for beyond design-basis accident monitoring. Indicating lights constantly show the operating or position status of each item of equipment in this system. The system is manually controlled by remote switches in the electrical protection room adjacent to the Control Room, and is manually actuated after a beyond design-basis accident. The control switches located on the control room radiation monitoring panel enable

the operator to open and close the sample valves within the Containment in sequence in order to obtain samples from various areas.

The containment atmosphere is monitored after a beyond design-basis accident in order to maintain combustible gas.

The combustible gas can be removed by the containment hydrogen purge subsystem (if available) which directs purge flow through the hydrogen purge filtration system which provides filtration before release to the outside.

To initiate system operation the operator manually actuates:

a) Hydrogen analysis sampling equipment

b) Hydrogen purge fans and valves

Bypasses, Interlocks and Sequencing

Except for the containment hydrogen purge system, there are no bypass, interlock, or sequencing provisions for combustible gas control system.

Electric heating coil and supply valves CM-B1, CM-B2, CM-B3 are interlocked with the Hydrogen Purge Subsystem Exhaust Fan E4 (1X-NNS) starter. The valves are opened when the fan starts.

Redundancy and Diversity

Except for the containment hydrogen purge subsystem, the system is composed of redundant equipment A and B. The instrumentation and controls of the components and equipment in Train A are physically and electrically separate and independent of the instrumentation and controls of the components and equipment in Train B. The redundancy and independence provided are adequate to maintain equipment functional capabilities. The containment hydrogen purge subsystem is designed on a non-redundant basis and consists of an exhaust train and a supply train (valves only). This system with the exception of components necessary for containment isolation is not safety-related and is used after a beyond design-basis accident only if available.

Display Instrumentation

The display instrumentation provides the operator with sufficient information to monitor the performance of the Combustible Gas Control System and to perform the required functions, is described in Section 7.5.

7.3.1.5 Automatic and Manually Controlled ESF Support Systems

7.3.1.5.1 Emergency power systems

Refer to Section 8.3.1 for a description of the Emergency Power Systems and Figure 8.3.1-1 for the diesel generator starting logic.

Initiating Circuits and Logic

Each diesel generator has a manual and an automatic starting mode. A control switch on the main control board and a control switch on the diesel generator local panel, allows the operator to manually start and stop the diesel generator and control the diesel generator breakers for synchronizing with the offsite power system. Manual starting is used for the testing and for anticipating abnormal conditions within the unit.

Emergency starts are initiated automatically in response to contact closures from the bus undervoltage relay (86 UV), safety injection slave relays K601 or K610, or tie breaker 105 or 125 52Sb contacts. Loss of AC power supplied to the ESF buses is sensed when the 6.9 kv emergency bus voltage falls below approximately 80 percent of rated bus voltage (6900 v) for more than 1.2 second. This value was selected to prevent unnecessary engine starts due to voltage drops occurring during normal starting of large motors. After the diesel generator is on line feeding the ESF loads, the undervoltage load shedding system is blocked. Undervoltage relays are connected to the secondary side voltage transformers to detect the ESF bus low voltage.

Three undervoltage relays connected in a two out of three logic configuration provide the ESF bus undervoltage signal.

The diesel generator circuit breakers tying the diesel generators to their respective ESF buses will have two modes of operation, automatic and manual.

The diesel generator circuit breaker closes automatically when all the following conditions are satisfied:

a) The emergency bus is not energized

b) The diesel generator frequency is 54 Hz or greater

c) The generator voltage is 90 percent of rated or greater

d) The diesel generator lockout relay in the diesel generator local panel is reset.

The operator may close the diesel generator breaker by using a control switch in the Control Room or locally at the diesel generator local panel.

The operator turns the control switch to the closing position and the generator breaker closes when the following conditions are satisfied:

a) The synchronizing selector switch (located in either the Control Room or the diesel generator local panel) is in the proper position.

b) The synchro-check relay indicates a phase agreement between generator and the bus or the emergency bus is de-energized.

c) The diesel-generator "lock-out" relay is in the reset position.

To aid in manual synchronizing, a governor speed/load changer control switch is provided in the Control Room and local diesel generator panel. After synchronizing, the operator may use this same switch to load the diesel generator.

Bypasses, Interlocks and Sequences

A breaker open/closure overlap time of two cycles is utilized to prevent the automatic starting of the diesel generator during automatic switch-over of auxiliary transformers to the startup transformers. Diesel generators trip automatically on any of the following conditions:

a) Negative sequence

b) Diesel engine/generator mechanical trips

c) Voltage controlled overcurrents (trips diesel generator output breaker only)

d) Loss of excitation

e) Reverse power

f) Associated 6.9 Kv bus differential*

g) Diesel generator differential*

h) Diesel generator overspeed*

i) Loss of generator potential transformer circuit*

A trip of the diesel generator is annunciated locally and in the Control Room.

Upon loss of power on the emergency bus, all loads will be automatically tripped from the ESF bus and the required safety-related loads will be connected to the ESF bus automatically in proper sequence via the sequence panel.

The diesel generator will be periodically tested under load. Should normal AC power be lost during such a condition, or if a design basis accident precedes or follows this loss of normal AC power, the ESF bus tie breaker between the diesel generator and the ESF bus will open, the non-safety bus to ESF bus tie breaker will open, all non-safety-related loads will be shed from the ESF bus without being re-sequenced and the ESF bus automatic loading sequence will begin simultaneously.

Redundancy and Diversity

The system is composed of redundant diesel generators A and B. The instrumentation and controls for diesel generator A are physically and electrically separate and independent of the instrumentation and controls for diesel generator B. The redundancy and independence provided are adequate to maintain equipment functional capabilities following the design basis events shown in Table 7.3.1-1.

* The only conditions that will trip the diesel generator during a safety injection actuation signal.

Display Instrumentation

The safety-related display instrumentation, which provides the operator with sufficient information to monitor the performance of the Standby Power Systems and to perform the required safety functions, is described in Section 7.5.

Diesel generator supporting systems are discussed in Section 9.5.

Sequencer Description

There are separate but identical sequencers for each safety train (A and B). All the components of each sequencer (exclusive of inputs from external sensing devices, Main Control Board displays and controls and transfer switches) are located in a single cabinet. The train A sequencer is located in Switchgear Room A, and the Train B sequencer cabinet is located in Switchgear Room B, both of which are located on elevation 286 of the Reactor Auxiliary Building. Sequencer A is powered from 125 VDC Distribution Panel 1A-SA and Sequencer B is powered from 125 VDC Distribution Panel 1B-SB.

The primary function of the sequencer is to actuate the large ESF loads in response to ESFAS signals in a timing sequence which is within the design capabilities of the onsite electric power system. (Refer to FSAR Subsection 8.3.1.1.2.8).

a) Initiating Circuit and Logic - Each sequencer panel is energized upon receipt of actuation signal from the ESFAS SSP (Safety Injection Signal "LOCA") or loss of offsite power "LOOP". When the diesel generator has attained rated speed and voltage, the safety-related loads are connected to the 6.9 KV emergency buses (10 sec after the initiating of LOOP signal) sequentially by the Load Sequencer which actuates major ESF components in accordance with the Load Sequencing Table 8.3.1-2c in the FSAR. See also Section 8.3.1.1.2.8 for description of buses tripping and loading.

   There are three load sequencing programs in each sequencer:

   1) Program A - Loss of Offsite Power (LOOP) only.

   2) Program B - LOCA and LOOP.

   3) Program C - LOCA only.

   Each large ESF load actuated by the sequencer has a separate sequencer timer, although there is some sharing of sequence timers for the smaller ESF loads. Each sequencer timer consists of two time delay relays with their contacts in series, the first being a time delay relay whose a contacts close at the start of the load block (this is an instantaneous relay for load block 1 components) and the second being a time delay relay whose b contacts open five seconds after the start of the load block. Thus, the "Start" signal in each load block will remain for the duration of the load block rather than a pulse at the beginning of the loading block. This is done to ensure MCC Contactor pickup following unforeseen transient voltage dips.

   The sequence timers for loads which are actuated only on Program A are energized from sequencer Bus "A". Sequence timers for loads which are actuated on Program B and C but

not A are energized from Bus "BC", and sequence timers for loads which are actuated for all programs are energized from Bus "ABC". There are no loads unique to Program B or to Program C, nor are there any loads actuated on Programs A and B but not C, or on Programs A and C but not B. Also, there is no shifting of load block assignment for a given component depending on Program selection.

The only major automatically actuated ESF load which is not always actuated by one of the programs is the containment spray pump. The spray pump is a "roving" load because its CSAS actuation signal does not occur at a predictable time (when all LOCAs and MSLBs are considered) in relation to an SLAS. Design of the onsite power system is such that the spray pump load can be accommodated at any time during sequencing except starting with the Emergency Service Water Pump in load block 3. The sequencer design accounts for this by actuating the spray pump as follows:

1) CSAS generated before the first second of load block 2 has elapsed: The spray pump starts in load block 2, its normal assignment.

2) CSAS generated after the first second of load block 2 has elapsed but before load block 3 is complete: Spray pump start is delayed until the start of load block 4. This delay is within the limits assumed in the containment transient analyses.

3) CSAS generated after load block 3 is complete: The spray pump starts immediately.

4) Manual Loading Blocking: The sequencer blocks the manual start of certain loads (all manually actuated and some automatic major ESF loads) to assure that the operator cannot interface with the orderly load sequencing. This blocking begins at sequencer start and ends 10 seconds after the loading sequence is complete (as indicated by the breaker for Chiller WC-2, the last load to be sequenced, being commanded and confirmed to be closed).

5) MOV TOL Bypass: The sequencer initiates the bypass of the thermal overload and torque switches for the motor operated valves per Regulatory Guide 1.106.

6) 6.9kV and 480V Safety Bus Undervoltage Trip Bypass: The sequencer bypasses the 6.9kV and 480V safety bus undervoltage trip during Programs A and B.

b) Testing - The sequencer test is initiated manually either from the main control room or at the sequencer panel. The location for observing the test is at the sequencer panel because its component light array arrangement permits better test observation than the ESS light box in the main control room.

The sequencer is designed for testing during operation. This is accomplished through logic which generates simulated LOCA and/or LOOP signals and injects them into the program determination logic. The logic associated with the internally redundant relays LOCA-1(2)/X, LOCA-1(2)/XS, PRX1(2), UR1(2), and UR3(4,4X) of the program determination logic is individually testable during the test. Programs A, B, and C are simulated sequentially for a duration of 90 seconds each. The ability of each group of relays to initiate the programs and the action of all the sequencer timers is thus tested. Component actuation is stopped by

blocking relays that are automatically opened on test start and reclosed when the test is ended. During each periodic test, the test personnel turn switch SS to select the opposite group of relays listed above to test their ability to initiate the program. The test logic also regenerates a simulated Program B and Program A demand to retest the ability of the sequencer to initiate those programs.

The loading interruption on CSAS is tested during the periodic test. During the testing sequence, CSAS will automatically be tested in Load Block 2, Program BC sequence, and manually tested by depressing SOS/PB after Load Block 4 sequence. This tests the ability of the CSP to start during the second, fourth and any time after the fourth Load Block. The secondary sequencer functions are also exercised and tested during the periodic test.

During the testing of the sequencer internal circuits during normal operating condition, if any accident condition occurs, testing stops and all the circuits will be de-energized in 5 seconds.

During the testing of the sequencer programs, circuits to the components are temporarily bypassed in order to prevent actuation of the circuits.

Lamp Test - All the indicating lamp circuits are tested either from the MCB Lamp test switch or from the Sequencer lamp test push button.

Overload and Torque Switch Test - Motor overload and valve torque limit switch bypass circuit can also be tested from the MCB, control switch or from the sequencer panel.

c) Indications and Annunciators - The sequencer is equipped with annunciators and indication lights to monitor its status and operation. Various indications are available at the sequencer panel and in the main control room to facilitate testing/loading sequencer observation.

   The availability of the output contacts of the Load Sequencer actuating relays are supervised during plant normal operation as well as during testing of the Load Sequencer circuits at the sequencer panel.

   During normal operation the integrity of the load actuating circuit is monitored by an indicating light located under the corresponding load indicating light at the sequencer panel.

d) Reset - Sequencer internal circuit resets automatically when the actuation signal is reset.

e) Reliability Study - The reliability study and sneak circuit search was performed and resulting corrective actions were incorporated into the design. The proper operation of the sequencer will be verified during pre-operational testing.

7.3.1.5.2 Service water system

Refer to Section 9.2.1 for a description of the Service Water System (SWS) and to Figures 9.2.1-1 and 9.2.1-2 for the system flow diagram. See Figure 7.3.1-15 for the instrument schematic and logic diagrams.

Initiating Circuits and Logic

Controls and instrumentation necessary for remote manual operation of the normal and emergency service water pumps are located in the Control Room and the auxiliary control panel. Local instrumentation is also provided at pumps and the various heat exchangers for performance evaluation, maintenance and testing.

During normal plant operation one normal service water pump is used to remove rejected heat loads from the heat exchangers serviced by the SWS.

In the event of loss of offsite power, the emergency service water pumps are started automatically by the sequencer panels and each train provides cooling water to its associated diesel generator and other safety-related components.

In the event of a safety injection actuation signal (S), the emergency SWS pumps start automatically via the sequence panels. Should a loss of off-site power occur during a DBA, the emergency SWS pumps stop and restart automatically again from the diesel generator according to the loading sequence. Also upon an "S" signal, the non-safety-related portion of the SWS is automatically isolated and the water return shifted from the Cooling Tower to the Auxiliary Reservoir.

In the event of loss of their respective discharge line pressures, the emergency service water pumps start automatically to supply cooling water to essential equipment for plant shutdown.

The service water booster pumps to the safety-related containment fan coolers are operated in a similar manner to the emergency SWS pumps under DBA and loss of offsite power conditions. When a service water booster pump is started, the return bypass valve from its respective fan coolers closes, thus forcing the return flow through a restriction orifice in order not to overpressurize the SWS return header, but to allow the header pressure to be greater than the containment accident pressure.

Bypasses Interlocks and Sequencing

The normal SWS pumps are interlocked so that under normal operation if the operating pump trips, the other pump starts automatically upon an electrical fault of the operating normal service water pump. Upon loss of both normal service water pumps, both emergency service water pump will start on low header pressure.

Redundancy and Diversity

The system is composed of redundant Trains A and B. The instrumentation and controls of the components and equipment in Train A are physically and electrically separate and independent of the instrumentation and controls of the components and equipment in Train B. The redundancy and independence provided are adequate to maintain equipment functional capabilities following the design basis events shown in Table 7.3.1-1.

Display Instrumentation

The safety-related display instrumentation, which provides the operator with sufficient information to monitor the performance of the Emergency Service Water System and to perform the required safety functions, is described in Section 7.5.

7.3.1.5.3 Component Cooling Water System

Refer to Section 9.2.2 for a description of the Component Cooling Water System (CCWS) to Figures 9.2.2-1 through 9.2.2-4 for the system flow diagram.

Initiating Circuits and Logic

During normal operation, one CCWS pump in one train operates to supply cooling water to all essential and non-essential loads with the exception of the residual heat removal heat exchangers, which are isolated.

Upon receipt of an "S" signal, the CCWS converts from normal to emergency operation by isolating the non-essential loads and starting all the standby CCWS pumps.

The CCWS pumps may be operated manually by the operator either from the Control Room or the auxiliary control panel. The isolation of each redundant essential loop from each other, and the opening of the RHR heat exchanger CCWS isolation valves is manually accomplished by the operator from the Control Room. All non-essential loads may be manually isolated by the operator from the Control Room.

Bypasses, Interlocks and Sequencing

Upon the receipt of an "S" signal or loss of offsite power, two CCWS pumps are sequenced on line by the sequencer panels. During normal operation a standby CCWS pump is started on low CCWS header pressure. Refer to Sections 8.3.1.1.2.3, 8.3.1.1.2.4 and 9.2.2.3 for further information on the power supply arrangements.

Redundancy and Diversity

The system is composed of redundant Trains A and B. The instrumentation and controls of the components and equipment in Train A are physically and electrically separate and independent of the instrumentation and controls of the components and equipment in Train B. Refer to Figure 7.3.1-15a for the control scheme of the Service Water to the component Cooling Water Heat Exchangers. The redundancy and independence provided are adequate to maintain equipment functional capabilities following the design basis events shown in Table 7.3.1-1.

Display Instrumentation

The safety-related display instrumentation, which provides the operator with sufficient information to monitor the performance of the Component Cooling Water System and to perform the required safety functions, is described in in Section 7.5.

7.3.1.5.4 Essential Service Chilled Water System

Refer to Section 9.2.8 for a description of the Essential Service Chilled Water System (ESCWS) and to Figures 9.2.8-1 through 9.2.8-3 for the system flow diagram. See Figure 7.3.1-16 for the instrument logic and schematic diagrams of the ESCWS.

Initiating Circuits and Logic

The two essential chilled water trains are redundant and only one is required to operate. There are three separate and independent means of activating each train:

1. The chiller and the chilled water pump can be energized directly from their switches in the Control Room.

2. The chiller can be energized directly from its own local, integrally mounted control panel; and the chill water pump from the ACP.

3. The chiller and chilled water pump are automatically started upon receipt of an "S" signal.

A flow switch in the chilled water line is interlocked with the chiller to prevent the chiller start up before the flow of chilled water is established. The flow switch will also trip the chiller when flow loss occurs. Once the chiller is started, it remains under the control of a temperature controller which is furnished with the chiller package and is located in the unit-mounted control cabinet. This controller maintains a selected chilled water supply temperature.

Failures of the chilled water flow (high flow) and the condenser water flow (high and low) are alarmed and annunciated at the Control Room.

The non-safety portion of the ESCWS is isolated from the safety portion on the receipt of an "S" signal, or manually by the operator from the Control Room.

Interruption of the chiller operation as a result of the protective trips (cutouts) that require manual resetting, is annunciated at the Control Room through a common alarm which serves all such cutouts. Individual alarm annunciators are provided on the MCB for Compressor High Oil Temperature, Compressor High High Discharge Temperature, Compressor Refrigerant Low Pressure and Compressor Refrigerant High Pressure.

No means are provided during normal operation to automatically operate the idle train upon failure of the operating train. However, as the failure is annunciated at the Control Room, the operator manually takes the proper action to switch operation to the idle train and its associated air handling equipment accordingly.

Bypasses, Interlocks and Sequencing

Each chiller is interlocked with its respective chilled water flow switch so that it operates after water flow is established.

Three-way temperature control valves are provided in the supply lines of various chilled water cooling coils in order to maintain the system design head and design flowrate through the chiller within acceptable operating limits regardless of fluctuation in chilled water demand by the

various connected units. The temperature control valve recirculates excess supply water to the chilled water return.

The level in the expansion tank is automatically maintained by high and low level switches.

The chiller condenser water recirculation pump has a local control panel with a manual start and auto start feature. The chiller condenser pump will operate in any of these modes provided the corresponding chiller compressor has been started.

When the service water supply to the chiller condenser is less than the low flow setpoint value and with the chiller condenser water recirculation pumps' local control switch in the auto start mode, the pump will start in order to maintain the inlet water flow. When the service water flow is greater than the high flow setpoint value, the pump stops.

When started from low flow, the pump will continue to run until the service water flow is greater than the high flow setpoint value at which time the pump will stop.

In the manual start mode, after starting, the condenser water recirculation pump will continue to run until stopped by operator action or stopping of the corresponding chiller compressor. This feature assists in the routine performance of surveillance tests and in those instances where low condenser flow conditions exist in conjunction with service water flow greater than the high flow setpoint.

Upon loss of offsite power, the chillers and their chilled water pumps are automatically sequenced to reduce starting power requirements from the standby diesel generator. Each chiller is furnished with a compressor starter, operational and safety controls, interlocks and other controls for local and remote operation. If a chiller was active but stopped because of momentary loss of electrical power, it will resume operation upon receipt of the automatic actuating signals. The chiller design takes into consideration the restarting operation.

Redundancy and Diversity

The system is composed of redundant subsystems. The instrumentation and controls of the components and equipment in subsystem A are physically and electrically separate and independent of the instrumentation and controls of the components and equipment in subsystem B. The redundancy and independence provided are adequate to maintain functional capabilities following the design basis events shown in Table 7.3.1-1.

Display Instrumentation

The safety-related display instrumentation, which provides the operator with sufficient information to monitor the performance of the Essential Services Chilled Water System and to perform the required safety functions is described in Section 7.5.

7.3.1.5.5 120 Volt Uninterruptible AC Power System

Refer to Section 8.3.1 for a description and analysis of the 120 Volt Uninterruptible AC System.

7.3.1.5.6 Safety-related 125V DC Power Systems

Refer to Section 8.3.2.2 for a description and analysis of the 125 Volt DC Power System.

7.3.1.5.7 Control Room Ventilation System

Refer to Section 9.4.1 for a description of the Control Room Ventilation System and to Figure 9.4.1-1 for the system air flow diagram. See Figure 7.3.1-17 for the instrument logic and schematic diagrams.

The system is designed to allow for separate controls of the ambient temperature maintenance operation, normal fresh air makeup, normal exhaust and pressurization of the control room envelope, emergency air cleaning, emergency air makeup and pressurization.

During normal plant operation, one air handling unit and one normal exhaust fan are required to operate. The normal outside air intake and exhaust valves are opened. Emergency air intake valves are closed.

Following a Control Room Isolation Signal (CRIS), the outside air intakes and exhaust valves are automatically closed, the normal exhaust fan is stopped, and emergency filtration units start. In addition, the RAB Normal Ventilation System will be secured, and the RAB Emergency Exhaust System (RABEES) will be started. The RAB Normal Ventilation System must be secured to preclude the possibility of postulated system failures from impacting the ability of the Control Room Envelope (CRE) to maintain a positive pressure of ≥ 1/8 INWG relative to adjacent areas. When the RAB Normal Ventilation System is secured, the RAB Emergency Exhaust System is initiated to maintain the potentially contaminated areas of the RAB at sub-atmospheric pressure in an effort to limit outleakage and to remove radon gas from the RAB. The operator may shut down one of the two air cleaning units and air conditioning units (AH-15 A and B). These units are automatically started by a "S" or loop signal via the load sequencer. At the control operator's discretion, fresh air may be admitted to the system from one of the two emergency air intakes.

<u>Initiating Circuits and Logic</u>

A CRI signal is activated by any of the following signals:

a) Safety injection actuation signal

b) High radiation signal generated by redundant radiation detectors at the normal or emergency air intake.

c) Fire signal generated by fire detectors at the control room zone 1-150.

The isolation of the control room can be accomplished manually through the Safety Injection (SI) manual actuation control switch from the MCB. However, individual components of the control room isolation can be manually operated from the MCB with the exception that SI and CRI signals must be reset prior to the equipment changeover from an actuated mode to a normal mode. Separate control switches (Train A and Train B) are provided on the MCB for the resetting of the SI and CRI signal. The control room can be effectively isolated manually (without actuating the manual SI) by closing the normal supply air inlet butterfly valve 3CZ-B1SA

or 3CZ-B2SB and exhaust butterfly valves 3CZ-B3SA or 3CZ-B4SB from the Main Control Board.

Each air handling unit is normally operated by a control switch in the Control Room. Each of the normal outside air intake and exhaust valves is operated by a control switch in the Control Room.

Each normal exhaust fan is operated by a control switch in the Control Room. The exhaust isolation dampers are in parallel interlock with both normal exhaust fans. The dampers close when both exhaust fans stop and are opened when any of the two exhaust fans start. After an exhaust fan is started, its outlet flow control damper is automatically controlled by a pressure differential signal to maintain a constant positive pressure in the control room envelope relative to the surroundings.

Each emergency air filtration unit fan is operated by control switches in the Control Room. When a fan is started, its filter train valves are opened and the filter train electric heating coil is energized and its output power will be controlled from the downstream temperature element.

Redundant class IE radiation monitors are utilized for the Control Room Isolation system and are located in the normal outside air intake duct and emergency outside air intakes #10 and #11A. These monitors are interlocked to provide an isolation signal to the outside air intake and exhaust valves upon high radiation level detected by either monitor. The signals from these monitors are also interlocked to provide isolation signals to post-accident outside air intake valves and emergency filtration system. For the functional logics refer to FSAR Figure 7.3.1-1, sheet 2. For additional information, refer to Section 12.3.4.2.8.

Each electrically operated emergency outside air intake valve is normally operated by a control switch in the Control Room. The outside air intake valves may be opened or closed to any desired position by the operator in order to provide the proper makeup to the Control Room Ventilation System through the emergency system.

The smoke purge fans are operated by their respective control switches located in the Control Room. When a smoke purge fan is started the ventilation system is converted to a once through system. The purge makeup air dampers and purge dampers are opened and air recirculation dampers are closed.

All instrumentation and control switches, with the exception of the emergency filtration fans and outside air intake valves, are duplicated on the auxiliary control panel in the event the Control Room is evacuated.

Bypass, Interlocks and Sequencing

The chilled water flow control valve is modulated by a control signal generated from the control room temperature/moisture analog control of the control room space.

Electric reheat coils in zone supply air ducts are individually controlled by their temperature controllers. Each reheat coil is energized only after both of its built-in temperature and air flow switches make contact and either fan is running.

Upon the receipt of an "S" signal, air handling fans and emergency filter-fans are sequenced on line if not already running. When there is a loss of offsite power condition, these loads also are sequenced on line.

There is no bypass for the automatic closure of the normal fresh air intake and exhaust isolation valves. The valves cannot be reopened in the presence of their automatic actuating signals.

There is no bypass for the automatic starting of the emergency filtration unit. A unit can be stopped in the presence of its automatic actuating signals at the discretion of the operator after conditions have stabilized.

The emergency filtration unit fan is interlocked with its filter train valves and electric heating coil. The electric heating coil is controlled by its temperature controller.

The emergency air intake valves are manually operated through their control switches at the operator's discretion. These valves are normally closed and automatically closed if open when a control room isolation signal is generated and then released to operator control after a short time period.

Redundancy and Diversity

The system is composed of redundant safety-related train components A and B and non-safety-related components. The instrumentation and controls of the safety-related train A components are physically and electrically separate independent of the instrumentation and controls of the safety-related train B components. Instrumentation and controls of non-safety-related components are physically and electrically separate from all safety-related components. The redundancy and independence provided are adequate to maintain equipment functional capabilities following the design basis events shown in Table 7.3.1-1.

Display Instrumentation

The safety-related display instrumentation, which provides the operator with sufficient information to monitor the performance of the Control Room Air

Conditioning System and to perform the required safety functions, is described in Section 7.5.

7.3.1.5.8 RAB ESF Equipment Cooling System

Refer to Section 9.4.5.1 for a description of the RAB ESF Equipment Cooling System to Figures 9.4.3-1, 9.4.3-2, 9.2.8-1, and 9.2.8-2 for the system flow diagrams. See Figure 7.3.1-18 for the system instrument logic and schematic diagrams.

Initiating Circuits and Logic

Each ESF fan cooler is remotely operated by its control switch in the Control Room. Each ESF fan cooler is automatically started and stopped by space temperature switches.

Bypass, Interlocks and Sequencing

The chilled water flow control valve is interlocked with the cooler fan in such a way as to supply water to the cooling coils when the fan is running and bypass the coils when the fan is stopped. Upon receipt of an "S" signal or loss of offsite power, the fan coolers are sequenced on line by the sequencer panels.

During emergency start through sequencer, the temperature switch interlock is bypassed.

Redundancy and Diversity

The system is composed of redundant trains; Train A and Train B. The instrumentation and controls of the components and equipment in Train A are physically and electrically separate and independent of the instrumentation and controls of the components and equipment in Train B. The redundancy and independence provided are adequate to maintain equipment functional capabilities following the design basis events shown in Table 7.3.1-1.

Display Instrumentation

There is no display instrumentation for the ESF Equipment Cooling System except for fan status indicating lights and annunciators.

7.3.1.5.9 Diesel Generator Building Ventilation

Refer to Section 9.4.5.2.5 for a description of the Diesel Generator Building Ventilation System, to Figure 9.4.5-2 for the system flow diagram and to Figure 7.3.1-19 for instrument logic and schematic drawings.

The Diesel Building Ventilation System is divided into independent subsystems for each diesel generator area. Each area has a ventilation system for the diesel generator room, the electrical equipment room and the day tank and silencer rooms.

Initiating Circuits and Logic

Each fan associated with the Diesel Generator Building Ventilation System is remotely operated by its control switch in the Control Room. Under normal conditions, one diesel generator room exhaust fan (lead) is automatically started when its associated diesel generator is started. The fan continues to run after the diesel generator is stopped until the room temperature is below 105 F. The second fan also starts automatically whenever the diesel generator is running and either the temperature exceeds 105 F in the room or the outside air exceeds 80 F. The fan automatically stops when the room temperature drops below 105 F. In the event it is determined that a fire condition exists, both fans are automatically started when the operator places the smoke mode control switch in the "smoke" position.

The day tank/silencer exhaust fans and electrical room air handling fans are operated in a similar manner. Under normal conditions the operator manually initiates one fan for each subsystem, which operates continuously.

Interlocks, Bypasses, and Sequencing

Whenever a safety injection actuation signal or loss of offsite power condition exists, the diesel generator building ventilation system lead fans are automatically started via the sequencer panels.

The standby fans for the day tank/silencer room and electrical rooms are interlocked so that upon failure of their respective lead fans, they are automatically started.

The exhaust dampers from the silencer and the diesel generator rooms are interlocked. Whenever the diesel generator is started, the damper from the silencer room assumes full open position and the diesel generator room damper closes. Since the diesel generator room exhaust fan is also started at this time, the exhaust from the axial fan room and the diesel generator room is directed to those fans. The outside air intake damper for the electrical equipment room is at its minimum opening whenever the room temperature is less than 95 F, the outside air temperature is less than 70 F, the smoke mode switch is in the normal position and one air handling fan is running. Should any of these conditions not be present, then the outside air intake damper will change to its opposite (failure) position. In addition, whenever an electrical room air handing fan is running, the room temperature is maintained by a heating coil. The heater is modulated by a controller set at 70 F.

Redundancy and Diversity

The system is composed of redundant trains; Train A and Train B. The instrumentation and controls of the components and equipment in Train A are physically and electrically separate and independent of the instrumentation and controls of the components and equipment in Train B. The redundancy and independence provided are adequate to maintain equipment functional capability following those design basis events shown in Table 7.3.1-1.

Display Instrumentation

The safety-related display instrumentation, which provides the operator with sufficient information to monitor the performance of the Diesel Generator Building Ventilation System and to perform the required safety functions, is described in Section 7.5.

7.3.1.5.10 Essential Electrical Area HVAC Systems

7.3.1.5.10.1 Electric Equipment Protection Room HVAC System

The electric equipment protection rooms in the Reactor Auxiliary Building are heated and cooled by separate essential HVAC systems which are required to operate during normal plant operation, as well as a DBA. Refer to Section 9.4.5.2.3 for system description of the essential HVAC systems and Figure 9.4.5-1 for the system flow diagram. Instrument logic and schematic diagrams for this system are shown on Figure 7.3.1-20.

Initiating Circuits and Logic

Each essential HVAC system supply fan is operated by a control switch in the Control Room. The supply fans are automatically actuated by a "S" or Loss of Offsite Power signal via the Load Sequencer and recirculate air within the Electric Equipment Protection Room, by closing intake

and exhaust valves upon a CRI signal. When a HVAC unit is idle, its chilled water valve and air dampers at the supply are closed and the electric heating coil is deenergized. The HVAC room exhaust fans are operated by control switches in the Control Room. These exhaust fans are automatically stopped by a CRI signal.

Bypass, Interlocks and Sequencing

Whenever, a CRI signal is the result of an "S" signal or there is loss of offsite power, the essential HVAC supply fans are started by the sequencer panels. Each essential HVAC unit fan is interlocked with its chilled water valve duct dampers and electric heaters.

There is no bypass in the automatic actuation of the essential system by the CRI signal.

When the system is placed in the smoke purge mode all return air dampers close, except from the computer room which opens, and the smoke purge intake dampers open. Thus, with the purge fans running the HVAC system is converted to a "once" through system.

Redundancy and Diversity

The instrumentation and controls of the components in the essential HVAC system Train A are physically and electrically separate from those of the essential cooling system Train B. The redundancy and independence provided are adequate to maintain functional capabilities following the design basis shown in Table 7.3.1-1.

Display Instrumentation - There is no display instrumentation for the electric equipment protection HVAC systems provided for the operator in the Control Room, except for fan status indicating lights.

7.3.1.5.10.2 Reactor auxiliary building switchgear rooms

The essential switchgear rooms in the Reactor Auxiliary Building are heated and cooled by separate essential air cooling systems which are required to operate during normal plant operation as well as a DBA. Refer to Section 9.4.5.2.2 for system description of the essential HVAC systems and Figure 9.4.5-1 for the system flow diagram. Instrument logic and schematic diagrams for the system are shown on Figure 7.3.1-21.

Initiating Circuits and Logic

Each essential air cooling system supply fan is operated by a control switch in the Control Room. The system is automatically actuated by an "S" signal. When an air cooling unit is idle, its chilled water valve and air dampers at the supply are closed and the electric heating coil is de-energized. Upon an "S" signal, the battery room exhaust fan automatically stops and its bypass return air damper opens.

Bypass, Interlocks and Sequencing

Upon receipt of an "S" signal or loss of offsite power, the essential HVAC unit fans are started by the sequencer panels. The battery room exhaust fans are only restarted upon return of offsite power.

Each essential HVAC unit fan is interlocked with its chilled water valve and dampers and electric heaters.

When an essential HVAC supply fan is started, its corresponding battery room exhaust fan is automatically started. If there is a failure due to low air flow or electrical fault of a fan, the idle combination supply/exhaust fans are started as a ready standby.

There is no bypass in the automatic actuation of the essential system by the receipt of an "S" signal.

The system is placed in the smoke purge mode by the operator manually opening the purge damper of the switchgear affected from the Control Room. This in turn automatically starts its respective purge supply fan and its corresponding exhaust fan, and closes the system's return air damper.

Redundancy and Diversity - The instrumentation and controls of the components in the essential HVAC system Train A are physically and electrically separate from those of the essential cooling system Train B. The redundancy and independence provided are adequate to maintain functional capabilities following the design basis events shown in Table 7.3.1-1.

Display Instrumentation

There is no display instrumentation for the RAB switchgear rooms HVAC systems in the Control Room except for fan status indicating lights.

7.3.1.5.11 Spent Fuel Pool Pump Room Ventilation System

Refer to Section 9.4.2 for a description of the Spent Fuel Pool Pump Room Ventilation System, to Figure 9.4.2-1 for the system flow diagram, and to Figure 7.3.1-22 for instrument logic and schematic drawings. This system provides cooling to the spent fuel pool pump room and emergency exhaust system during normal and fuel handling accident conditions.

Initiating Circuits and Logic

Each of the redundant fan coolers can be remotely operated by its control switch in the Control Room. Cooling water is supplied from the Essential Services Chilled Water System and the chilled water control valve is automatically positioned upon the starting of the fan. The cooling water flow to the cooling water coils is modulated based on the temperature of the affected spaces.

Bypass, Interlocks and Sequencing

The chilled water flow control valve is interlocked with the cooler fan in such a way as to supply water to the cooling coil when the fan is running and bypass the coils when the fan is stopped. In the event of a loss of offsite power or an "S" signal actuation, the fans will trip, and may only be restarted manually once the manual loading permissive is received (Load Block 9). These fans may be manually loaded on the safety bus, when necessary, to control area temperature.

Redundancy and Diversity

The instrumentation and controls of the redundant isolation dampers are physically and electrically separated. The damper controls are not connected to other ventilation components. Electrical and physical separation is adequate to retain the redundancy required to maintain equipment functional capability following those design basis events shown in Table 7.3.1-1.

Display Instrumentation

The safety-related display instrumentation, which provides the operator with sufficient information to monitor the performance of the isolation dampers and to perform the required safety functions, is described in Section 7.5.

7.3.1.5.12 Containment Vacuum Relief System

Refer to Section 6.2.1.1.3.4 for a description of the Containment Vacuum Relief System, to Figure 6.2.2-3 for the system flow diagram, and to Figure 7.3.1-23 for the instrument logic and schematic diagrams. This system is designed to protect the Containment Building against excessive differential pressure that could result from inadvertent actuation of the containment spray system.

Initiating Circuits and Logic

There are two redundant vacuum relief trains. Each of the redundant containment vacuum relief trains has a butterfly valve that can be remotely operated by a control switch in the Control Room. Each of these butterfly valves has a slave damper at a RAB air intake which functions at the same time as with its associated valve as long as instrument air is available. Each butterfly valve has an air accumulator which will allow extended operating duty after loss of the plant air system. Each train is automatically controlled based on containment building pressure between a negative 0.25 in. water gage and negative 2.5 in. water gage.

Excess flow check valves are installed to meet the requirements of GDC 56.

Bypass, Interlocks and Sequencing

In the event there is a containment ventilation isolation signal (CVI), the butterfly valve and damper of each train will close or be prevented from opening until this signal is reset. Once this signal has been reset for a particular safety train, the associated vacuum relief train will operate automatically.

Redundancy and Diversity

The instrumentation and controls of the redundant trains are physically and electrically separated. The controls for these systems are not connected to other containment ventilation systems. In addition, the differential pressure transmitters used for control and monitoring are of different manufacture to minimize common mode failures between manual and automatic operation. The differential pressure transmitters are located outside the Containment in the vicinity of other instrument sensing lines in the RAB. The redundancy and independence provided are adequate to maintain functional capabilities following the design basis shown in

Table 7.3.1-1. The arrangement and containment penetration details are described in FSAR Section 6.2.4.

Display Instrumentation

The safety-related display instrumentation which provides the operator with sufficient information to monitor performance of the Containment Vacuum Relief System and to perform the required safety functions is listed in Table 7.5.1 1.

7.3.1.5.13 Fuel Oil Transfer Pump House Ventilation System

Refer to Section 9.4.5.2.4 for a description of the Fuel Oil Transfer Pump House Ventilation System, to Figure 9.4.5-2 for the system flow diagram, and to Figure 7.3.1-24 for the instrument logic and schematic diagrams. The system is used to maintain the pump room temperature below 104 F, and remove fuel oil fumes both under normal and accident conditions.

Initiating Circuits and Logic

There are two pump rooms each having two redundant exhaust fans. Each of the fans can be remotely operated by its control switch in the Control Room.

Bypass, Interlocks and Sequencing

Under normal conditions one of the two fans is running. In the event there is a low flow condition due to loss of the operating fan, the second fan will automatically start after a time delay. In the event there is a loss of offsite power or an "S" signal actuation condition, the lead exhaust fan will be started automatically.

Redundancy and Diversity

The instrumentation and controls of the components of each pump house ventilation system are physically and electrically separate from each other. The redundancy and independence provided are adequate to maintain functional capabilities following the design basis events shown in Table 7.3.1-1.

Display Instrumentation

There is no display instrumentation for the fuel oil transfer pump house ventilation system, except for fan status indicating lights and annunciators.

7.3.1.5.14 Emergency service water intake structure ventilation system

Refer to Section 9.4.5.2.6 for a description of the Emergency Service Water Intake Structure Ventilation System, to Figure 9.4.5-2 for the system flow diagram, and to Figure 7.3.1-25 for the logic and schematic diagrams. This system is to insure the maximum temperatures of the electrical and pump rooms of 116°F and 122°F respectively are not exceeded.

Initiating Circuits and Logic

Each electrical equipment and pump room has its own distinct ventilation system. The electrical equipment room system includes a supply fan, cooling coil (isolated), electric heating coil, filter and associated supply and return dampers. Exhaust fans are provided for the pump room ventilation. Each fan associated with the ventilation system is remotely operated by its control switch in the Control Room.

Bypass, Interlocks, and Sequencing

Under normal operation, the electrical room supply fan is automatically started when the room temperature exceeds 102°F. The pump room exhaust fan will automatically start when either the outside air temperature exceeds 70°F or the room temperature exceeds 90°F and its associated emergency service pump is running.

The electric heating coil is permitted to operate only when its associated supply fan is running. The cooling coil has two sources of water supply (isolated), emergency service water or cooling tower makeup. Normally water is used from the cooling tower makeup source. Whenever the associated emergency service water pump is running, the water supply is from the emergency service water. The water flow is regulated to the coil based on outside air temperature while the electric heating coil is modulated based on room temperature.

The electrical room dampers are positioned so that the outside damper is fully open and the return air damper fully closed whenever the supply fan is not running, or the outside air temperature is greater than 73°F, or room temperature is greater than 97°F or the smoke mode switch in the Control Room is in the smoke position. Whenever the outside air temperature is below 73°F, the outside air damper is fully closed and the return air damper is fully open.

Whenever there is a loss of offsite power or an "S" signal actuation, the ventilation fans will be either manually or automatically started by temperature after they receive a permissive signal from the load sequencer.

Redundancy and Diversity

The instrumentation and controls of the safety trains are physically and electrically separated. Each safety train is powered from its associated safety bus.

Display Instrumentation

There is no display instrumentation for the emergency service water intake structure ventilation system except for fan status indicating lights and annunciators.

7.3.1.5.15 Diesel fuel oil system

Refer to Section 9.5.4 for a description of the Diesel Fuel Oil System, to Figure 9.5.4-1 for the system flow diagram, and to Figure 7.3.1-26 for the instrument logic and schematic diagrams. This system supplies the diesel generator day tank in order to maintain six hour fuel reserve for the associated diesel generator.

Initiating Circuits and Logic

Each diesel generator has a day tank, fuel oil transfer pump and storage tank associated with it. The fuel oil transfer pump can be remotely operated from the Control Room or locally from the diesel generator engine panel. A two position "local-remote" selection switch is provided on the engine panel for manual transfer of control. In the event of control room evacuation, the control of the pump will be automatically transferred to the engine panel via the transfer panel. The day tank has a supply inlet valve (solenoid operated) that can be manually operated in a similar manner to the fuel oil transfer pump.

The day tank will be automatically filled on low level or after the diesel generator is stopped and the tank level is not full.

Bypass, Interlocks and Sequencing

The fuel oil transfer pump will start on low level in the fuel oil day tank and will stop on full level. The supply valve will shut upon high-high level in the day tank in order to prevent flooding of the tank cubicle.

Redundancy and Diversity

Each diesel fuel oil system train is powered from the emergency bus that is fed-by its associated diesel generator. The instrumentation and controls of each train are physically and electrically separated. The redundancy and independence provided are adequate to maintain functional capabilities following the design basis shown in Table 7.3.1-1.

Display Instrumentation

The safety-related display instrumentation, which provides the operator with sufficient information to monitor performance of the Diesel Fuel Oil System and to perform the required safety functions, is shown in Table 7.5.1-3.

7.3.1.6 Design Basis Information

The safety-related instrumentation and controls of the Engineered Safety Features Systems and ESF supporting systems are designed to adequately perform their safety functions. The functional diagrams presented on Figure 7.3.1-1 provides a graphic outline of the functional logic associated with requirements for ESFAS. The design basis information required by Section 3 of IEEE-279-1971 "Criteria for Protection Systems of Reactor Generating Stations" is discussed in the following Sections 7.3.1.6.1, 7.3.1.6.2 and 7.3.1.6.3.

7.3.1.6.1 Automatically initiated ESF systems.

Applicable Systems:

a) Containment Heat Removal System

b) Containment Isolation System

c) Auxiliary Feedwater System

d) Emergency Exhaust System

e) Emergency Core Cooling System

Minimum Performance Requirements - Minimum performance requirements are as follows:

The engineered safety features actuation system response time is defined as the interval required for the engineered safety features sequence to be initiated subsequent to the point in time that the appropriate variables(s) exceed setpoints. The response time includes sensor/process (analog) and logic (digital) delay plus, the time delay associated with tripping open the reactor trip breakers and control and latching mechanisms. The values listed herein are maximum allowable times consistent with the safety analyses and are systematically verified during plant preoperational startup tests. These maximum delay times thus include all compensation and therefore require that any such network be aligned and operating during verification testing.

The Engineered Safety Features Actuation System is always capable of having response time tests performed using the same methods as those tests performed during the preoperational test program or following significant component changes. Response time testing contains the criteria of Section 14.2.12.1.11.

The response time ranges of the sensed variable and systems accuracies for the initiating signals are specified in Table 7.3.1-12. There is no time delay associated with transmitting the initiation signal from the ESFAS to the actuated component.

7.3.1.6.2 Manually Initiated ESF Systems - Combustible Gas Control Systems - Instrumentation and Control

The Combustible Gas Control System is a manually actuated system which is not governed directly by the requirements of IEEE-279-1971. However, the provisions of Section 3 will be used as a guide in the design of instrumentation and controls of the system as follows:

a) 3.1 Generating Station Conditions - Generating station conditions which require corrective action are excess hydrogen levels in the Containment following a beyond design-basis accident listed in Table 7.3.1-1.

b) 3.2 Generating Station Variables - The concentration of hydrogen in the containment atmosphere is monitored to provide indication of when corrective action is required.

c) 3.3 Sensor Number and Location - The number and location of hydrogen analyzer sample points from which samples can be drawn are given in Section 6.2.5.

d) 3.4, 3.5, 3.6 Limits, Margins and Levels - The operation limit, actuation set points and margins to operation are specified in Sections 6.2.5.2 and 6.2.5.3.

e) 3.7, 3.8 Abnormal Events - The system components are designed to function so that:

    1) The system provides a process capacity such that the containment hydrogen can be monitored in accordance with the guidance in Regulatory Guide 1.7, "Control of Combustible Gas Concentration in Containment."

2) Reliable power suppliers are provided to each redundant component.

3) The environmental conditions that accompany beyond design-basis accidents will not limit the ability of the system to perform its function. Acceptable environmental design conditions used as surrogate inputs in lieu of actual conditions are discussed in Section 3.11.

f) 3.9 Minimum Performance Requirements - The ranges and system accuracies are specified in Section 6.2.5.2.3.

7.3.1.6.3 ESF Supporting Systems

The ESF Supporting System I and C may be in operation during normal plant operation or plant shutdown. In addition, they are required to support the operation of the Engineered Safety Features Systems. The ESF Supporting System I and C conforms to the requirements of IEEE-279-1971 Section 3 as follows:

a) 3.1 Generating Station Conditions - The design basis events which require the supporting systems operate to support the ESF are specified in Table 7.3.1-1.

b) 3.2 Generating Station Variable - Generating station variables that are required to be monitored in order to initiate supporting system operation are given in Tables 7.3.1-2 and 7.3.1-3.

c) 3.3 Sensor Number and Location - The number and location of sensors are given in Tables 7.3.1-2 and 7.3.1-3. None of the variables referred to in 3.2 above are spatially dependent.

d) 3.4, 3.5, 3.6 Limits, Margins and Levels - The operational limits for appropriate variables are provided to the operator in the Plant Operating Manual. Operational limits for applicable variables were chosen with adequate margin from the level considered to mark the onset of unsafe conditions.

e) 3.7, 3.8 Abnormal Events - The redundant components are provided so that:

1) Any single failure will not prevent system actuation when required.

2) Independent power supplies are provided to each redundant supporting system component.

IEEE 279 Section 3 Applicability

a) 3.1 Generating Station Conditions - The design basis events requiring protective action are specified in Table 7.3.1-1.

b) 3.2 Generating Station Variables - Generating station variables that are required to be monitored in order to provide protective actions are given in Tables 7.3.1-2 and 7.3.1-3.

None of the variables referred to in 3.2 above are spatially dependent.

c) 3.3 Sensor Number and Location - The number and location of sensors are given in Tables 7.3.1-2 and 7.3.1-3.

d) 3.4, 3.5, 3.6 Limits, Margins and Levels - The operational limits for appropriate variables are provided to the operator in the Plant Operating Manual. Operational limits for applicable variables were chosen with adequate margin from the level considered to mark the onset of unsafe conditions.

e) 3.7, 3.8 Abnormal Events -The malfunctions, accidents, or other unusual events which could physically damage protection system components or could cause environmental changes are as follows:

1) Loss-of-coolant accident (see Chapter 15)

2) Steam line breaks (see Chapter 15)

3) Earthquakes (see Chapters 2 and 3)

4) Fire (see Section 9.5.1)

5) Explosion-hydrogen buildup inside Containment (see Section 5.2)

6) Missiles (see Section 3.5)

7) Flood (see Chapters 2 and 3)

Redundant components are provided so that;

1) A single failure will not prevent system actuation when required.

2) Independent power supplies are provided to each redundant actuated component.

3) The environmental conditions that accompany the design basis accident will not limit the ability of these systems to perform their safety function. The environmental design conditions are discussed in Section 3.11.

4) The systems are designed to withstand the loading conditions associated with the safe shutdown earthquake without loss of function as discussed in Section 3.10.

f) 3.9 Minimum performance requirements are as follows:

1) The response times and system accuracies for the initiating signals are specified in Table 7.3.1-12. There is no time delay associated with transmitting the initiation signal from the ESFAS to the actuated component.

2) The ranges of the sensed variables are specified in Table 7.3.1-12.

7.3.1.7 Final System Diagrams

Function block diagrams, instrument schematic and logic diagrams, and control wiring diagrams are provided in Figures 7.3.1-1 through 7.3.1-27 and Drawing CAR-2166-B-401.

7.3.2 ANALYSIS

The design of each of the Engineered Safety Features Systems and ESF supporting systems, including design bases and evaluation, is discussed in Chapters 6, 8, 9, and 10. The following analyses address the instrumentation and controls of the ESF and supporting systems.

7.3.2.1 Failure Modes and Effects Analyses (FMEA) (IEEE-352)

Failure modes and effects analyses have been performed on the ESFAS by Westinghouse within their scope of work (refer to Section 7.2.2 and Ref. 7.3.1-4, WCAP-8584/8670). The results verify that these systems meet protection single-failure criteria as required by IEEE Standard 279-1971. The Shearon Harris Nuclear Power Plant complies either physically or with analytical justification with the interface requirements of Appendix B of WCAP-8584/8670. This FMEA together with the assumption of compliance to the interface requirements of Appendix B and the considerations of Appendix C has applicability to engineered safety features equipment within NSSS and BOP scope and design changes subsequent to the design analyzed.

The failure mode and effects analyses for the Ebasco supplied ESF systems and ESF supporting systems are given in their respective FSAR sections as identified in Table 7.3.1-1.

Failure mode and effects analysis was used during system design. Control circuits were designed (schematics and logic diagrams) as follows:

a) The failure mode of each component was established.

b) The operation of the circuit under each failure mode established was analyzed and the results recorded.

c) When a circuit did not meet the single failure criteria the circuit was redesigned.

d) The above referenced tables represent each type of equipment now in the circuits, the failure modes, and the effects on circuit operation.

7.3.2.2 Compliance With Standards and Design Criteria

Discussions of GDC are provided in various sections of Chapter 7 where a particular GDC is applicable. Applicable GDC's include 13, 20, 21, 22, 23, 24, 25, 27, 28, 35, 37, 38, 40, 43 and 46. Compliance with certain IEEE Standards is presented in Section 7.1.2 and Table 7.1.0-1. Compliance with RG 1.22 is discussed in Section 7.1.2.5. The discussion given below demonstrates that the ESFAS complies with IEEE Standard 279-1971.

7.3.2.2.1 Automatic Initiation (IEEE-279 Section 4.1; GDC 20, IEEE 308, RG 1.32, and RG 1.106)

With the exception of the Combustible Gas Control System, all ESF systems and supporting systems are automatically actuated. The signals on variables which actuate each system are listed in Tables 7.3.1-2 and 7.3.1-3. The Combustible Gas Control System is manually actuated.

7.3.2.2.2 Single failure criterion (IEEE-279 Section 4.2; GDC 21, GDC 23, RG 1.53, RG 1.106, BTP 1CSB 18, IEEE 308, IEEE 379)

Compliance with single failure criteria is accomplished by providing redundancy of the instrumentation and control systems and by separating them (see Section 8.3.1.4) sufficiently to prevent single events from affecting more than one channel. The discussion in Section 7.2.2.2.3 is applicable to the ESFAS with the following exception. In the ESF, a loss of instrument power will cause actuation of ESF equipment controlled by the specific bistable that lost power (containment spray, RWST level and one channel of steam- line differential pressure excepted). The power supply for the protection systems is discussed in Section 7.6 and Chapter 8. For containment spray, the final bistables are energized to trip to avoid spurious actuation. In addition, manual containment spray requires a simultaneous actuation of two manual controls. This is considered acceptable because containment spray actuation on containment pressure (Hi-3) signal provides automatic initiation of the system via protection channels. Moreover, two sets (two switches per set) of containment spray manual initiation switches are provided to meet the requirements of IEEE Standard 279-1971. Also, it is possible for all ESF equipment to be individually manually actuated from the main control board. Hence, a third mode of containment spray initiation is available. The design meets the requirements of GDC 21 and 23.

The refueling water storage tank level bistables are normally de-energized, de-energize on loss of power, and must energize on lo-lo level to open the sump isolation valves (injection/recirculate mode switchover). Reference Figures 7.3.1-3, 7.6.1-5, and 7.6.1-6.

One channel of the steam line differential pressure input to AFW isolation bistables is energized "to trip" to avoid isolation of AFW isolation valves with a postulated loss of the "B" DC bus followed by feed line break and loss of off-site power. Loss of power to the "B" DC bus and loss of "B" AC bus will not cause completion of 2/3 logic to create inadvertent AFW isolation by failing one channel "to trip" and another channel "to deactivate." Actuation would still be achieved to isolate, if required, with the remaining third channel. Also, it is possible in normal operation to manually actuate AFW isolation from the main control board. This configuration is considered more acceptable than one causing inadvertent AFW isolation.

7.3.2.2.3 Quality of components and module (IEEE-279 Section 4.3, RG 1.30, and RG 1.106)

The Engineering and Construction Quality Assurance Program approved by the NRC and enforced during design component selection, testing and equipment fabrication, verifies that quality components and modules are used in the equipment.

1. Instrumentation and controls are heavy duty industrial type of standard design well proven by service in industry or in nuclear power plant applications.

2. Motor starters and breakers are effectively derated for motor starting applications, since their nameplate ratings are based on short circuit interruption capabilities as well as on continuous current carrying capabilities. Short circuit current interrupting capabilities are many times the starting current or the motors being started, so that normal duty does not begin to approach maximum equipment capability.

3. Normal motor starting equipment ratings include allowance for a much greater number of operating cycles than the system will demand.

7.3.2.2.4 Equipment qualification (IEEE-279 Section 4.4; GDC 21, IEEE-323, RG 1.106)

Refer to Section 3.10 and 3.11 for additional discussion of seismic and environmental equipment qualification.

7.3.2.2.5 Channel integrity (IEEE-279 Section 4.5; RG 1.29, RG 1.100, RG 1.106, IEEE-308, IEEE-344, BTP ICSB 10)

Type testing or analysis of components, separation of sensors and channels and qualification of cabling are utilized to ensure that the components and systems will maintain the functional capability required under applicable extremes of conditions relating to environment, energy supply, malfunction, and accidents. All Seismic Category I components have Seismic Category I supports and are located in Seismic Category I structures.

Loss of or damage to any one train will not prevent the required protective action. Components which must operate during or after a design basis accident are rated for the post-accident environment (see Section 3.11). Results of type tests are used to verify these ratings.

7.3.2.2.6 Channel Independence (IEEE-279 Section 4.6, GDC 22, RG 1.6, RG 1.75, IEEE-308, IEEE-384)

The discussion presented in Section 7.2.2.2.3, Channel Independence, 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.

Locations of components and associated cable runs for redundant I&C systems have been selected to provide physical separation to preclude a situation in which a single event could remove or negate a protective function. This includes separation at the containment penetration areas. See Section 8.3.1.4 for a discussion of physical separation criteria.

Electrical isolation of Class IE portions of circuits for non-Class 1E portions is accomplished through the use of isolation devices. The digital signals in Ebasco's scope are isolated through the use of special relays. Other isolation devices, for digital and analog signals are provided by Westinghouse and are described in Westinghouse references listed in Section 7.2.

7.3.2.2.7 Control and Protection Interaction (IEEE-279 Section 4.7, GDC24)

The I&C systems and components used to actuate and control operation of ESF systems and supporting systems during safe shutdown or post-accident conditions are not directly interconnected with any non-safety-related I&C systems.

Non-safety-related alarms and status indications which are generated by the safety-related I&C equipment are isolated by use of isolated contacts. No credible failure in the alarm or status indication systems will prevent the safety-related controls from properly performing any of their functions. Examples of these failures are fused contacts, open circuits, voltage spikes and grounds. The discussions presented in Section 8.3.1.2.30 are applicable.

In certain instances, digital non-class 1E (control) signals may provide input to digital class 1E circuits. Where non-class 1E control signals provide input to class 1E control circuits, a failure of the non-class 1E components will not affect the proper safety operation of the class 1E control circuits. The signal inputs from the non-class 1E devices which feed the class 1E circuits are through isolation devices and will be overridden by the class 1E portion of the safety circuits.

7.3.2.2.8 Derivation of system inputs (IEEE-279 Section 4.8)

Refer to the Section 7.2.2 for a discussion of derivation of system inputs for the ESFAS signals. Other parameters, which provide inputs to ESF and supporting systems I&C are identified in Tables 7.3.1-2 and 7.3.1-3. These inputs are derived from direct measurements of conditions indicating a need for the required system protective action.

7.3.2.2.9 Capability for sensor checks (IEEE-279 Section 4.9)

Refer to the Section 7.2.2.2.3 for a discussion of capability of checks of sensors providing input signals to the ESFAS logic.

For other sensors providing input signals for actuation of ESF and supporting systems, means are provided to check sensor operability either through comparative indications of redundant sensors measurement channels or by periodic testing of the sensors.

7.3.2.2.10 Capability for test and calibration (IEEE-279 Section 4.10; GDC 21, GDC 37, GDC 40, GDC 43, RG 1.22, RG 1.106, RG 1.118, IEEE 338, BTP 1CSB 22)

The methods and provisions for testing the Engineered Safety Feature (ESF) Actuation System at power are described below and allow essentially all the ESF to be tested with the plant in service, (see Section 7.3.2.2.10.7 for exceptions).

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

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

7.3.2.2.10.1 General testing program

The Engineered Safety Features Systems are tested to provide assurance that the systems will operate as designed and will be available to function properly in the unlikely event of an accident. The testing program meets the requirements of Criteria 21, 37, 40 and 43 of the GDC and Regulatory Guide 1.22. The tests described in Section 7.2.2.2.3 and further discussed in Section 6.3.4 meet the requirements on testing of the Emergency Core Cooling System as

stated in GDC 37 except for the operation of those components that will cause an actual safety injection.

The test, as described, demonstrates the performance of the full operational sequence that brings the system into operation, the transfer between normal and emergency power sources and the operation of associated cooling water systems. The safety injection and residual heat removal pumps are started and operated and their performance verified in a separate test discussed in Section 6.3.4. When the pump tests are considered in conjunction with the emergency core cooling system test, the requirements of GDC 37 on testing of the Emergency Core Cooling System are met as closely as possible without causing an actual safety injection.

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

a) Prior to initial plant operation a complete system test is conducted.

b) A complete system test will be conducted during each regularly scheduled refueling outage.

c) During normal operation with the Unit in service, essentially all of the engineered safety features components, analog, logic and actuation circuitry will be tested. For a listing of the exceptions, see Section 7.3.2.2.10.7.

d) During normal operation the operability of all testable final actuation devices of the Engineered Safety Features will be tested by manual initiation from the Control Room.

The following sections describe the testing circuitry and procedures for Item c of the General Testing Program given above.

During reactor operation the basis for engineered safety features actuation systems acceptability will be the successful completion of the overlapping tests performed on the initiating system and the Engineered Safety Features Actuation System, see Figure 7.3.2-1. Checks of process indications verify operability of the sensors. Analog checks and tests verify the operability of the analog circuitry from the sensor input through to and including the input relays and logic circuits of SSPS, except for the input relays and logic circuits associated with the containment spray function which are tested during solid state logic testing. Solid state logic testing checks the digital signal path from and including the input of the logic circuits 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 main control board indication and visual observation that the appropriate pump breakers close and automatic valves shall have completed their travel.

The basis for acceptability for the engineered safety features interlocks will be main control board indication of proper receipt of the signal upon introducing the required input at the appropriate setpoint.

7.3.2.2.10.2 Guidelines

a) The test procedures will not involve the potential for damage to any plant equipment.

b) The test procedures will not expose the plant to an increased potential for accidental tripping.

c) The provisions for on line testing will not complicate the engineered safeguards feature actuation circuits to the extent that their reliability will be degraded.

7.3.2.2.10.3 Description of initiation circuitry

Since several fluid systems comprise the total engineered safety features, each of which may be initiated by different process conditions and reset independently of each other, separate initiating circuits exist for the following systems in each of the two trains of the engineered safety features actuation circuitry:

a) Safety Injection System

b) Containment Isolation Phase A

c) Containment Isolation Phase B

d) Containment Spray System

e) Containment Ventilation Isolation

f) Main Steam Line Isolation

g) Main Feedwater Line Isolation

Each output 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 cabinets designated Train A and Train B respectively for the redundant counterparts. The master and/or slave relay circuits operate various pump circuit breakers, motor operated valve contactors and solenoid operated valves.

7.3.2.2.10.4 Circuit operation

Initiation of an engineered safety features function is accomplished by redundant process (analog) signals, each of which operates a bistable device which in turn drives two relays (A and B). One of these bistable relays is located in the Train A logic cabinet and the other in Train B. These logic cabinets are provided with separate relay compartments for each of the redundant analog channel protection set bistable relays. This relay input circuitry is provided in the solid state logic systems.

7.3.2.2.10.5 Analog testing

Analog testing is identical to that used for reactor trip circuitry described in Section 7.2.2.2.3. In the analog racks, bistable trip switches, proving lamps and analog test switches are provided.

Administrative control requires during bistable testing that the bistable output be put in a trip condition by its trip switch (exceptions noted below), which connects the proving lamp to the bistable and thus deenergizes (operates) the bistable output relays in Train A and Train B cabinets. Status lights in the Control Room verify the bistable relays have been de-energized and the bistable outputs are in the trip mode. Exceptions are containment spray, refueling water storage tank level and pressurizer pressure input to P-11 circuitry. Containment spray and refueling water storage tank level may be bypassed during analog testing as permitted by Technical Specifications. For containment spray, bypassed indication is provided in the Control Room. The input to permissive P-11 may be momentarily simulated below P-11 with the bistable not tripped to allow testing of P-11 since tripping of the pressurizer pressure input to P-11 causes it to fail high. Each of these test procedures is applied to one channel at a time.

The analog test switch is then operated and a signal is inserted through a test jack. Verification of the bistable trip setting is now confirmed by the proving lamp.

7.3.2.2.10.6 Solid State Logic Testing

After the individual channel analog testing is completed, the logic matrices are tested from the Train A and Train B logic rack test panels. This step provides overlap between the analog and logic portions of the test program. During this test, each of the bistable relay outputs are 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. During logic testing, bistable relays remain in their normal positions and can be actuated by a true signal.

7.3.2.2.10.7 Actuator Testing

At this point, testing of the initiation circuits through operation of the master relay and its contacts to the coils of the slave relays has been accomplished.

The engineered safety features logic slave relays in the solid state protection system output cabinets are subjected to coil continuity tests by the output relay tester in the solid state protection system cabinets. Slave relays (K601, K602, etc.) do not operate because of reduced voltage applied to their coils by the mode selector switch (TEST/OPERATE). A multiple position master relay selector switch selects the master relays and corresponding slave relays to which the coil continuity test voltage is applied. The master relay selector switch is returned to "OFF" before the mode selector switch is placed back in the "OPERATE" mode. However, failure to do so will not result in defeat of the protective function. The engineered safety features actuation system slave relays are activated during the testing by the on-line test cabinet, so that overlap testing is maintained.

The engineered safety features actuation system final actuation device or actuated equipment testing shall be performed from the engineered safeguards test cabinets. These cabinets are normally located near the solid state protection system equipment. There is one set of test cabinets provided for each of the two protection trains A and B. Each set of cabinets contains individual test switches necessary to actuate the slave relays. To prevent accidental actuation, test switches are of the type that must be rotated and then depressed to operate the slave relays. Assignments of contacts of 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 a safety injection actuation signal is initiated during the test of the final device that is actuated by this test, the device will already be in its safeguards position.

During this last procedure, close communication between the control room operator and the man at the test panel is required. Prior to energizing of a slave relay, the operator in the Control Room assures plant conditions will permit operation of the equipment which is actuated by the relay. After the tester has actuated the slave relay, the control room operator observes that all equipment has operated as indicated by appropriate indicating lamps, monitor lamps and annunciator on the control board, and in accordance with a prepared check list records all operations. He then resets all valves and pump breakers and prepares for operation of the next slave relay driven equipment.

By means of the procedure outlined above, all pumps and valves actuated by Engineered Safety Features initiation circuits are operated by the automatic circuitry, except for the following:

a) Main Steam Isolation -Air cylinder tripped valves are used for each main steam line. The valve is tested at cold shutdown frequency.

b) Feedwater Isolation - Air cylinder operated regulating and nitrogen cylinder operated main isolation valves are provided for each main feedwater line. Air operated, spring closed regulatory bypasses are also provided for each feedwater line. The operation of the feedwater regulating valves is continually monitored through operating procedures. The main feedwater isolation valve is tested at cold shutdown. Also excepted are the stroke testing of the feedwater pump discharge valves and the tripping of the feedwater pumps.

c) Reactor Coolant Pump Essential Service Isolation

    1) Component cooling water supply and return. The valves in these lines cannot be fully tested during normal operation.

    2) Seal water return header. These valves in this line cannot be fully tested during normal operation.

    The main reason for not testing these valves periodically is that the reactor coolant pumps may be damaged. Although pump damage from this type of test would not result in a situation which endangers the health and safety of the public, it could result in unnecessary shutdown of the reactor for an extended period of time while the reactor coolant pump or certain of its parts are replaced. This would place a great economic burden on Carolina Power & Light Company. They will be tested during scheduled reactor shutdowns (as permitted by Regulatory Guide 1.22) to assure that they can perform their intended function.

d) Auxiliary Feedwater Isolation - Closure testing of the Auxiliary Feedwater (AFW) isolation and flow control valves is not conducted at power to prevent isolation of AFW flow to the respective steam generators. This isolation could adversely affect plant response to a loss of feedwater or loss of offsite power event requiring AFW actuation. The valves would not automatically open in response to the event until the test signal was manually reset. The

valves are routinely tested during scheduled reactor shutdowns (as permitted by Regulatory Guide 1.22) to assure that they can perform their intended function.

Containment spray system pump tests will be performed periodically. The pump tests will be performed with the isolation valves in the spray pump discharge lines at the Reactor Auxiliary Building verified closed; the sodium hydroxide storage tank valves are also verified closed. The valves are tested with the pumps stopped.

Emergency core cooling system tests will be performed periodically during plant shutdown in accordance with the Technical Specifications with the Reactor Coolant System isolated from the Emergency Core Cooling System by closing the appropriate valves. A test safety injection actuation 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.

During normal power operation, the standby diesel generators can be started, manually synchronized with the preferred power supplies and loaded with certain ESF equipment. However, the entire sequence, from ESFAS signal to complete automatic loading of the diesel-generators cannot be accomplished during normal power operation.

All "actuation devices" will be tested during normal power operation, but not necessarily in the same sequence that would occur following an accident with concurrent loss of offsite power. ESF "actuated" equipment will be tested individually or in groups during normal power operation. These methods of testing are designed such that plant operation will not significantly be affected due to any unacceptable system perturbations.

Testing of the complete automatic loading sequences can be accomplished during plant shutdown conditions.

Manually operated control switches for S, CSAS, and T signals will be tested during plant shutdown conditions.

7.3.2.2.10.8 Actuator blocking and continuity test circuits

Those few final actuation devices that cannot be designed to be actuated during plant operation (discussed in Section 7.1.2.5) 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, the devices control circuit cabling, control voltage and the devices actuation solenoids. 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. If an accident occurs during testing, the automatic actuation circuitry will override testing as noted above. One exception to this is that if the accident occurs while testing a slave relay whose output must be blocked, those few final actuation devices associated with this slave relay will not be actuated; however, the redundant devices in the other train would be operational and would perform the required safety function. Actuation devices to be blocked are identified in Section 7.1.2.5.

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

The typical schemes for blocking operation of selected protection function actuator circuits are shown on Figure 7.3.2-2 as details A and B. The schemes operate as explained below and are duplicated for each safeguards train.

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

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

7.3.2.2.10.9 Summary

The description of the testing circuits and procedures as given above, presents the method of complying with Regulatory Guide 1.22.

The procedures described provide capability for complete testing, from the process signal to the logic cabinets and from there to the individual pump circuit breakers, valve starters or pilot solenoid valves including all field cabling actually used in the circuitry when called upon to operate for an accident condition. Those protective functions for which credit is taken in safety analysis in Chapter 15 and which are not tested at power, are given in Section 7.3.2.2.10.7 and 7.1.2.5. As required by Regulatory Guide 1.22, where actuated equipment is not tested during reactor operation, it has been determined that:

a) There is no practical system design which would permit operation of the actuated equipment without adversely affecting the safety or operability of the plant.

b) The probability of the protection system failing to initiate the operation of the actuated equipment is, and can be maintained, acceptably low without testing the actuated equipment during reactor operation.

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

Where the ability of a system to respond to a bona fide accident signal is intentionally bypassed for the purpose of performing a test during reactor operation, each bypass condition is automatically indicated to the reactor operator in the Control Room by a common "ESF testing" annunciator for the train test. Test circuitry does not allow two ESF trains to be tested at the same time, therefore extension of the bypass condition to redundant system is prevented. For the few devices whose testing during plant operation could seriously affect plant or equipment operation, the procedure provides for testing from the process signal to the logic rack and from there, low voltage application to output cables and circuit breakers and valve starter coil circuits.

The procedures require testing at various locations, as follows:

a) Analog testing is accomplished at the respective racks. Verification of bistable operation is done at the control room status lights or at the logic racks. Verification of bistable setpoint is done at the analog rack.

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

c) Testing of all pumps and valves is done at the test panel located in the vicinity of the solid state protection system logic racks, in combination with the control room operator.

d) Low voltage application to those devices that cannot be tested during normal plant operation is done at the same test panel mentioned in c) above.

7.3.2.2.10.10 Time required for testing

It is estimated that analog testing can be performed at a rate of several channels per hour. Logic testing is normally performed in approximately 1 hour and 30 minutes per train. Testing of actuated components (including those which can only be partially tested) will be a function of Control Room operator availability. It is expected to require several shifts to accomplish these tests. During this procedure automatic actuation circuitry will override testing, except for those few devices associated with a single slave relay whose outputs must be blocked and then only while blocked. It is anticipated that continuity testing associated with a blocked slave relay could take several minutes. During this time the redundant devices in the other trains would be functional.

7.3.2.2.11 Channel bypass and removal (IEEE-279 Section 4.11)

Equipment from one channel may be removed from service without affecting plant operation.

7.3.2.2.12 Operating bypasses (IEEE-279 Section 4.12)

There are no operating bypasses in the ESF and supporting I&C Systems, except for the bypass circuitry for the motor operated valves' thermal overload relays and torque switches in the event of an automated signal based on either Safety Injection, Phase “A” Isolation, Emergency Bus Undervoltage, Prog “A”, Prog “B” or Prog “C” signals through the sequencer.

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

7.3.2.2.13 Indication of bypasses (IEEE-279 Section 4.13, RG 1.47, RG 1.106, BTP ICSB 21)

Table 7.3.2-1 describes the indications available to the control room operator which allows him to determine if any part of the ESF Actuation System has been administratively bypassed or taken out of service.

In general, if any analog channel in the ESF Actuation System is taken out of service for any reason, the channel is placed in the tripped mode, and a channel trip status light is lit on the main control board. In addition, an alarm will sound and an associated annunciator panel light will be lighted. This holds true for the containment pressure channels associated with safety injection and steamline isolation functions. The channel bistable output relays associated with the containment spray and RWST Low-Low level functions are not tripped, but are bypassed for test and maintenance purposes. This reduces the possibility of inadvertent containment spray actuation or swapover from injection to recirculation mode, respectively. For containment spray, a status light indicating a bypassed condition is provided for each channel. For RWST Low-Low level, a bypassed condition status light is not provided. This is allowed by Regulatory Guide 1.47, section C.3.b, since the bypassed condition is not expected to occur more frequently than once per year. An annunciator indicating 2/4 channels bypassed for containment spray actuation is also provided.

In addition, status lights are provided to indicate opening of any protection racks, or the associated safeguards set cabinets, and it is alarmed (one per rack or cabinet per train) in the Control Room.

With respect to final actuators and components of the ESF Systems, a number of indications are provided, depending on the importance of the device.

a) For any circuit breaker or motor starter, red and green status lights are provided adjacent to the controller. If a breaker or motor starter is racked out for maintenance or any other reason, both status lights will be extinguished.

b) For critical functions, the plant design includes one, or a combination of the following indications to show the operator the status of plant systems and to highlight the existence of an incorrect configuration:

    1) Indication lights (red-open and green-closed) at the control switch for each valve.

2) A separate white monitor light indication grouped with lights for other devices having a similar function. The lights in the group are all on or are all off to provide for quick operator evaluation of systems status during any mode of plant operation.

3) Alarms (audible and visual) redundant to the above indications, which serve to alert the operator of the improper state, relative to plant conditions, of a critical device (pump, valve, etc.).

See Section 7.5 for a more detailed description of the above displays.

By looking at valve position indications, an operator can determine if any component (tank, pump, etc.) in the ESF Systems has been isolated or bypassed.

In addition to the foregoing information available to the operator, a separate "Bypass and Inoperable Status Panel" is located in the Control Room in clear view of the operator. Automatic indication is provided, on a system and train basis, for each bypass or deliberately induced inoperable status that meets all of the following conditions:

a) Renders inoperable any redundant portion of the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the systems it actuates to perform their safety-related functions.

b) Is expected to occur more frequently than once per year.

c) Is expected to occur when the affected system is normally required to be operable.

Additionally, manual capability exists in the Control Room to activate each system train level indicator.

The Design Criteria, or their equivalent, put forth in Branch Technical Position BTP 1CSB 21, dated 11/24/75, as found in Standard Review Plan - Appendix 7A, have been incorporated into the design of the Bypass and Inoperable Status Panel, (refer to Section 7.5).

7.3.2.2.14 Access to means for bypassing (IEEE-279 Section 4.14)

Access to means of bypassing or removal of components from the ESF and supporting systems is under administrative control.

7.3.2.2.15 Multiple set points (IEEE-279 Section 4.15)

There are no multiple set points in the I&C for the ESF and supporting systems.

7.3.2.2.16 Completion of action once it is initiated (IEEE 279 Section 4.16)

Once initiated, the ESF and supporting system protective action will go to completion. Deliberate operator action is required to interrupt operation once the systems have actuated automatically.

Upon initiation by loss of voltage, the diesel generator will start automatically and accept loads as described in Section 8.3.1. In the case of a safety injection actuation signal, the diesel generator will start automatically, but will not accept load if preferred power is available at the ESF bus. If preferred power is not available the diesel generator will accept the loads described in Section 8.3 and in the sequence defined in Table 8.3.1-2c.

The manual reset feature associated with containment spray actuation is provided in the design of the Solid State Protection System design for two basic purposes: first, the feature permits the operator to start an interruption procedure of automatic containment spray in event of false initiation of an actuate signal; second, although containment spray system performance is automatic, the reset feature enables the operator to start a manual takeover of the system to handle unexpected events which can be better dealt with by operator appraisal of changing conditions following an accident.

It is most important to note that manual control of the containment spray system does not occur, once actuation has begun, by just resetting the associated logic devices alone. Components will seal in (latch) so that removal of the actuate signal, in itself, will neither cancel or prevent completion of protective action or provide the operator with manual override of the automatic system by this single action. In order to take complete control of the system to interrupt its automatic performance, the operator must deliberately unlatch relays which have "sealed in" the initial actuate signals in the associated motor control center, in addition to tripping the pump motor circuit breakers, if stopping the pumps is desirable or necessary.

The manual reset feature associated with containment spray, therefore, does not perform a bypass function. It is merely the first of several manual operations required to take control from the automatic system or interrupt its completion should such an action be considered necessary.

In the event that the operator anticipates system actuation and erroneously concludes that it is undesirable or unnecessary and imposes a standing reset condition in one train (by operating and holding the corresponding reset switch at the time the initiate signal is transmitted) the other train will automatically carry the protective action to completion. In the event that the reset condition is imposed simultaneously in both trains at the time the initiate signals are generated, the automatic sequential completion of system action is interrupted and control has been taken by the operator. Manual takeover will be maintained, even though the reset switches are released, if the original initiate signal exists. Should the initiate signal then clear and return again, automatic system actuation will repeat.

Note also that any time delays imposed on the system action are to be applied after the initiating signals are latched. Delay of actuate signals for fluid systems lineup, load sequencing, etc., do not provide the operator time to interrupt automatic completion, with manual reset alone, as would be the case if time delay was imposed prior to sealing of the initial actuate signal.

7.3.2.2.17 Manual initiation (IEEE-279 section 4.17, RG 1.32, RG 1.62 IEEE-308)

All ESF and supporting systems may be actuated on a system or component level manually from the Control Room. Manual actuation on a system level of the safety injection actuation signal(s) will indirectly initiate through the SSPS logic the following protective signals: T, CRI, MFIS, and MSIS. Manual actuation of the Containment Isolation Signal (T) will also initiate a CVI signal indirectly through the SSPS logic. Manual activation of the Containment Spray

actuation signal will also initiate a CVI signal and a Containment Phase B signal indirectly through the SSPS logic.

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

7.3.2.2.18 Access to set point adjustments and calibrations (IEEE-279 section 4.18, RG 1.105)

Access to set point adjustments and calibrations for the ESF and supporting systems I&C required for system operation is under administrative control.

7.3.2.2.19 Identification of system operation (IEEE-279 section 4.19)

Operation of ESF and supporting system components is identified in the Control Room by key valve positions indicating lights, pump and fan operating lights and display of key system operating parameters such as flowrates, pressures, and temperatures. Refer to Section 7.5 for a discussion of the safety-related display information for ESF and supporting systems.

7.3.2.2.20 Information readout (IEEE-279 section 4.20)

Sufficient information is provided on a continuous basis so that the operator can have a high degree of confidence that the ESF and supporting systems are available and/or operating properly. Refer to Section 7.5 for a discussion of the specific safety-related display information provided.

7.3.2.2.21 System repair (IEEE-279 section 4.21)

Identification of a defective I and C channel or component is accomplished by observation of system indicators or status lights or by periodic testing. Replacement or repair of actuated components is accomplished as allowed by the Technical Specifications.

7.3.2.2.22 Identification (IEEE-279 section 4.22; IEEE-494)

Physical identification of redundant safety-related I and C and electrical components is described in Section 8.3.

7.3.2.2.23 Design of instrumentation and controls provided to accomplish changeover from injection to recirculation mode (BTP 1CSB 20)

The transfer from injection to recirculation is accomplished automatically when a low level signal 2/4 logic in the RWST is received (see Section 7.3.1.3.1.1).

7.3.2.2.24 Conformance to regulatory guide 1.7

The Combustible Gas Control System conforms to Regulatory Guide 1.7 in that controls and instruments are provided to allow the operator to manually initiate the Combustible Gas Control System and sample the hydrogen concentration.

7.3.2.2.25 Design criteria for auxiliary feedwater systems (BTP ICSB 13)

Auxiliary feedwater system I and C are designed with the required redundancy to meet single failure criteria for all design basis events and with the required diversity from AC and DC power sources. See Section 7.3.1.3.3.

7.3.2.2.26 GDC 17, 38, 41, 44

For compliance with General Design Criteria 17, 38, 41, and 44, see Section 3.1.

7.3.2.3 Further Considerations

In addition to the considerations given above, a loss of instrument air or loss of component cooling water to vital equipment has been considered. Neither the loss of instrument air nor the loss of component cooling water (assuming no other accident) can cause safety limits as given in Chapter 16 to be exceeded. Likewise, loss of any one of the two component cooling water trains will not adversely affect the core or the RCS, or will it prevent an orderly shutdown if this is necessary. Furthermore, all pneumatically operated valves and controls will assume a preferred operating position upon loss of instrument air or electrical power. For conservatism during the accident analysis (see Chapter 15), credit is not taken for the instrument air systems (except for safety-related portions) nor for any control system operability. Plant design 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 for a period of time (approximately ten 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. This time period presently is undetermined but if it cannot be substantiated, safety grade instrumentation will be provided to give reliable indication. See Section 5.4.1 for a detailed discussion on loss of component cooling water to the reactor coolant pumps.

The following two cases have been identified as incidences where instrument transmitters supplying information to more than one protection channel share a common instrument line or tap: (1) the Reactor Coolant System flow transmitters, three to each loop, (2) each steam generator where at each of two upper taps a steam flow transmitter is connected along with a narrow range steam generator water level transmitter. In the first case, the high pressure elbow tap for the three redundant Protection System Reactor Coolant System (RCS) flow transmitters is where the shared tap is located. Redundancy is not compromised by having a shared tap. If this tap were to break, the instrumentation would fail low which is in the direction of initiation of

protective action. If the shared tap is plugged, which is really not credible, the affected channels will remain static and the condition is easily detectable. In the second case, a failure of the common tap, either due to breaking or plugging, does not compromise redundancy or prevent automatic protective action if an initiating condition continued long enough to require protective action.

The protective action is provided either by 2/3 steam-generator low-low water level or by two channels of steam-feedwater flow mismatch due to low feedwater flow indication. For the discussion on this diverse protection, refer to Section 7.2.2.3.5 which gives recognition to the fact that the steam generator level signal used in the feedwater control originates separately from that used on a low S. G. water level signal which, in coincidence with the low feedwater flow signal, will trip the reactor. Protection from a control system action due to the failure of a steam generator water level or steam flow impulse line is provided by ensuring that common upper taps are only shared by the same channel instruments.

7.3.2.4 Summary

The effectiveness of the ESFAS is evaluated in Chapter 15, based on the ability of the system to contain the effects of ANS Condition III and IV faults, including LOCA and steam line break accidents. The ESFAS 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 ESFAS must detect ANS Condition III and IV faults and generate signals which actuate the ESF. The ESFAS 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 ESF. This includes the time required for switching and bringing pumps and other equipment to speed, and the time required for them to take load.

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

7.3.2.4.1 Loss-of-coolant protection

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

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

High containment pressure also actuates the ECCS. Therefore, emergency core cooling actuation can be brought about by sensing this other direct consequence of a reactor coolant system break, i.e., the ESFAS detects the leakage of the coolant into the Containment. The maximum actuation signal generation time of 2.0 seconds, after detection of the consequences of the accident, is adequate.

Containment spray will provide additional cooling of the Containment and also limit fission product release upon sensing elevated containment pressure (HI-3), to mitigate the effects of a LOCA.

The maximum delay time between detection of the accident condition and the generation of the actuation signal for these systems is assumed to be 2.0 seconds, well within the time capability of the protection system equipment to perform its safety function. 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 a LOCA.

7.3.2.4.2 Steam line break protection

The ECCS is also actuated in order to protect against a steam line break. Section 7.3.1.6.1 gives the time between occurrence of low steamline pressure, high containment pressure (for breaks in Containment) or high steam line pressure rate and generating of the actuation signal. Analysis of steam break accidents assuming this delay for signal generation shows that the ECCS is actuated for a steamline break in time to limit or prevent core damage for steamline break cases.

Additional protection against the effects of a steam line break is provided by feedwater isolation, which occurs upon actuation of the ECCS (the S signal). Feedwater line isolation is initiated in order to prevent excessive cooldown of the reactor vessel and thus protect the reactor coolant pressure boundary.

Further protection against a steamline break accident is provided by closure of all steamline isolation valves in order to prevent uncontrolled blowdown of all steam generators. The generation of the protection system signal (maximum 2.0 seconds) is again short compared to the time to trip the steamline isolation valves, which are designed to close in less than approximately 5.0 seconds.

In addition to actuation of the ESF, the effect of a steam line break accident is generation of a signal resulting in a reactor trip on overpower or following ECCS actuation. However, the core reactivity is further reduced by the highly borated water injected by the ECCS.

The analyses in Chapter 15 of the steam line break accidents and evaluation of the protection system instrumentation and channel design show that the ESFASs are effective in preventing or mitigating the effects of a steam line break accident.

REFERENCES: SECTION 7.3

7.3.1-1 Reid, J.B., "Process Instrumentation for Westinghouse Nuclear Steam Supply System (4 Loop Plant Using WCID 7300 Series Process Instrumentation," "WCAP-7913, March, 1973. (Additional background information only).

7.3.1-2 Katz, D.N., "Solid State Logic Protection System Description," WCAP-7488-L (Proprietary) and WCAP-7672 (Non-Proprietary), June, 1971. (Additional background information only).

7.3.1-3 Swogger, J.W., "Testing of Engineered Safety Features Actuation System, WCAP-7705, Revision 2, January 1976. (Information only; i.e., not a generic topical WCAP.)

7.3.1-4 Eggleston, F.T., Rawlins, D.H., and Petrow, J.R., "Failure Mode and Effects Analysis (FMEA) of the Engineering Safeguards Features Actuation System", WCAP-8584 (Proprietary), April, 1976, and WCAP-8760, Revision 1 (Non-Proprietary), February, 1980.

7.4 SYSTEMS REQUIRED FOR SAFE SHUTDOWN*

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

For a description of systems required for safe shutdown due to fire, refer to Safe Shutdown Analysis in case of fire (SSA).

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

a) Prevent the reactor from achieving criticality in violation of the Technical Specifications, and

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

The modes of shutdown are defined in Chapter 16 as follows:

Mode No.	Mode	Reactivity	% Rated	Avg. Coolant

*Further information is contained in the TMI Appendix.

		Condition, k_{eff}	Thermal Power[1]	Temperature
3.	Hot Standby	<0.99	0	≥ 350 F
4.	Hot Shutdown	<0.99	0	350 F > T avg. > 200 F
5.	Cold Shutdown	<0.99	0	≤ 200 F

7.4.1 DESCRIPTION

Functions required to achieve and maintain the above conditions of shutdown are:

a) Proper boration and reactor coolant inventory

b) Auxiliary feedwater supply

c) Removal of residual heat

7.4.1.1 Systems & Equipment Used for Modes of Shutdown

Systems and equipment used for the modes of shutdown include:

(Note: The equipment listed below which is preceded by an asterisk (*) is considered required for the mode of shutdown described. Equipment not preceded by the asterisk is desirable, but not required).

a) <u>Hot Standby</u>

* Auxiliary feedwater system

* Boric acid transfer pumps

* Steam generator safety valves (No I&C required)

Reactor Coolant Inventory Control (CVCS)

Letdown

* Charging

* Pressurizer heaters

Pressurizer sprays

* Steam generator power operated relief valves

Pressurizer power operated relief valves

Reactor Coolant Pump (with auxiliaries)

[1] Excluding decay heat

b) Hot Shutdown

* Auxiliary feedwater system
* Boric acid transfer pumps
* Steam generator PORV's

Reactor coolant inventory control (CVCS)

Letdown

* Charging
* Residual heat removal pumps (p < 363 psig)

Pressurizer heaters and sprays (if not solid)

Pressurizer power operated relief valves

Reactor Coolant Pump (with auxiliaries)

* Accumulator isolation valves

c) Cold Shutdown

* Residual heat removal system

Boric acid transfer pumps

Reactor coolant inventory control (CVCS)

Letdown

Charging

Supporting systems and associated equipment required for the modes of shutdown include:

* Component Cooling Water System
* Service Water System
* Onsite Power Supply System - diesel generators and batteries
* Diesel Generator Fuel Oil Storage and Transfer System
* HVAC Systems/Chilled Water for areas containing equipment required for the modes of shutdown
* Control Room Panels or Auxiliary Control Panel

* Emergency Lighting

7.4.1.2 Instrumentation and Control Systems

The instrumentation and control systems required for safe shutdown (i.e., those that are asterisked in above list), while they are not considered protective systems, conform to the applicable requirements of IEEE-279 to insure maximum reliability. The basic factors which are considered in the design are:

a) No single failure will prevent or inadvertently terminate a required control function. Instrument redundancy is applied at subsystem level (i.e., train A and B of a particular system are redundant to each other) so that redundancy is not required within one train.

   For application of the single failure criteria for the residual heat removal system inlet isolation valves, see Section 5.4.7.

b) Systems required for safe shutdown can be periodically tested during normal operation whenever possible to do so without adverse effect on plant safety or availability.

c) The equipment essential to the shutdown modes are designed to withstand design basis earthquake loads in combination with other loads, as specified in Section 3.10, without loss of their safety function.

d) The Control Room is designed to be available at all times. However, if continued occupancy of the Control Room is impossible, a separate auxiliary control panel (ACP) will be used to achieve and maintain hot standby. The reactor can be brought to cold shutdown from the Control Room, and, if necessary, from outside the Control Room.

7.4.1.3 Auxiliary Feedwater System

The auxiliary feedwater system design is described in Section 10.4.9 and shown on Figures 10.1.0-3, 10.1.0-4 and 9.2.1-1. The system consists of two motor driven and one steam turbine driven pumps with associated valves, piping and instrumentation. The actuation logic is shown on Figures 7.3.1-9 and 7.3.1-10.

When in a shutdown condition, manual initiation of the selected auxiliary feedwater pumps is required. This is accomplished by using the manual control switches provided on the main control board (MCB) or the auxiliary control panel (ACP). Auxiliary feedwater flow indication is provided on the MCB and ACP for each steam generator. Steam generator level and feedwater flow is controlled by remote manual control of the auxiliary feedwater regulating valves. The two motor driven pumps and their associated controls are redundant and powered from safety train A and B respectively. In case of loss of offsite power source, the emergency diesel generators will supply power for the auxiliary feedwater pump motors.

The auxiliary feedwater pump turbine is driven by steam supplied from the main steam piping of two steam generators (1B & 1C). Control of the motor operated turbine stop valve is provided on the MCB and ACP. The auxiliary feedwater pump turbine speed is automatically controlled to maintain a preset differential between the pump discharge pressure and the turbine steam inlet pressure. Manual speed control is also provided at both locations (MCB and ACP).

Since the auxiliary feedwater pumps take suction from the condensate storage tank (CST), redundant Class 1E level transmitters are provided on the tank in order to provide the status of the tank inventory. If the "empty" water level setpoint is reached, an alarm will be annunciated in either the Control Room or on the auxiliary control panel alerting the operator of the need to switchover the auxiliary feedwater suction from the CST to the emergency service water system. This switchover, if needed, is performed manually from control switches located on the MCB or ACP. The alarm level will allow sufficient water for 20 minutes of operator action. For a discussion of the CST and the auxiliary feedwater requirements, refer to Section 9.2.6 and 10.4.9, respectively. For a discussion of service water capability, refer to Section 9.2.1.

All essential monitoring instruments are listed in Tables 7.4.1-1 and 7.4.1-2.

a) Initiating Circuits

For ANS Condition I type of occurrences, such as normal shutdown, no automatic control of the auxiliary feedwater pumps is provided. Auxiliary feedwater is supplied to each steam generator by manually starting the selected auxiliary feedwater pump. Feedwater flow control is also accomplished manually, until the desired flow and steam generator level is reached. For shutdown during ANS Condition II type of events (incidents of moderate frequency), the following signals are used in addition to the manual control for automatic start-up of the auxiliary feedwater pumps (see Figures 7.3.1-9 and 7.3.1-10).

1) Motor Driven Pumps

   a) Loss of both main feedwater pumps

   b) Low-low level in any steam generator

   c) Loss of offsite power

   d) Safety injection signal

2) Turbine Driven Pump

   (Note: The following initiating signals are bypassed on transfer to the ACP (train-specific)).

   a) 2/3 low low level in any two steam generators

   b) Loss of offsite power

In case of ANS Condition III (infrequent incidents) or ANS Condition IV (limiting faults) type of events, the Auxiliary Feedwater System is operated as part of the ESF system as described in Section 7.3. Definition of ANS Conditions I, II, III, & IV is given in American National Standard, ANSI-N18.2 Chapter 2.1 "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants".

b) Bypasses

If the system is intentionally bypassed or made inoperable, it will be indicated in the Control Room in accordance with Regulatory Guide 1.47 (see Section 7.5).

c) Interlocks

No interlocks are provided for normal (ANS Condition I) shutdown. In the event of loss of offsite power, the motor driven auxiliary feedwater pumps are interlocked with the sequencer. After establishing the emergency onsite power by starting the diesel generators, the motors will start after the permissive signal is generated by the sequencer. The sequencing cycle is shown in Section 8.3.

d) Redundancy

The two motor driven pumps are redundant to the steam turbine driven pump. Each pump has separate and independent instrumentation and control circuitry. Safety-related 125V DC power is provided (see Section 8.3) for the turbine driven auxiliary feedwater pump control.

The two motor driven auxiliary feedwater pump controls are powered from separate 125V DC safety buses, which are redundant to each other (SA & SB). Initiating signals for the separate trains are redundant with the exception of loss of main feedwater pump signal, which is generated through a non-safety system.

e) Diversity

Auxiliary feedwater system diversity requirements are met by using motor and steam turbine drives. Actuation signal diversity requirements are met by virtue of different actuation methods:

1) Manual

2) Automatic - Initiating signals that start turbine and motor driven pumps (see Section 7.3. for automatic start description).

f) Supporting System

Class IE electrical systems are required for controlling the operation of the Auxiliary Feedwater System.

g) Portion of System not Required for Shutdown

Instrumentation used to generate signals for the annunciator on the MCB and computer is not necessary for shutdown.

h) Design Basis Information

The design bases of the auxiliary feedwater pump system control as used for shutdown are provided below and correspond to the requirements of Section 3 of IEEE 279-1971:

Basis 1: The generating station condition which requires protective action;

a) For ANS Condition I events, the Auxiliary Feedwater System (AFS) is initiated and controlled manually.

b) For ANS Condition II events, the AFS is initiated either manually or automatically and controlled manually.

c) For ANS Condition III and IV events, the AFS is controlled as part of the ESF system (see Section 7.3).

Basis 2: The generating station variables that are required to be monitored in order to provide protective actions are discussed in Section 7.3.

The process variables to be monitored during safe shutdown are listed in Table 7.4.1-1.

Basis 3: Not applicable, the process variables of the AFS have no spatial dependence.

Basis 4: The operational limits for variables listed in Basis 2 in applicable reactor operation modes are provided to the operator in the Plant Operating Manual.

Basis 5: Operational limits for applicable variables were chosen with adequate margin from the level considered to mark the onset of unsafe conditions.

Basis 6: The level that, when reached, will require protective action is loss of feedwater flow.

Basis 7: The range of transient and steady-state conditions of both the energy supply and the environment during normal, abnormal, and accident circumstances throughout which the system must perform are factored into the design of the control equipment used.

The control equipment is designed to the pressure, temperature, and humidity environment given in Section 3.11. The Class IE Power System is discussed in Chapter 8.

Basis 8: The Auxiliary Feedwater System is designed to withstand the effects of design basis earthquake without loss of function. The system components are physically located to prevent loss of function from missile damage.

Basis 9: Minimum performance requirements, including system response times, system accuracies, ranges and rates of change of sensed variables, to be accommodated until proper conclusion of the protective action is assured;

a) For ANS Condition I events the initiation of the AFS is conditional and the responsibility of the operator. Therefore manual operation is sufficient.

b) For ANS Condition II events two cases are possible:

   i. The AFS is not necessarily required, the initiation is dependent on the judgement of the operator. Manual operation is acceptable.

ii. The AFS is automatically started. The maximum time lag during the worst case situation (steam generator water level--low-low), is less than or equal to 61.5 seconds for pump to be up to speed, which is acceptable considering the steam generator inventory.

The inventory of the steam generators is sufficient to allow manual control of auxiliary feedwater flow in credible cases.

ANS Conditions III and IV events are discussed in Section 7.3.

i) Drawings

Figures 7.3.1-9 and 7.3.1-10 show the control logics for the Auxiliary Feedwater System (AFS).

7.4.1.4 Boric Acid Transfer System (Part of CVCS)

The Boric Acid Transfer System provides the means to change the boron inventory of the Reactor Coolant System (RCS) as required for achieving and maintaining reactor shutdown condition. A description of the Boric Acid Transfer System is provided in Section 9.3.4. (See Technical Specifications, Chapter 16, for boration control limiting conditions of operation.) The boric acid transfer pumps and associated valving are controlled through the Reactor Make-Up Control System described in Section 9.3.4.

The following discussion is limited to the boric acid transfer pump operation during shutdown. Charging pumps are discussed in Section 7.4.1.5.

a) Initiating circuits

The boric acid pumps are operated when boron addition to the RCS is required. Moreover, the pumps are also run to fill the refueling water storage tank, mix the boric acid tank, fill the boric acid tank from the batching tank, and for a normal volume control tank makeup. These pumps can be manually started or stopped, if required, by their own control switches, either from the MCB or ACP.

b) Bypasses

No bypass indication is provided.

c) Interlocks

No interlocks are involved in the manual control system.

d) Redundancy

Two independent boric acid transfer pumps are provided, either of which can supply the necessary boric acid for safe shutdown condition.

e) Diversity

No diversity is provided for boric acid pump control.

f) Supporting System

The boric acid transfer pumps and controls are powered from independent Class IE safety buses.

g) Portion of System not Required for Shutdown

The instrumentation used to monitor the Boric Acid Transfer System (excluding the boric acid tank Level Indicator LI-0161.2 on the ACP), alarms for the annunciator on the MCB and computer, and automatic pump control are not necessary for shutdown.

h) Design Bases Information

Although the Boric Acid Transfer Pumps are not considered a protection system, the design bases of the above pump control as used for shutdown are provided below and correspond to the requirements of Section 3 of IEEE 279-1971.

Basis 1: Prolonged hot shutdown or cold shutdown are the station conditions requiring protective action for compensating the effect of Xenon decaying.

Basis 2: Process variables to be monitored are listed in Table 7.4.1 1.

Basis 3: The monitored process variables of the Boric Acid Transfer System have no spatial dependence.

Basis 4: The operational limits for variables listed in Basis 2 in applicable reactor operation modes are provided to the operator in the Plant Operating Manual.

Basis 5: Operational limits for applicable variables were chosen with adequate margin from the level considered to mark the onset of unsafe conditions.

Basis 6: Reactivity changes due to poison decay require the operation of the Boric Acid Transfer System.

Basis 7: Safety Class IE power systems are discussed in Chapter 8. The equipment is designed for the pressure, temperature and humidity environment given in Section 3.11.

Basis 8: The manual boric acid transfer pump control system is designed to withstand the effects of design bases earthquake without loss of function. The system components are physically located to prevent loss of function from missile damage.

Basis 9: The boric acid transfer pumps are required only for extended safe shutdown (either for cold shutdown or for maintained hot shutdown over 8 hours), therefore manual operation is sufficient.

Basis 10: Boric acid pumps are not operated in parallel, without the boric acid tank recirc line orifice bypass valve open, due to the potential to "dead-head" the weaker pump, in accordance with NRC Bulletin 88-04.

i) Figure 7.4.1-1 is the logic diagram of boric acid transfer pump.

7.4.1.5 Reactor Coolant Inventory - Charging Pumps

During shutdown the charging system is required to maintain reactor coolant inventory and increase or decrease boron concentration as necessary. Normal operation of the charging system is described in Section 9.3.4. Reactor coolant inventory is automatically controlled through the pressurizer level controller so that the level is always maintained above the pressurizer heaters.

The adjustment of boron concentration during the modes of shutdown is accomplished by blending demineralized water with borated water through the volume control tank (VCT), or directly to charging pump suction bypassing the VCT. Manual control is provided both on the MCB and ACP. During normal shutdown conditions, charging flow is regulated by a flow control valve. If this valve is not available for automatic or remote manual operation, operators will manually control the charging control bypass valve to maintain pressurizer level. A detailed description of the charging system and its operation and safety evaluation is provided in Section 9.3.4. Another option that can be considered is local manual operation of the charging flow control valve bypass. This option may be used if conditions at the bypass valve allow access. If this option is used, the operator at the valve will be in communication with the main control room or the ACP.

The following discussion is limited to the charging pump on-off control requirements for shutdown:

a) Initiating Circuits

For safe shutdown service, the charging pumps can be controlled manually either from the MCB or ACP.

b) Bypass

No bypass of the manual controls is provided other than maintenance provisions. If the system is bypassed or inoperable, it will be indicated in the Control Room in accordance with Regulatory Guide 1.47. (see Section 7.5).

c) Interlocks

There are no interlocks associated with the manual controls.

d) Redundancy

Three separate charging pumps are provided. Two charging pumps and their controls are powered from two separate Class IE buses. The third can be powered from either of these two Class IE buses. The single failure criterion of electrical power supply systems is met by selecting the appropriate power train for the third pump.

e) Diversity

No diversity is provided for charging pump control.

f) Supporting System

The charging pump motor on-off controls are powered from Class IE power system (See Chapter 8 for details).

g) Portion of System not Required for Safe Shutdown

The instrumentation used to monitor the charging pump operation (except indicating lights), alarms for the annunciator on the MCB, and computer, and the automatic charging pump control through the pressurizer level controller, is not required for safety.

h) Design Bases Information

Although the charging pump control is not considered a protective system, the design bases of the charging pump control as used for shutdown are provided below and correspond to the requirements of Section 3 of IEEE 279-1971.

Basis 1: The operation of the charging system during shutdown with or without offsite power is required on low pressurizer level following a reactor trip.

Basis 2: Process variable to be monitored are listed in Table 7.4.1-1.

Basis 3: The monitored process variables have no spatial dependence.

Basis 4: The operational limits for variables listed in Basis 2 in applicable reactor operation modes are provided to the operator in the Plant Operating Manual.

Basis 5: Operational limits for applicable varibles were chosen with adequate margin from the level considered to mark the onset of unsafe conditions.

Basis 6: Reactivity changes due to poison buildup and decay and reactor coolant inventory changes require the operation of the charging pumps.

Basis 7: Safety Class IE power supply is discussed in Chapter 8. The equipment is designed for the pressure, temperature and humidity environment given in Section 3.11.

Basis 8: The charging pump manual control system is designed to withstand the effects of SSE without loss of function. The system is designed, and its components located, to prevent loss of function from missile damage.

Basis 9: The charging pumps are required for a extended safe shutdown. Manual control and operation is sufficient.

i) Drawings

Figure 7.4.1-2 is the logic diagram of the charging pumps.

7.4.1.6 Reactor Coolant Inventory - Letdown Orifice Isolation Valves

Letdown and charging are employed to maintain proper reactor coolant inventory during all phases of plant operation including shutdown. The system is needed for economical and/or operational reasons but is not required for safety. The charging rate is automatically controlled

by pressurizer water level. The letdown rate, however, is manually adjusted by selecting the proper combination of letdown orifices in the letdown flow path. If the make-up system is not in operation, the pressurizer water level can be maintained above the heaters by closing the letdown isolation valves. This is accomplished by manual closure of the valves. A detailed description of the letdown system is provided in Section 9.3.4.

a) Initiating Circuits

For safe shutdown the letdown isolation valves are operated manually on-off, if required. Manual controls are provided both on the main control board and auxiliary control panel.

b) Bypass

No bypass indication is provided.

c) Interlock

There are no interlocks provided.

d) Redundancy

Redundant isolation valves are provided powered from separate safety Class IE electric buses.

e) Diversity

There is no diversity between the redundant isolation valve controls.

f) Supporting System

The letdown isolation valve controls are powered from the Class IE power system (see Chapter 8 for details).

g) Portion of System not Required for Safe Shutdown

The instrumentation used to monitor the letdown system and alarms for the annunciator on the MCB and computer are not necessary for shutdown.

h) Design Bases Information

Although during shutdown the letdown isolation valve controls are not considered a protective system, they conform to the following bases in Section 3 of IEEE 279-1971.

Basis 1: Low pressurizer level with or without offsite power requires the operation of the letdown isolation valves.

Basis 2: Process variables to be monitored are listed in Table 7.4.1-1.

Basis 3: The monitored process variables have no spatial dependence.

Basis 4: The operational limits for varibles listed in Basis 2 in applicable reactor operation modes are provided to the operator in the Plant Operating Manual.

Basis 5: Operational limits for applicable variables were chosen with adequate margin from the level considered to mark the onset of unsafe conditions.

Basis 6: Low level in pressurizer requires the operation of the letdown isolation valves.

Basis 7: The Class IE power system is discussed in Chapter 8. The equipment is designed for the pressure, temperature and humidity environment given in Section 3.11.

Basis 8: The controls of letdown containment isolation valves are designed to withstand the effects of SSE without loss of function. The system is designed and its components are physically located to prevent loss of function from missile damage.

Basis 9: During safe shutdown the response of the Reactor Coolant System is relatively slow. Manual operation is sufficient.

i) Figure 7.4.1-3 is the logic diagram for the letdown orifice isolation valve.

7.4.1.7 Steam generator safety and power operated relief valves

The steam generator safety and power operated relief valves, described in Section 5.4.13, consist of the following:

Fifteen spring operated safety valves (5 per steam generator). These valves are safety-related valves, located upstream of the main steam isolation valves, and function during hot standby to provide overpressure protection for the steam generator and overtemperature protection for the RCS if the power operated relief valves are not available. These valves contain no instrumentation and control features and are completely self-regulated.

A main steam power operated relief valve is installed on each steam generator main steam line upstream of the main steam isolation valve outside the Containment. These power operated relief valves, while they are not required to operate during hot standby, will be operated as necessary to maintain the reactor coolant at the desired temperature.

The power operated relief valves are automatically controlled by main steam pressure. The valves are designed to fail closed on loss of power and are connected to safety buses for maximum reliability. Manual/automatic control stations are located on the MCB and the ACP for use when bringing the plant from hot standby to cold shutdown from inside or outside of the Control Room. The status of the power operated relief valves is indicated by opened and closed indicating lights and by the controller output indication. Refer to FSAR Section 3.6A.3.2 for further information.

a) Initiating Circuits

No initiating circuits are required for the self-actuating main steam safety relief valves.

The power operated relief valves are controlled through a pressure controller and can be manually actuated by selecting the manual mode. The required instrumentation readout for manual system control is tabulated in Table 7.4.1-1.

b) Logic

No logic is required for the spring loaded main steam safety valves. The power operated relef valve is controlled by its own pressure control loop or operated manually through the controller.

c) Bypass

No bypass is provided. Placing the power operated relief valves on manual mode does not preclude the steam relief functional requirements since the spring loaded main steam safety relief valves are capable of providing the steam pressure relief capacity.

d) Interlock

No interlock is provided.

e) Redundancy

Redundancy is accomplished on a limited system basis. Hot standby can be accomplished with one steam generator and associated relief valves (the set of spring loaded valves or one power operated relief valve is sufficient to provide heat removal requirements).

f) Diversity

Diversity is accomplished by the spring loaded main steam safety relief valves and power operated relief valves.

g) Supporting System

The controls of the power operated relief valves are powered from Class IE buses.

h) Portion of system not required for safety

The alarms to the station annunciator and indicating signals to the computer are not required for safety.

i) Design bases information

Section 3 of IEEE 279-1971 does not apply because the main steam safety relief valves are spring-loaded, self-actuated type. The power operated relief valves are not required for hot standby.

j) Drawings

Figures 7.4.1-4, 7.4.1-5, and 7.4.1-6 show the control scheme for the safety-related power operated relief valves on each main steam line from the steam generators.

7.4.1.8 Residual Heat Removal System (RHRS)

The Residual Heat Removal System is designed to remove residual heat from the core and reduce the temperature of the Reactor Coolant System during the plant cooldown to cold shutdown condition. The system is permitted to be manually initiated when the reactor coolant indicated shutdown temperature and pressure are reduced to 350°F and 363 psig or below.

The rate of heat removal is manually controlled by regulating the reactor coolant flow through the residual heat removal exchanger. An automatically operated bypass valve is provided to adjust the bypass flow keeping the total flow constant. Manual control capability is provided both on the main control board (MCB) and auxiliary control panel (ACP) for the system operation.

A detailed discussion of the RHR System is provided in Section 5.4.7.

a) Initiating circuits

The RHRS is permitted to be controlled manually either from the MCB or ACP when RCS temperature < 350°F and indicated pressure ≤ 363 psig,

b) Bypasses

Placing the RHR heat exchanger bypass valve on the manual mode will bypass the automatic flow totalization. System bypass or inoperable status indication is provided in the control room in accordance with RG 1.47 (see Sections 7.2.1.6 and 7.5.1.9).

c) Interlocks

The RHRS inlet isolation valves are interlocked in such a manner that the operator is not able to open them as long as the indicated reactor coolant system pressure is greater than or equal to 363 psig. For a discussion on the RHRS inlet isolation valves see Sections 7.6 and 5.4.7 for application of the single failure criteria.

The valves additionally provide alarms when RCS pressure is high and any valve is not shut. For decreasing flow, a flow switch located on the RHR pump discharge will open the motor operated recirculation valves assuring that pump minimum flow requirement is satisfied. No interlock is provided for the pump operation.

d) Redundancy

Two independent residual heat removal pumps are provided, either of which can provide the necessary heat removal capacity to the Reactor Coolant System for the safe shutdown condition. The two RHR pumps are powered from two separate Class IE buses.

e) Diversity

For opening permissives diverse RCS pressure transmitters by different manufacturers are used. There is no other diversity in the RHR system control.

f) Supporting System

The RHR system controls are powered from Class IE buses (see Chapter 8 for details).

g) Portion of System not Required for Safety

Instrumentation used to monitor the RHR system performance (except RHR pump status lights and RHR pump motor ammeter which are associated with the safety pump control) and alarm signals for the annunciator on the MCB and computer are not required for safety.

h) Design Bases Information

Although the RHRS is not considered a protection system, the design bases as used for shutdown are provided below and correspond to the requirements of Section 3 of IEEE 279-1971.

Basis 1: During safe shutdown the Residual Heat Removal System is required to remove residual decay heat from the reactor core and heat transferred to the reactor coolant by the reactor coolant pumps. This heat load is removed by cooling the reactor coolant through the RHRS.

Basis 2: Process variables to be monitored are listed in Table 7.4.1-1.

Basis 3: The monitored process variables have no special dependence.

Basis 4: The operational limits for variables listed in Basis 2 in applicable reactor operation modes are provided to the operator in the Plant Operating Manual.

Basis 5: Operational limits for applicable variables were chosen with adequate margin from the level considered to mark the onset of unsafe conditions.

Basis 6: Not applicable, as the RHRS is used to achieve cold shutdown from an already safe hot shutdown condition.

Basis 7: The Class IE power system is discussed in Chapter 8. The equipment is designed for the pressure, temperature, and humidity environment given in Section 3.11.

Basis 8: The controls of RHR system are designed to withstand the effects of SSE without loss of function. The system is designed, and its components are physically located, to prevent loss of function from missile damage.

Basis 9: During safe shutdown manual operation of the RHR system control is sufficient.

i) Figure 7.4.1-7 is the logic diagram for the RHR pumps. Figures 7.6.1-1 and 7.6.1-2 are the logic diagrams for the RHR isolation valves.

7.4.1.9 Primary Coolant Pressure Control (Pressurizer Heaters and Spray)

The reactor coolant system pressure is maintained by heaters in the water region and sprays in the steam region of the pressurizer.

The heaters and spray control valves are on automatic control during normal operation with manual override. The control system is non-safety-related as the heaters and spray are not required for safety.

a) Initiating Circuits

All four of the pressurizer heater groups (A, B, C, and D) can be automatically or manually controlled by positioning the selector switches on the main control board (MCB) to the required position.

In the automatic position the heaters are initiated by the following signals:

1) Low pressure in the pressurizer.
2) High level deviation from the programmed level setpoint.

All four heater groups (A, B, C, and D) can be manually turned on from the MCB. Heater groups A & B have separate control switches on the auxiliary control panel (ACP) providing control capability during emergency. The two spray valves are normally on automatic with manual control capability.

b) Bypass

No bypasses are provided for the backup pressurizer heaters on ACP control. The heaters are blocked on MCB control as discussed in item c) below. The control of the two spray valves can be placed on manual mode bypassing the automatic signals. Open and closed positions of the valve are indicated on the MCB and ACP.

c) Interlocks and Logic

All pressurizer heater groups are interlocked with pressurizer low level signal to prevent the operation of the heaters without sufficient cooling. For groups A and B this interlock is bypassed when the control is transferred to the ACP.

d) Redundancy

Two redundant backup heater groups (A and B) are provided, either of which can provide the necessary heat input to the Reactor Coolant System during safe shutdown. The two redundant backup heater groups are normally powered from two independent non-safety power sources, but can be manually connected to safety-related buses.

e) Diversity

No diversity of control is provided.

f) Supporting Systems

Heaters are fed from non-safety selected buses. The backup heater groups (A and B) can be powered from the safety electrical buses which, in turn, are powered from the two redundant diesel-generators.

g) Portion of Systems not Required for Safe Shutdown

The group C and D pressurizer heaters and the spray valves are not required for safe shutdown.

h) Design Bases Information

The pressurizer heaters and spray controls are not safety-related and, as such, do not comply with the design bases of IEEE 279-1971.

i) Figures 7.2.1-1 sheet 11 and sheet 12 are the function diagrams for the pressurizer spray valves and pressurizer heaters, respectively.

7.4.1.10 Supporting Systems For Safe Shutdown

The other systems required to achieve and maintain the generating station in the safe shutdown condition are:

a) Component Cooling Water System (Section 9.2.2).

b) Service Water System (Section 9.2.1).

c) Portions of the Onsite Power System (Section 8.3).

d) Diesel Fuel Oil Storage and Transfer System (Section 9.5.4).

e) Control Room Area Ventilation System (Section 9.4.1).

f) Reactor containment fan coolers (Section 6.2.2).

g) HVAC Systems for areas containing equipment required for the modes of shutdown (Section 9.4.0)

h) Accumulator Isolation Valves (Section 7.6.1.2).

i) Chilled Water System (Section 9.2.8).

j) Emergency Lighting (Section 9.5.3).

k) Reactor Coolant Pump (Section 5.4).

These systems are normally operating continuously except for the diesel generators and diesel fuel oil systems.

The instrumentation and controls for these systems are described in the respective sections noted above. Further discussion of the actuation and controls for the Engineered Safety Features Systems is provided in Section 7.3.

7.4.1.11 Safe Shutdown From Outside the Control Room

If temporary evacuation of the Control Room is required, the operator can establish and maintain the station in safe shutdown condition from outside the Control Room from the Auxiliary Control Panel (ACP), Auxiliary Transfer Panels (ATPs), and essential local control stations. The prime intent of the ACP and ATPs is to enable the operators to achieve and maintain hot standby condition. For a description of systems required due to control room fire, refer to Safe Shutdown Analysis in case of fire (SSA).

Two transfer and two auxiliary transfer panels (A-SA and B-SB) are provided for the two electrical safety trains, SA and SB. Their function is to transfer the control by isolating the controls at the MCB and activate the controls of the respective safety equipment on the ACP and ATPs. The transfer panels are designed as enclosed cabinets and all relays are mounted inside with locking type rear doors for access. Opening of any cabinet door activates an alarm on the MCB. The ACP and the four transfer panels are designed in accordance with Class IE requirements IEEE 323-1974 and 344-1975.

The transfer is initiated manually by transfer relays provided on the transfer panels and auxiliary transfer panels. However, before leaving the Control Room, the operator should trip the reactor.

The ACP, two transfer panels, and two auxiliary transfer panels are located on Elevation 286 ft. in the Reactor Auxiliary Building.

A list of all indicators, controllers, control switches and indicating lights located on the ACP are given in Table 7.4.1-2.

The front view of ACP is shown in Figure 7.4.1-8.

Present staffing requirements are sufficient to man all the required remote stations necessary to place the plant in a safe shutdown condition following an evacuation of the control room.

Design Bases Information

In accordance with NRC General Design Criterion (GDC) 19, the capability of establishing a safe shutdown condition and maintaining the station in that mode is considered an essential function. The monitoring instrumentation essential and/or desirable to support this function is identified in Table 7.4.1-1.

To ensure availability of the auxiliary control panel and essential load control stations after Control Room evacuation, the following design features have been utilized:

1) The auxiliary control panel, transfer panels, and auxiliary transfer panels, including essential instrumentation mounted on it, are designed to withstand an SSE with no loss of essential functions.

2) The essential local stations and the auxiliary control panel, including essential controls and indicators are designed to comply with applicable portions of IEEE Standard 279-1971.

3) The auxiliary control panels maintain the separation criteria by the use of metal enclosures for Class IE circuits within the panels. Class IE devices are mounted in metal enclosures (module cans) and wiring from these devices are enclosed in flexible

metallic conduits and/or enclosed sheet metal wireways which are train dedicated inside the panels. Non-class IE circuits are separated from Class IE circuits by the use of internal wiring runs and exit points which are physically separated from those for class IE circuits.

7.4.2 ANALYSIS

7.4.2.1 General

Safe shutdown is a stable plant condition that is reached following a plant shutdown. Instrumentation and controls are provided assuring that the safe shutdown condition can be maintained for an extended period of time.

If the Control Room is evacuated, the plant can be kept in a safe shutdown condition until the Control Room can be reentered, by the use of the remote monitoring indicators, essential local stations, controls on the auxiliary transfer panels, and the controls mounted on the auxiliary control panel (ACP) as listed in Table 7.4.1-2.

Controls are designed to provide the following functions:

a) Full capability for actuation of adequate heat sink in order to maintain the design safety limit.

b) Achieve desired reactor subcriticality as per technical specification guidelines.

c) Monitor and control RCS pressure and coolant inventory.

The results of the accident analyses are presented in Chapter 15. These analyses show that safety is not adversely affected by ANS Condition II events (such as loss of normal feedwater, loss of electrical load, turbine trip, loss of offsite power) assuming that the instrumentation and control indicated in Sections 7.4.1.1 and 7.4.1.5 are available to control and monitor shutdown.

7.4.2.1.1 System design criteria

The following applies to systems and equipment required for the modes of shutdown defined in Section 7.4.1.1.

The instrumentation and control design for these systems is in conformance with the requirements of the NRC General Design Criteria (GDC), IEEE Std 279-1971, IEEE-323-1971 or 1974 as indicated in Table 3.11.0-2, and 3.11.1-1 IEEE Std 336-1971, IEEE Std 338-1971, IEEE Std 344-1971 or 1975 as indicated in Table 3.10.1-1.

Appendix A of 10 CFR 50, General Design Criteria for Nuclear Power Plants, establishes minimum requirements for the principal design criteria for water cooled nuclear power plants.

Section 3.1 provides a detailed discussion of all General Design Criteria. This section describes how the requirements that are applicable to the systems required for safe shutdown are satisfied.

<u>Criterion 1:</u> Quality Standards and Records

The requirements of Regulatory Guide 1.30 (See Section 1.8) are met. The quality assurance for the design of equipment and components is as described by the Engineering and Construction QA Program approved by the NRC during the Construction Permit review.

Criterion 2: Design Bases for Protection Against Natural Phenomena

The design bases for protection against natural phenomena are described in Chapter 3.

Criterion 3: Fire Protection

The design bases for fire protection are described in Section 9.5.1.

Criterion 4: Environmental and Missile Design Bases

Environmental design bases are described in Section 3.11. Missile design bases are described in Section 3.5.

Criterion 10: Reactor Design

Not applicable to the instrumentation and control for the systems required for safe shutdown.

Criterion 13: Instrumentation and Control

Sensor ranges are sufficient to monitor all pertinent plant variables over the expected range of plant operation in normal and transient conditions. All variables that affect plant design limits are monitored. The safety-related information readout for plant monitoring is described in Section 7.5.

Criterion 19: Control Room

Emergency shutdown from outside the Control Room is described in Section 7.4.1.11.

Criterion 20: Protection System Functions

Refer to Section 7.2.1.1.7.

Criterion 21: Protection System Reliability and Testability

Functional reliability is ensured by compliance with the requirements of IEEE Standards 279-1971, as described in Section 7.4.2.1.2. Testing is in compliance with the recommendations of Regulatory Guide 1.22 as discussed in Section 7.1.2.5.

Criterion 22: Protection System Independence

The system independence is assured through redundancy and diversity, as described in Section 7.4.1.

Criterion 23: Protection System Failure Modes

The instrumentation and control associated with these systems are not part of the protection system defined in Section 1.0 of IEEE 279-1971. However, redundancy is built in these systems to enhance safety.

Criterion 24: Separation of Protection and Control Systems

Refer to Section 7.3.2.2.6.

Criterion 26: Reactivity Control System Redundancy and Capability

Two reactivity control systems are provided: control rods and Chemical Shim Control System (see Sections 4.6 and 9.3.4).

Criterion 27: Combined Reactivity Control Systems Capability

The combined reactivity control systems are designed to ensure a very high probability of accomplishing and maintaining safe shutdown (see Sections 4.6 and 9.3.4).

Criterion 33: Reactor Coolant Makeup

The Chemical and Volume Control System provides a means of reactor coolant makeup and adjustment of the boric acid concentrations (see Section 9.3.4).

Criterion 34: Residual Heat Removal System

The Residual Heat Removal System is discussed in Section 7.4.1.8.

7.4.2.1.2 Equipment Design Criteria

IEEE Standard 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," establishes minimum requirements for safety-related functional performance and reliability of the system required for safe shutdown. This section describes how the requirements listed in Section 4 of IEEE Standard 279-1971 are satisfied:

IEEE-279 Section 4.1: GENERAL FUNCTIONAL REQUIREMENT

The equipment is designed for manual actuation under shutdown conditions. Instrument performance characteristics, range response time, and accuracy are selected for compatibility with and adequacy for the particular function.

IEEE-279 Section 4.2: SINGLE FAILURE CRITERION

See Section 7.4.1.2 for discussion on single failure criteria.

IEEE 279 Section 4.4: EQUIPMENT QUALIFICATION

Instrumentation and control equipment are qualified to the requirements as stated in Section 3.10 and 3.11.

IEEE-279 Section 4.6: CHANNEL INDEPENDENCE

Channel separation is provided for instruments and controls required for safe shutdown in accordance with Regulatory Guide 1.75 (See Section 1.8).

IEEE-279 Section 4.10: CAPABILITY FOR TEST AND CALIBRATION

Testing capability is in accordance with IEEE Standard 338-1971 and discussed in Section 7.3.2.

IEEE Standard 308-1971 - Electric Power for Class IE Systems

Systems required for safe shutdown are supplied with redundant Class IE power supplies which are in compliance with IEEE-308-1971.

Regulatory Guides

For the applicable revision and additional information on Regulatory Guides, see Section 1.8.

Regulatory Guide 1.11

Not applicable

Regulatory Guide 1.22

Testing capability is in accordance with Regulatory Guide 1.22 as discussed in Section 7.3.2

Regulatory Guide 1.29

Instrumentation and controls required for safe shutdown are designed to withstand the effects of an SSE. They are capable of performing their functions during and after seismic event.

Regulatory Guide 1.30

The components of the systems required for safe shutdown are designed to operate during and after an accident in the area in which they are located. See discussions in Sections 3.10 and 3.11.

Regulatory Guide 1.32

Chapter 8 discusses in full the aspects of the electric power systems.

Regulatory Guide 1.47

Refer to Section 7.5.1.g.

Regulatory Guide 1.53

For application of single failure criterion see Section 7.4.1.2.

Regulatory Guide 1.62

The function of these systems is to provide adequate heat sink and assure subcriticality of the reactor. As such they are not part of the protective systems and therefore Regulatory Guide 1.62 is not considered to be applicable.

Regulatory Guide 1.63

For compliance see Chapter 8.

Regulatory Guide 1.70

The requirements of RG 1.70 are fully satisfied by this FSAR.

Regulatory Guide 1.75

The wiring arrangement of all the Class IE electrical systems required for safe shutdown is in full compliance with the requirements of Regulatory Guide 1.75.

Regulatory Guide 1.89

The instrumentation and control for the required equipment is qualified as Class IE. Compliance with the regulatory positions is discussed in Sections 3.10 and 3.11.

7.4.2.2 Consideration of Selected Plant Contingencies

7.4.2.2.1 Loss of Instrument Air System

Electrically powered instrument sensors and controls are supplied from Class IE Power System and therefore not affected by loss of instrument air. Upon loss of instrument air, pneumatically operated valves in systems required for safe shutdown will take the position required for system operation in the plant shutdown mode.

Boric Acid System

The two piston operated valves in the boric acid transfer pump discharge fail open on loss of instrument air, so that the boron injection path remains unobstructed. The boric acid flow control valve will not be able to regulate the flow after an air failure as it fails open. However for cold shutdown manual on-off operation of the boric acid pump is sufficient. For hot standby no boron injection is required except where in this condition for greater than 8 hours.

The failure of the flow control valves upstream and downstream of the boric acid blender prevents the addition of boric acid to the volume control tank. However, by manually rearranging the injection path, boric acid can be introduced to the suction of the charging pumps. Therefore, the loss of instrument air does not impair the safety function of the Boric Acid Transfer System.

Reactor Coolant Inventory - Charging and Letdown

Upon loss of instrument air, the isolation valves on the letdown line are designed to fail closed to terminate letdown to the volume control tank. The failure of the charging flow control valve, the seal water flow control valve, and the charging flow isolation valves (1-8146, 1-8147) does not

impair the safety of this system, as all valves fail open. If the pressurizer level changes, manual closure of the charging line isolation valves (MOVS 1-8107, 1-8108) will control the level increase. If pressurizer level decreases, manual opening of the charging line isolation valves will restore the level. Alternatively, if instrument air is not expected to be restored, the charging flow control and/or seal water flow control valves may be isolated and manual flow control achieved by the respective flow control valve bypass globe valve. This is sufficient for achieving and maintaining safe shutdown.

Residual Heat Removal System

There are two remotely operated flow control valves in each RHR train that are used for temperature/flow control.

Upon loss of instrument air or instrument power the RHR heat exchanger outlet flow control valves fail to the open position, to insure uninterrupted RHR flow to the core. Conversely the RHR heat exchanger by-pass valves fail closed to ensure adequate core cooling.

Upon loss of remote operation of the heat exchanger outlet and bypass valves alternate temperature controls are utilized. If the reactor coolant cooldown rate is near the allowable limits, temperature will be manually controlled, using one of the following methods, to prevent exceeding the stress limits of the reactor coolant system:

1. Starting/stopping of the RHR pump.

2. Opening/shutting of the RHR to RCS discharge valves

3. Manually throttling the RHR heat exchanger outlet valve

Pressurizer Pressure Control-Spray

Pressurizer auxiliary spray is not available upon loss of instrument air, because the pneumatically operated valve on this line fails closed. The auxiliary spray is used at the end of the core cooldown when RCS pumps are not available. By controlling the pressurizer heaters the vapor space can be maintained during this phase of the cooldown even without the auxiliary spray.

An alternate pressure relief system consisting of pressurizer power operated and spring loaded relief valves is provided to prevent overpressurization, when spray is not available. Upon loss of pneumatic power, only the code safety valves will be operable since the power operated valves require air or nitrogen to open. There is, however, a "limited" supply of nitrogen available in the accumulators for a few PORV strokes.

7.4.2.2.2 Loss of cooling water to vital equipment

As discussed in Section 9.2.2, the Component Cooling Water System is designed with full redundancy. Failure or loss of one train will not prevent the safe shutdown of the plant.

7.4.2.2.3 Plant load rejection, turbine trip, and loss of offsite power

In the event of loss of offsite power coincident with plant load rejection or turbine trip, power for safe shutdown is provided by the onsite emergency power system. The description and analysis of the emergency power system are discussed fully in Section 8.3. The emergency diesel generators provide power for operation of all necessary pumps and valves. The station batteries provide DC power for operation of control and instrumentation systems required to actuate and control essential components.

The emergency power system is designed to meet the single failure criterion and withstand design basis natural phenomena.

7.5 SAFETY-RELATED DISPLAY INSTRUMENTATION*

This section describes those display instrumentation systems which provide minimum and timely information to the operator as defined in Chapter 15. This instrumentation allows the operator to adequately monitor conditions in the Reactor, Reactor Coolant System, Containment, and safety-related process systems, throughout all operating conditions of the plant so that he may adequately perform all required manual actions important to plant safety.

Display instrumentation is identified on Tables 7.5.1-1 through 7.5.1-15 which is provided for the monitoring of anticipated operational occurrences, accident conditions, and post-accident condition within the Nuclear Steam Supply System (NSSS) and balance of plant (BOP) systems.

7.5.1 DESCRIPTION

The display instrumentation described in this section is organized in the following manner:

a) Plant Process Display Instrumentation - Provides information needed by the operator for monitoring conditions in the reactor, in the Reactor Coolant System, in the Containment Ventilation System and BOP systems.

b) Reactor Trip System (RTS) Monitoring - For a description of the reactor trip system monitoring, refer to Section 7.2.

c) Engineered Safety Features (ESF) System Monitoring - Provides information needed by the operator for monitoring the status of each ESF system during all operating conditions including accident and post-accident conditions. This information is described in Section 7.5.1.3.

d) ESF Support Systems Monitoring - Provides information needed by the operator for monitoring the support systems required to function for the operation of the ESF systems. This information is given in Section 7.5.1.4.

e) Auxiliary Control Panel Instrumentation - For a description of the auxiliary control panel instrumentation, refer to Section 7.4.

f) RCCA Position Indication System - The display instrumentations for this system is listed in Table 7.5.1-15.

---

* Further information is contained in the TMI appendix.

g) Safe Shutdown Monitoring System - For a description of the safe shutdown monitoring system, refer to Section 7.4.

h) Post-accident Monitoring Instrumentation (PAMI) - Provides information needed by the operator for monitoring the plant parameters after a postulated accident.

i) Bypassed and Inoperable Status Indication - Provides information needed by the operator for monitoring the availability of the safety-related equipment.

j) Control Board Annunciation and Light Boxes - In addition to the safety display instrumentation on the MCB, annunciators, monitor light boxes, status light boxes, and service water leak detection indication are provided to the operator on the MCB for surveillance throughout all operating conditions of plant. These light boxes are described in Section 7.5.1.10.

7.5.1.1 Plant Process Display Instrumentation (PPDI)

Tables 7.5.1-1 through 7.5.1-15 list the safety display instrumentation which is provided in the Control Room to inform the operator of the status of the plant process monitoring sensors located in the reactor, Reactor Coolant System, Containment Ventilation System, containment isolation and the BOP systems. This information provided by the PPDI is used for start-up, operation and shutdown of the plant and is provided on the main control board. This information, which is provided in a form that is useful to the operator, may be indicated, or monitored.

Alternate indication and control instrumentation is provided at the auxiliary control panel outside the Control Room to allow reactor shutdown and maintenance of the reactor in a safe condition during hot shutdown or cold shutdown if the Control Room becomes uninhabitable.

7.5.1.2 Reactor Trip System Monitoring

This system is described in Section 7.2.

7.5.1.3 Engineered Safety Features (ESF) System Monitoring

The Engineered Safety Features Actuation System continuously monitors the system parameters. In case the predetermined setpoints are exceeded, the resulting signals generated by redundant instrumentation are provided into channels and combined in logic matrices. Once the logic combination is completed, the system sends actuation signals to the appropriate ESF components. Even though the actuation of the ESF systems is automatic and does not require operator action, sufficient information is provided in the Control Room to allow the operator to monitor the operation of the ESF and EST support systems during normal operation. This information consists of valve position indication, pump operating status, tank level indication, flow indication, RCS temperature and pressure, and indication of the process parameters that actuate ESF systems.

The ESF systems described in this section are organized in the following manner:

7.5.1.3.1 Containment Isolation System (CIS)

Under specified accident conditions, the Containment Isolation System (CIS) isolates the normally open lines penetrating the Containment which are not essential to reactor protection.

The containment isolation Phase A actuation signal (T signal) or the containment isolation Phase B actuation signal (P signal) is generated by either the manual actuation switches on the main control board or through the containment high pressure actuation logic. (See Sections 6.2.4 and 7.3.1.3.2.2 for the system description.) No safety display instrumentation for the Containment Isolation System is provided for the operator in the Control Room except for valve status indicating lights.

7.5.1.3.2 Main Steam Supply System

The display instrumentation for the Main Steam Supply System is listed in Table 7.5.1-11.

7.5.1.3.3 Containment Spray System

Containment Spray System is automatically initiated by the containment spray actuation signal. This signal initiates the Containment Spray System by starting the containment spray pumps, and opening the containment spray isolation valves. Containment spray reduces containment pressure and temperature following a LOCA or steam line break accident inside the Containment (see Section 7.3.1.3.1.1 for system description).

The display instrumentation for this system is listed in Table 7.5.1-1.

7.5.1.3.4 Containment Cooling

This system consists of four safety-related fan cooler units and three non-safety fan cooler units. During normal power operation, safety-related units operate in conjunction with the non-safety units; during accident and post-accident conditions only safety-related fan cooler units will operate (see Section 7.3.1.3.1.2 for system description).

In order to assess system operation, the control room operator has status indicating lights for the fans and dampers. A multipoint seismically qualified temperature recorder (TR-0005) is provided to record cooling coil air outlet and containment temperature. The display instrumentation for this system is listed in Table 7.5.1-1.

7.5.1.3.5 Auxiliary Feedwater System

The Auxiliary Feedwater System consists of two motor-driven pumps and one turbine-driven pump. These pumps are energized automatically during emergency situations such as steam line rupture, loss of normal feedwater and loss of offsite power (see Section 7.3.1.3.3 for system description).

A three pen Class 1E Seismic Category I recorder is provided to record auxiliary feedwater flow to steam generator A, B and C. The recorder is actuated only when pumps are running. The display instrumentation for this system is listed in Table 7.5.1-2. Additional information regarding auxiliary feedwater system instrumentation may be found in Section 7.3.1.3.3 and 7.4.1.3.

7.5.1.3.6 Combustible Gas Control System

The Combustible Gas Control System consists of two non-safety-related subsystems which operate as follows:

a) A hydrogen analyzing subsystem (grab sample skid) provides the capability to monitor the containment atmosphere.

b) The containment hydrogen purge subsystem for providing a controlled purge of the Containment through fission product removal equipment.

Display instrumentation for the Combustible Gas Control System is provided on a separate control panel located in the Control Room.

7.5.1.4 ESF Support Systems

ESF support systems are those systems which are required to function when the ESF systems are operating. The instrumentation provided enables the operator to monitor important process variables for these systems, in order to take appropriate action when required.

The ESF support systems described in this section are organized in the following manner:

7.5.1.4.1 Emergency Power Supply System

The emergency power supply is provided by the diesel generators which will start automatically on loss of normal power supply. When the diesel generator has attained rated speed and voltage (within 10 seconds after the start signal), the safety-related loads are connected to the bus automatically by the emergency load sequencer in accordance with the loading sequence (see Sections 7.3.1.5 and 8.3.1.1.2.8 for system description.)

The display instrumentation for this system is listed in Table 7.5.1-3.

7.5.1.4.2 Emergency Service Water System

The Emergency Service Water System provides cooling water to the charging pumps oil coolers, containment fan coolers, diesel generators, component cooling water heat exchangers and HVAC water chillers (see Section 7.3.1.5.2 for system descriptions).

The display instrumentation for this system is listed in Table 7.5.1-4.

7.5.1.4.3 Component Cooling Water System

The Component Cooling Water System provides cooling water to RHR heat exchangers, RHR pump coolers, reactor coolant drain tank, letdown heat exchanger, reactor coolant pumps and gross failed fuel system (see Section 7.3.1.5.3 for system description).

The display instrumentation for this system is listed in Table 7.5.1-13.

7.5.1.4.4 120 Volt uninterruptible AC power system

See Section 8.3.1 for the description and analysis of the 120V AC power system.

7.5.1.4.5 Safety-related 125 Volt DC system

See Section 8.3.2 for the description and analysis of the 125V DC system.

7.5.1.4.6 Control room ventilation system

The Control Room Ventilation System provides air conditioning to the Control Room during normal operation with the Control Room Emergency Filtration System de-energized. During accident and post-accident conditions, all isolation valves at normal and emergency outside air intakes will be closed, the fans in each Control Room Emergency Filtration System will start and the respective fan inlet valve will open (see Section 7.3.1.5.7 for system description). In addition, the RAB Normal Ventilation System will be secured, and the RAB Emergency Exhaust System (RABEES) will be started. The RAB Normal Ventilation System must be secured to preclude the possibility of postulated system failures from impacting the ability of the Control Room Envelope (CRE) to maintain a positive pressure of ≥ 1/8 INWG relative to adjacent areas. When the RAB Normal Ventilation System is secured, the RAB Emergency Exhaust System is initiated to maintain the potentially contaminated areas of the RAB at sub-atmospheric pressure in an effort to limit outleakage and to remove radon gas from the RAB.

A multipoint seismically qualified temperature recorder (TR-0005) is provided to record the electric heating coil inlet and HEPA filter outlet air temperature.

The display instrumentation for this system is listed in Table 7.5.1-5.

7.5.1.4.7 Essential services chilled water system

The essential services chilled water is provided in areas where safety-related equipment is located (see Section 7.3.1.5.4 for system description). No safety display instrumentation for the Essential Services Chilled Water System is provided for the operator on the main control board, except for the pumps, valves, status indicating lights, and annunciation of the water chiller conditions.

7.5.1.4.8 Diesel generator building ventilation system

No display instrumentation for the Diesel Generator Building Ventilation System is provided for the operator on the MCB, except for the fan status indicating lights and alarm.

7.5.1.4.9 Essential switchgear room cooling system

Switchgear room cooling is provided in the areas where essential electrical equipment is located. The supply fans and dampers operate automatically in response to a safety injection signal, or manually from the Control Room (see Section 7.3.1.5.10 for the system description).

No safety display instrumentation for the Essential Switchgear Room Cooling System is provided for the operator on the main control board, except for a fan status indicating light.

7.5.1.4.10 Electrical equipment protection room HVAC system

The electrical equipment protection rooms in the Reactor Auxiliary Building (RAB) are heated and cooled by separate essential HVAC systems which are required to operate during normal plant operation and design basis accidents (see Section 7.3.1.5.10.1 for system description).

No display instrumentation for the electric equipment protection HVAC system is provided for the operator on the main control board (MCB), except for the fan status indicating light.

7.5.1.4.11 Emergency exhaust system

7.5.1.4.11.1 Reactor auxiliary building emergency exhaust system

The Reactor Auxiliary Building Emergency Exhaust System serves that portion of the RAB which contains selected equipment essential for safe shutdown. The charging pump area, RHR heat exchanger area, containment spray pump area, and RHR pumps rooms, mechanical room, electrical room, H&V room, and mechanical, electrical & H&V penetration areas are provided coverage. In normal operation, the normal supply and normal exhaust system are in operation. Upon receipt of a Safety Injection Actuation Signal (SIAS) or a Control Room Isolation Signal (CRIS), the normal supply and exhaust systems stop and the emergency exhaust system starts (see Section 7.3.1.3.4 for system description).

A multipoint seismically qualified temperature recorder (TR-0005) is provided to record the electric heater coil and HEPA filter inlet and outlet air temperature.

The display instrumentation system is listed in Table 7.5.1-6.

7.5.1.4.11.2 Fuel handling building emergency exhaust system

In normal operation, the normal supply and normal exhaust systems are in operation. On receipt of a high radiation signal, the normal supply and exhaust systems stop, and both emergency exhaust systems start (see Section 7.3.1.3.4 for system description).

A multipoint seismically qualified temperature recorder (TR-0005) is provided to record the electric heating coil inlet and HEPA filter inlet and outlet air temperature.

The display instrumentation for this system is listed in Table 7.5.1-7.

7.5.1.4.12 Spent fuel pool pump room ventilation system

This system provides cooling to the spent fuel pool pumps and emergency exhaust system during normal and fuel handling accident conditions (see Section 7.3.1.5.11 for system description).

The display instrumentation for this system is listed in Table 7.5.1-8.

7.5.1.5 Auxiliary Control Panel Instrumentation

For a description of this instrumentation, refer to Section 7.4.

7.5.1.6 RCCA Position Indication System

The display instrumentation for this system is listed in Table 7.5.1-15.

7.5.1.7 Safe Shutdown System

For a description of this system, refer to Section 7.4.

7.5.1.8 Post-Accident Monitoring Instrumentation

The Post-Accident Monitoring System is designed to monitor plant variables during and following an accident.

Instrumentation provided for the remote monitoring of post-accident parameters indicated in the PAMI column in 7.5.1 tables is qualified for operation in post-accident environmental and seismic conditions in accordance with the commitment to RG 1.97. Refer to Section 1.8 and Reference 7.5.1-1.

The post-accident display instrumentation is provided for the operator to enable him to perform manual safety functions and to determine the effect of manual actions taken following a reactor trip due to ANS Condition II, III or IV events as defined in Chapter 15.0. Tables 7.5.1-1 through 7.5.1-13 include the information readouts required to maintain the plant in a hot shutdown condition or to proceed to cold shutdown within the limits of the Technical Specifications. The following systems parameters are listed in Tables 7.5.1-1 through 7.5.1-13.

a) Reactor coolant COLD LEG and HOT LEG temperature

b) Pressurizer water level

c) Reactor coolant pressure (wide range)

d) Containment pressure and containment wide range pressure

e) Steam line pressure

f) Steam generator water level (wide range)

g) Steam generator water level (narrow range)

h) Component cooling water heat exchanger discharge pressure

i) Component cooling water surge tank level

j) Component cooling water heat exchanger discharge temperature

k) Refueling water storage tank level

l) Containment spray pump A and B discharge header pressure

m) Auxiliary feed water flow to steam generator

n) Auxiliary feed water pumps A and B discharge pressure

o) Turbine auxiliary feed water pumps discharge pressure

p) Emergency service water pumps A and B discharge pressure

q) Service water pumps A and B header flow

r) Service water booster pumps A and B pressure

s) Service water booster pumps A and B flow

t) Diesel generators A and B voltage

u) Diesel generators A and B field voltage

v) Diesel generators A and B current

w) Batteries A and B voltage

x) Containment sump level

y) Neutron Flux Monitoring System

z) Boric acid tank level

There are two independent, redundant channels of containment wide range pressure monitoring as described in FSAR Table 7.5.1-10. Each channel consists of a Class 1E, seismic Category I pressure transmitter which is physically located inside the Containment. Signal wires are routed from inside Containment to the control room via electrical penetrations described in FSAR Section 3.8.1.1.3.3.

The pressure transmitter output will be processed by a process instrumentation control system (PIC) which in turn will furnish signals for the Class 1E indicator and the Emergency Response Facility Information System. The operator has the capability for continuous recording if desired for trending.

For the instruments listed in this section the following test abstracts apply: 14.2.12.1.16, 14.2.12.1.19, 14.2.12.1.20, 14.2.12.1.30, 14.2.12.1.34, 14.2.12.1.37, 14.2.12.1.47 and 14.2.12.1.50.

7.5.1.8.1 Thermocouple Monitor

A core exit thermocouple monitor has been installed to provide improved information presentation and display to the plant operators on the status of core heat removal capability. The system monitors all core exit thermocouples utilizing redundant channels of instrumentation and control room displays.

The monitoring system displays three levels of core exit thermocouple information: a) a core map showing minimum, average, and maximum quadrant temperatures, b) a spatial map

exhibiting the thermocouple temperature at its respective location in the core, and c) a detailed data list exhibiting thermocouple location, tag number and temperature.

7.5.1.8.2 Reactor Vessel Level Instrumentation System

The Reactor Vessel Level Instrumentation System (RVLIS) consists of two redundant independent trains that monitor the reactor vessel water levels.

Each train provides three vessel level indications: full range, upper range, and dynamic head. The full range RVLIS reading provides an indication of reactor vessel water level from the bottom of the vessel to the top of the vessel during natural circulation conditions. The upper range RVLIS reading provides an indication of reactor vessel level from the hot leg pipe to the top of the reactor vessel head during natural circulation conditions. The dynamic head reading provides an indication of reactor core, internals and outlet nozzle pressure drop for any combination of operating reactor coolant pumps. Comparison of the measured pressure drop with the normal, single phase pressure drop provides an approximate indication of the relative void content of the circulating fluid.

7.5.1.9 Bypassed and Inoperable Status Indication (IEEE 279 Section 4.13, RG 1.47, and ICSB-BTP-21)

A pressure, flow, and temperature typical process loop diagram is shown on Figure 7.5.1-1. Bypassed and inoperable conditions are indicated on the main control board (MCB) on a system and train basis.

The MCB has two bypass and inoperable status panels for the redundant ESF and ESF support systems. Each panel has indicating windows to show inoperable status of the ESF and/or ESF support systems within each train. Inoperable status is indicated on loss of control power to the safety equipment, power circuit breaker in racked out position or any one of the associated powered valves in an unsafe or inoperable position. During the normal plant operation when any of the windows is energized an alarm will simultaneously alert the control room operator that ESF or support system is inoperable or bypassed. The status indication for that particular system will stay on until the inoperable condition is rectified.

The operator has manual capability to activate each system's inoperable status indication by depressing the window on the board. This manually activated system indication will stay on until the system is reset by depressing the same window again.

The bypass indication is located on the main control board enabling the operator to assess its status. Windows are arranged in a systematic configuration with identical and independent windows for each redundant train. Based on the window information, together with other related instrumentation, the operator can coordinate maintenance/test activities on safety-related equipment throughout the plant without compromising the plant safety.

Since the ESF bypass panel is non-safety, all the ESF equipment inputs are isolated between the bypass panel and associated safety equipment. The lamps and circuits in each train can be periodically tested by a test pushbutton provided on the ESF bypass panel.

The bypass panel layout and wiring diagram are shown on Figures 7.5.1-2 and 7.5.1-3.

7.5.1.10 Control Panels, Annunciators, Monitoring Light Boxes, Status Light Boxes, Service Water Leak Detection

7.5.1.10.1 Control Panels

The main control board is of the free standing benchboard type and consists of nine control panels, with control switch modules primarily arranged on the lower bench portion, indicators, A/M stations, recorders and display instrumentation primarily on the lower vertical section, and annunciators and light boxes primarily on the upper vertical section. The main control board structure and the internal wiring of the electrical equipment are designed to Class 1E and Seismic Category I requirements. The physical separation of the safety systems display instrumentation is designed such that a failure of any part of the whole train, channel or division will not prevent safe shutdown of the plant.

All the instrumentation cables are identified by color coded tags (see Section 8.3.1.3 for the discussion on identification of cables and separation).

7.5.1.10.2 Annunciators

The main control board has a total of 29 non-safety annunciator light boxes. The input to these boxes is wired to the two non-safety annunciator logic cabinets. Three different types of annunciator sequence are used: a) firstout b) reflasher c) plain (normal).

Each section of the board is equipped with a four position control switch to test, acknowledge, reset and silence the alarm in that particular MCB section annunciator light box. However, the circuit is designed to permit silencing of the alarm from any section of the board. The annunciator is provided with a chime feature for resetting the circuit. The window arrangement is done in accordance with the system control layout on the console. Annunciator systems are listed in Table 7.5.1-16.

7.5.1.10.3 Monitor Light Boxes

Monitor status lights are provided on the main control board for all pumps and valves which are required to function as a part of the engineered safe-guards systems. These monitor lights are provided specifically to alert the operator, should the operation or position of a component be incorrect with respect to its required status during normal full power operation or any one of the post-accident operational phase (injection, cold leg recirculation, hot leg recirculation). In addition to the monitor status lights, the majority of the safety injection system valves utilize an annunciator alarm system which is specifically provided to actuate an alarm in the Control Room should one of these valves be mispositioned during normal full power operations.

The monitor light system consists of a series of light boxes grouped in a specific fashion on the main control board. Each light box represents a particular safety-related component. In general, the component monitor lights should not be illuminated when the plant is at normal full power operation. The monitor lights should be illuminated only when the operation/position of any component is changed from its normal full power operational status. Therefore, with only a few exceptions, any illuminated monitor light during normal full power operations would indicate that a component was positioned or operating improperly. However, the correct position or operation of a component during normal full power operation may not be the correct position for that component during one of the post-accident operational phases. For those components, an

illuminated monitor light during a particular post-accident operational phase could indicate that the component had been properly positioned or was operating properly.

For this reason, the monitor lights are divided into several major groups, with each group containing only those monitor lights which should have the same status regardless of the operational status of the plant. For example, all the monitor lights in one specific group may be dark during the normal full power operation and injection phase whereas that same group of monitor lights may all be illuminated during the cold leg and hot leg recirculation phase.

The grouping of monitor lights, therefore, provides a relatively simple means for indicating on the main control board any improperly positioned or operating component during any phase of operation. In summary, any monitor light out of phase with the other monitor lights in that specific grouping would indicate that the corresponding component was improperly positioned or improperly operating.

In addition to the light arrangement, certain critical valves have an annunciator to indicate and alarm a change to the off-normal operational mode. For the operator to easily discover when a component is not in its correct mode, the monitor lights are to be arranged on the main control board as follows:

Group 1 - Those components whose status is not changed during the injection or recirculation phases of SIS operation.

Group 2 - Those components whose status is not changed during the injection phase, but is changed during the cold leg recirculation phase, and remains in that position for the hot leg recirculation phase.

Group 3 - Those components whose status is changed during the injection phase, is changed back during the cold leg recirculation phase, and remains in that position for the hot leg recirculation phase.

Group 4 - Those components whose status is changed for the injection phase and maintained throughout both recirculation phases.

Group 5 - Those components whose status is not changed during the injection or cold leg recirculation phases, but is changed for the hot leg recirculation phase.

Group 6 - Those components whose status is changed during the injection phase, remains changed for the cold leg recirculation phase, and changes back for the hot leg recirculation phase.

Group 7 - Those components whose status is not changed during the injection phase, changes for the cold leg recirculation phase, and changes back for the hot leg recirculation phase.

<u>Notes on Monitor Lights:</u>

1. The monitor lights will normally be "OFF" during normal plant operation, with the exception of one charging pump and one component cooling water pump in Group 4; and one boron injection recirculation pump and one letdown line orifice isolation valve in Group 1.

2. The monitor lights will come "ON" when the component is not in the normal mode. The component will be in the mode as marked on the window (i.e., windows are marked with the off-normal mode).

3. An abnormal situation during the injection or recirculation phases will be recognizable by a monitor light being out of phase with the other lights in that particular group. All the lights in each group should be on or off during phases of SIS operation as follows:

		Display During Recirculation	
Group	Display During Injection Phase	Cold Leg	Hot Leg
1	Dark	Dark	Dark
2	Dark	Light	Light
3	Light	Dark	Dark
4	Light	Light	Light
5	Dark	Dark	Light
6	Light	Light	Dark
7	Dark	Light	Dark

4. The windows marked (A) will also annunciate when the component is not in the normal mode. An annunciation is generally an indication of an abnormal, possibly safety-related, situation during full power operation. The component will be annunciated by groups, with one annunciator for each of the groups. The annunciator windows will be engraved as follows: Group (1,2,3,4,5,6 or 7) monitor lights, component off normal.

5. There will be one light unit for each component. A test button is provided to permit periodic testing of the display.

7.5.1.10.4 Status Light Boxes (SLB)

The main control board has a total of seven status light boxes. These status light boxes are separated into two groups, one group consists of five (SLB 1,2,3,4,7) non-safety light boxes which are used for the turbine generator and non-safety HVAC systems and located on the MCB panels 1B1, 1B2, and 1D2, the second group consists of two (SLB 5,6), Seismic Category I light boxes for each redundant train, these boxes are used for the safety-related HVAC system, and located on the MCB panel 1D2.

The Auxiliary Equipment Panel (AEP-1) has a total of five status light boxes. These status light boxes are separated into two groups, one group consists of four (SLB 8,9,10,11) seismic Category I light boxes which are used for the safety-related HVAC systems, the second group consists of non-safety light box used for the non-safety HVAC systems.

The function of these status light boxes is to show in the Control Room the status (open or close position) for all the mechanical equipment such as valves and dampers which are either hand

operated or interlocked with the permissive signals (i.e. fan start signal) to the control room operator. The status light is activated by the open and close limit switch which is mounted on the valve stem or on the damper.

The arrangement of safety-related status light boxes and typical wiring are shown on Figures 7.5.1-4 through 7.5.1-8, 7.5.1-14, and 7.5.1-15.

7.5.1.10.5 Service water leak detection indication

The main control board has two Class IE light modules for each redundant train. These light modules are located on the MCB panel 1A1 and indicate the service water flow condition for the component cooling water heat exchangers, containment cooler fans and HVAC water chillers to the Control Room operator. The leak detection light is activated through the process instrument cabinet (PIC). A line break upstream of the flow instrument will show low flow condition. Common alarm is also provided for the service water leakage system.

The arrangement of service water leak detection light boxes and typical wiring is shown on Figures 7.5.1-9 through 7.5.1-13.

7.5.1.10.6 Nuclear instrumentation

The display instrumentation is listed in Table 7.5.1-14. Upper and lower flux deviation and auto defeat annunciators ALB-13/5-3 and ALB-13/5-4 are screened through a time delay circuit in annunciator Cabinet No. 2 to prevent spurious nuisance alarms. The flux deviation alarm limit is reached for very short time periods due to nuclear instrumentation system process noise. Such flux deviations do not represent a sustained condition requiring operator action. If a sustained flux deviation condition exists the annunciator will actuate. The time delay setting is no greater than 1.5 minutes.

7.5.2 ANALYSIS

7.5.2.1 Plant Process Display and Post-Accident Monitoring Instrumentation

The indicator channels (see Tables 7.5.1-1 through 7.5.1-13) required to enable the operator to take the correct action during the course of a Condition II, III, or IV accident or during post-accident recovery are designed to the criteria listed in Section 7.5.2.1.1.

The indicators in Tables 7.5.1-1 through 7.5.1-13 are used for the operational monitoring of the plant. The indicators are functionally arranged on the main control board to enable the operator to readily understand and interpret plant conditions. Comparisons between duplicate information channels, or between functionally related channels, enable the operator to readily identify a malfunction in a particular channel. The range of the instrumentation, listed in Tables 7.5.1-1 through 7.5.1-13, extends over the maximum expected range of the variable being measured. The combined indicated accuracies of the instruments listed on Tables 7.5.1-1 through 7.5.1-13 are within the errors used in the safety analyses. The occurrence of an accident does not render the information required for that accident unavailable, and the status and reliability of the necessary information is known to the operator before, during, and after an accident.

7.5.2.1.1 Design criteria

7.5.2.1.1.1 Scope

The scope of IEEE Standard 279-1971 covers protection systems that initiate automatic protective actions. Therefore, in the absence of applicable industry standards for the Post-Accident Monitoring System (PAMS), the following criteria were developed, using applicable sections of IEEE Standard 279-1971 as a model for this purpose.

The environmental and seismic qualification of PAMS sensors is covered in Sections 3.10 and 3.11.

The following criteria establish requirements for the functional performance and reliability of the safety-related PAMS for the SHNPP. For purposes of these criteria, the SHNPP's safety-related PAMS encompasses those electric and mechanical devices and circuitry which provide information needed to:

1. Enable the operator to take the correct manual action during the course of an ANS Condition II, III, or IV event, or during recovery from a Condition II, III, or IV event.

2. Maintain safe shutdown.

7.5.2.1.1.2 Definitions

The definitions in this section establish the meanings of words in the context of their use in these criteria.

1. Channel - An arrangement of components and modules as required to generate a single information signal which monitors a generating station condition.

2. Components - Items from which the PAMS is assembled (for example, resistors, capacitors, wires, connectors, transistors, tubes, switches, springs).

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

4. Post-Accident Monitoring Function - A post-accident monitoring function consists of sensing one or more variables associated with a particular generating station condition, processing signals, and presenting visual information (including recorded information) to the operator.

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

7.5.2.1.3 Requirements

7.5.2.1.3.1 General functional requirements

The SHNPP's PAMS will function with precision and reliability to continuously display the appropriate monitored variables. This requirement will apply for the full range of conditions and performance enumerated.

7.5.2.1.3.2 Information readout

Tables 7.5.1-1 through 7.5.1-13 show which parameters are recorded to provide a historical record of the behavior of the parameters. The equipment used to record information need not be redundant, nor meet the single failure criterion.

7.5.2.1.3.3 Single failure criterion

Any single failure within the PAMS will not result in the loss of the monitoring function. ("Single failure" includes such events as the shorting or open-circuiting of interconnecting signal or power cables. It also includes single credible malfunctions or events that cause a number of consequential component, module, or channel failures. For example, the overheating of an amplifier module is a single failure even though several transistor failures result. Mechanical damage to a mode switch would be a single failure although several channels might become involved).

7.5.2.1.3.4 Quality of components and modules

Components and modules are of a quality that is consistent with minimum maintenance requirements and low failure rates. Quality levels are achieved through the specification of requirements which promote high quality, such as requirements for design, for the derating of components, for manufacturing, quality control, inspection, calibration, and test.

7.5.2.1.3.5 Equipment qualification

Type test data or reasonable engineering extrapolation based on test data will be available to verify that PAMS equipment will meet, on a continuing basis, the performance requirements determined to be necessary for achieving the PAMS requirements. Qualifications of recorders will only verify operability following (not during) a seismic event. Accelerating forces associated with the recording pen during the seismic shake period may cause an ink blur of the record during this period, and in some cases a mechanical loosening of the recording pens might be encountered.

7.5.2.1.3.6 Channel integrity

All PAMS channels are designed to maintain necessary functional capability, including accuracy and range, under extremes of conditions (as applicable) relating to environment, energy supply, and malfunctions during the circumstances throughout which the monitoring system must function.

7.5.2.1.3.7 Channel independence

Channels (exclusive of recorders as clarified in Section 7.5.2.1.3.2) which provide signals for the same monitoring function are independent and physically separated to accomplish decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis. This design also reduces the likelihood of interactions between channels during maintenance operations during channel malfunctions.

7.5.2.1.3.8 Power source

The post-accident monitoring display instrumentation is capable of operating independent of offsite power availability.

7.5.2.1.3.9 Post-accident monitoring system and control system interaction.

1. Classification of equipment - Any equipment that is used for both post-accident monitoring and control functions shall be classified as part of the PAMS.

b) Isolation devices - The transmission of control or monitoring signals from the post-accident monitoring equipment will be through isolation devices which are classified as part of the PAMS. No credible failure at the output of an isolation device will prevent the associated monitoring system channel from meeting the minimum performance requirements considered in the design bases. Examples of credible failures include short circuits, open circuits, grounds, and the application of the maximum credible AC or DC potential (140 volt DC or 118 volt AC). A failure in an isolation device is evaluated in the same manner as a failure of other equipment in the PAMS.

7.5.2.1.3.10 Derivation of System Inputs

Inputs to the PAMS are derived from signals that are direct measures of the desired variables. The PAMS channels listed in Tables 7.5.1-1 through 7.5.1-13 also in many cases bear a known relationship to each other during normal plant operation.

7.5.2.1.3.11 Capability for Sensor Checks

Means shall be provided for checking, with a high degree of confidence, the operational availability of each PAMS input sensor during reactor operation. This ,may be accomplished in various ways, for example:

a) By perturbing the monitored variable; or

b) By introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable; or

c) By cross checking between channels that bear a known relationship to each other and that have readouts available.

7.5.2.1.3.12 Capability for Verifying Operability

Means are available for verifying the operability of the PAMS channels. Where channels exhibit a dynamic response during normal plant operation or where channels are required frequently for normal plant operation, verification of operability is inherent in the normal functioning of the channels. For channels which monitor a normally static parameter, provisions are included to allow periodic testing which verifies channel operability. Identification of malfunctions will be adequately identified by cross checking between duplicate redundant channels or cross checking between channels that bear a known relationship to each other during normal plant operation.

7.5.2.1.3.13 Channel Bypass or Removal From Operation

The PAMS is designed to permit any one channel to be removed from service for maintenance during power operation. During such operation, the active parts of the PAMS need not themselves continue to meet the single failure criterion. As such, monitoring systems comprised of two redundant channels are permitted to violate the single failure criterion during channel bypass provided that acceptable reliability of operation is otherwise demonstrated. The bypass time interval allowed for a maintenance operation is specified in the Technical Specifications. Bypass indication may be applied administratively or automatically.

7.5.2.1.3.14 Access to Means of Bypassing

The design permits the manual bypassing of channels under appropriate administrative control.

7.5.2.1.3.15 Access to Setpoints Adjustments, Calibration, and Test Points

The design permits access to all setpoint adjustments, module calibration adjustments, and test points under appropriate administrative controls.

7.5.2.1.3.16 Identification of Monitoring Functions

Displays are indicated and identified down to the channel level.

7.5.2.1.3.17 System Repair

The PAMS is designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.

7.5.2.1.3.18 Identification

In order to provide assurance that the appropriate requirements are applied during the design, construction, maintenance, and operation of the plant, the PAMS equipment is identified distinctively to distinguish between redundant portions of the PAMS. The equipment, components, or modules mounted in assemblies that are clearly identified as being in the PAMS, do not themselves require identification.

7.5.2.2 Reactor Trip System Monitoring

This system is discussed in Section 7.2.

7.5.2.3 ESF Systems and ESF Supporting Systems

For a discussion of these systems, refer to Section 7.3.2.

7.5.2.4 Auxiliary Control Panel Instrumentation

For a discussion of this system, refer to Section 7.4.2.

7.5.2.5 Safe Shutdown Monitoring System

For a discussion of this system, refer to Section 7.4.2.

7.5.2.6 Bypassed and Inoperable Status Indication (IEEE 279, Section 4.13 and RG 1.47)

Bypassed and inoperable equipment conditions are governed by administrative procedures for ESF and ESF Support Systems. To add to the operator's knowledge of plant status, the administrative procedures are supplemented with automatic indication of the bypassed or inoperable status of each redundant portion of a system that performs a function important to safety.

The following design criteria were used in the selection of the status indication:

a) Automatically indicate a bypassed and inoperable status on a safety-related system and/or train.

b) Manual capability to activate each indication on a safety-related system and/or train.

The operator has sufficient information about the important safety-related systems which are disabled, removed from service, tested or being repaired to allow him to take the proper course of action.

7.5.2.7 Control Panel (Main Control Board)

This panel provides sufficient information to the operator concerning the different plant variables. With the help of display instrumentation, equipment status indication, bypassed and inoperable status indication and annunciation, the operator can properly assess the situation during various modes of the plant operation and take corrective or anticipatory action in order to maintain the plant in a safe condition.

For physical separation and wiring for redundant safety-related equipment, refer to Section 8.3.

REFERENCES: SECTION 7.5

7.5.1-1 CP&L Drawing Number CAR 2166-S-9000, Post-accident Monitoring Equipment Regulatory Guide 1.97, Revision 3

7.6 ALL OTHER INSTRUMENTATION SYSTEMS REQUIRED FOR SAFETY*

7.6.1 DESCRIPTION

This section includes a description of those instrumentation systems required for safety which have not been discussed in Sections 7.2 through 7.5. These systems include instrumentation for safety interlocks required to prevent overpressurization of the Residual Heat Removal System and the systems listed in Section 7.1.1.6.

7.6.1.1 Interlock Residual Heat Removal System Isolation Valves

The residual heat removal system (RHRS) pump suction isolation valves are normally closed and are only opened for residual heat removal after system indicated pressure is reduced to less than or equal to 363 psig and system temperature has been reduced to less than 350F.

There are two motor operated valves in series in each of the two residual heat removal pump suction lines from the reactor coolant system (RCS) hot legs. The two valves nearest the RCS (valves 8702A/V502 and 8702B/V500) are designated as the inner isolation valves, while the two valves nearest the residual heat removal pumps (valves 8701A/V503 and 8701B/V501) are designated as the outer isolation valves. The interlock features provided for the outer isolation valves, shown on Figure 7.6.1-1 are identical to those provided for the inner isolation valves, shown in Figure 7.6.1-2, except that equipment diversity is employed by virtue that pressure transmitter PT 402 is of a manufacture different than pressure transmitter PT 403.

Each valve is interlocked so that it cannot be opened unless the RCS pressure is below a preset pressure and valves 8809A (V575) and 8706A (V507), 8809B (V574) and 8706B (V506) are fully closed (see Figure 5.4.7-1). This interlock prevents the valve from being opened when the RCS pressure plus the residual heat removal pump pressure would be above the RHRS design pressure. An alarm for each valve will indicate when the valve is not shut and RCS pressure is high. Reactor coolant system wide range pressure signals for the valve interlocks are derived from transmitters which are located outside of containment.

7.6.1.2 Accumulator Isolation Valves Interlock

These signals to the accumulator isolation valves are designed to meet the following criteria:

a) Automatic opening of the accumulator valves when: 1) the reactor coolant system pressure exceeds a preselected value, or 2) a safety injection signal is initiated. Both signals shall be provided to the valves.*

b) Automatic removal (override) of any bypass feature, that is provided to allow an accumulator isolation valve to be closed for a short period of time when the RCS is at pressure, upon receipt of a safety injection signal.

The control circuit for these valves is shown on Figure 7.6.1-3. The valves and control circuits are further discussed in Sections 6.3.2 and 6.3.5.

---

* Further information is contained in the TMI Appendix.

The accumulator discharge isolation valves are motor operated, normally open valves which are controlled from the main control board. To prevent an inadvertent closing of these valves during normal operation, the accumulator valves motor circuit breakers will be administratively opened. Administrative control is required to ensure that these valves remain non-operational (circuit breakers are open) during normal power operation and plant shutdown, and that the valves remain operational (circuit breakers are closed) during start-up and cooldown.

These valves are interlocked such that:

a) They open automatically on receipt of a Safety Injection Signal (S signal) with the main control board switch in either the "NORMAL" or "SHUT" position.

b) They open automatically whenever the RCS pressure is above the safety injection unblock pressure (P-11) specified in the Technical Specifications only when the main control board switch is in the "NORMAL" position.

c) They cannot be closed as long as an "S" signal is present.

A control switch for each valve is provided on the MCB. These switches spring return to normal from the open position.

A redundant set of indicating lights is provided on the MCB for the accumulator isolation valves' position.

During plant shutdown, the accumulator valves are closed. To prevent an inadvertent opening of these valves during that period, the accumulator valve motor circuit breakers are opened or withdrawn. Administrative control is required to ensure that these valve circuit breakers are closed during the pre-startup procedures.

The accumulator normally open motor operated valves have alarms, indicating a malpositioning (with regard to their emergency core cooling system function during the injection phase). For the ECCS equipment not in a normal condition, an alarm is sounded in the Control Room and indicated on the monitor light boxes.

An alarm will also sound for any accumulator isolation valve under the following conditions when the RCS pressure is above the "safety injection unblocking pressure."

a) Valve motor operated limit switch indicates that the valve is not open.

b) Valve stem operated limit switch indicates that the valve is not open. The alarm of the condition can be silenced but will re-alarm at given time intervals.

7.6.1.3 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.

7.6.1.4 Cold Water Slug Injection

Cold water slug injection interlocks are not required since SHNPP does not utilize RCS loop isolation valves.

7.6.1.5 Spent Fuel Pool Cooling and Cleanup System

The Spent Fuel Pool Cooling System is controlled and monitored from the auxiliary equipment panel. The cleanup portion of the system is controlled from local panels. The system vital parameters such as high water temperature, and high, low and low-low water level conditions are indicated and alarmed in the Control Room. The spent fuel and new fuel pool inlet water low flow is alarmed in the Control Room and on a local panel. Fuel pool level and spent fuel pool cooling pump discharge low pressure are also alarmed on the fuel pool local panel.

The redundant Class IE monitoring instruments, such as temperature sensors and level switches for Unit 1 are located in the spent fuel and new fuel pools. (See Section 9.1.3 for the system description).

The fuel pool instrument logic and schematic diagram are shown on Figure 7.6.1 8 through 7.6.1-11.

7.6.1.6 ECCS Leak Detection

The ECCS Leak Detection System is described in Section 6.3.2.5.2.2.

7.6.1.7 Fire Protection and Detection Systems

See Section 9.5.1.2.3 for the description of the Fire Protection and Detection Systems.

7.6.1.8 Radiation Monitoring System

See Section 11.5 for the description of the Radiation Monitoring System.

7.6.1.9 Instrumentation and Control Power Supply System

The following is a description of the instrumentation and control power supply system:

a) Refer to Figure 7.6.1-4 for a single line diagram of instrumentation and control power supply system.

b) There are four inverters and four distribution panels. Each inverter is connected independently to one distribution panel.

c) The inverters provide a source of 118 volt, 60 Hz power for the operation of the nuclear steam supply system instrumentation. This power is derived from the 480 volt AC, 3φ, 60 Hz distribution system (preferred power supply), or from the station batteries which assure continued operation of instrumentation systems in the event of a station blackout.

d) Each inverter is also connected to a 120 VAC bypass power source and equipped with a static transfer switch. The static transfer switch will automatically align the output of the

inverter to the bypass power source upon inverter failure, inverter over-current, and inverter low output voltage or by manual alignment. The static transfer switch has an auto re-transfer feature which returns the output to the inverter, once the inverter output has returned to normal operating voltage and current remained within normal parameters for a predetermined time delay.

e) Each of four distribution panels may be connected to a back-up source of 120 volt AC power. The tie is through a local manually operated switch which is mechanically interlocked with the breaker connecting the inverter to the distribution panel such that the distribution panel cannot be connected to both sources simultaneously.

7.6.1.10 RHR Recirculation System Sump Isolation Valves Interlock

The details of achieving cold leg recirculation following safety injection are given in Section 6.3.2.8 and in Table 6.3.2-6. Figures 7.6.1-5 and 7.6.1-6 show the logic to automatically open the sump valves.

As noted in Table 6.3.2-3, protection logic is provided to automatically open the four safety injection system (SIS) recirculation sump isolation valves (8811A/V571 and 8812A/V573 in Train A and 8811B/V570 and 8812B/V572 in Train B) when two of four (2/4) refueling water storage tank (RWST) level indicators are less than the low-low level setpoint in conjunction with the initiation of the engineered safety features actuation signal ("S" signal). The S signal is initiated by the contact of a slave relay in the solid state protection system output cabinet that closes on safety injection and remains closed until manually reset from the main control board. This 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.

7.6.1.11 Interlocks for RCS Pressure Control During Low Temperature Operation

The basic function of the RCS pressure control during low temperature operation is discussed in Section 5.2.2. As noted in Section 5.2.2, this pressure control includes automatic actuation logic for two (of the three) pressurizer power operated relief valves (PORV's) to ensure that an automatic and independent RCS pressure control back-up feature is available to the operator during low temperature operations to mitigate any potential pressure transients. This system provides the capability for additional RCS inventory letdown, thereby maintaining RCS pressure within allowable limits. Refer to Sections 5.4.7, 5.4.10, 5.4.13, 7.7 and 9.3.4 for additional information on RCS pressure and inventory control during other modes of operation.

Analyses have shown that one PORV is sufficient to prevent violation of allowable limits due to anticipated mass and heat input transients. The mitigation system is required only during low temperature water solid operation. See Section 5.2.2.11 for a discussion of the analysis. 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 low temperature (see Section 5.2.2.11.2). The monitored system temperature signals are processed to generate the reference pressure limit program which is compared to the actual monitored RCS pressure. The system logic will first annunciate a main control board alarm whenever the measured pressure approaches within a pre-determined amount, thereby indicating a pressure transient is occurring, and on a further increase in measured pressure, an actuation signal is transmitted to

the power operated relief valves when required to mitigate the pressure transient. See Figure 7.6.1-7 for the block diagram showing the interlocks for RCS pressure control during low temperature operation. This control system is non-safety-related. However, isolation relays have been provided in the S.S.P.S. Cabinets for the two LTOPs valve control circuits to provide Safety grade contacts for the automatic actuation.

As shown on this figure, the generating station variables required for this interlock are channelized as follows:

1) Protection Set I

    a. Wide range RCS temperatures from hot legs

2) Protection Set II

    b. Wide range RCS temperatures from cold legs

3) Control Group 1

    c. Wide range RCS pressure (PT 440)

4) Control Group 4

    d. Wide range RCS pressure (PT 441)

The wide range temperature signals, as inputs to the Protection Sets I and II, continuously monitor RCS temperature conditions whenever plant operation is at a low temperature (see Section 5.2.2.11.2). In Protection Set I, each of the existing RCS hot leg wide range temperature channels will supply continuous analog input through an isolator to redundant auctioneering devices which are located in the Process Control Cabinet 5.

The lowest reading will be selected by one of the auctioneers as input to a function generator which calculates the reference pressure limit program considering the plant's allowable pressure and temperature limits. Available from Control Group 1 is the wide range RCS pressure signal which is located in Process Control Cabinet 5. The reference pressure from the function generator is compared to the actual RCS pressure monitored by the wide range pressure channel. The error signal derived from the difference between the reference pressure and the actual measured pressure will first annunciate a main control board alarm whenever the actual measured pressure approaches, within a predetermined pressure, the reference pressure. On a further increase in measured pressure, the error signal will generate an annunciated actuation signal. The actuation signal available from Solid State Protection System "A" will control PORV "A" whenever a temperature-dependent permissive signal from the lowest auctioneered temperature in Process Control Cabinet 8 is present. The lowest temperature is generated by both of the auctioneers. One derivation provides a permissive for the opposite train and one is used in the reference pressure limit program for PORV "B". The temperature-dependent permissive to the PORV's actuation device effectively disarms (blocks) the actuation signal at temperatures greater than the range of concern. Manual block switches can disable the permissive signals when operating in modes 1, 2 and 3. This will prevent unnecessary system actuation when at normal RCS operating conditions as a result of a failure in the process sensors.

The monitored generating station variables that generate the actuation signal for the "B" PORV are processed in a similar manner. In the case of PORV "B", the reference temperature available from Protection Set II is generated in Process Control Cabinet 8 from the lowest auctioneered wide range cold leg temperature; and the actual measured pressure signal is available from Process Control Cabinet 8. Therefore, the generating station variable signals from which the error signal is derived are provided from redundant and independent protection sets. 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. Upon sufficient RCS inventory letdown, the operating RCS pressure will decrease, clearing the actuation signal. Removal of this signal causes the PORV to close.

The control logic for the Low Temperature Overpressurization System has been designed to prevent a single failure of a temperature auctioneering device from preventing either Train A PORV or Train B PORV from performing its intended function. The hot-leg temperature inputs that normally supply the Train A auctioneering device, also supply an additional auctioneering device which provides the Train B PORV permissive. The cold-leg temperature inputs that normally supply the Train B auctioneering device, also supply an additional auctioneering device that provides the Train A PORV permissive. While the manual block switch is in the normal position the system remains automatic, with alarm annunciation, the potential single failure concern of the auctioneering device is eliminated.

7.6.2 ANALYSIS

7.6.2.1 Residual Heat Removal System Isolation Valves Interlock

Based on the scope definitions presented in IEEE Standard IEEE-279 "Criteria for Protection Systems" and IEEE-338 "Standard Criteria for the Periodic Testing of Protection Systems", 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 Standard 279-1971 will be applied with the following comments:

a) For the purpose of applying IEEE Standard 279-1971 to this circuit, the following definitions will be used.

    1) Protection System - The two valves in series in each line and all components of their interlocking and closure circuits.

    2) Protective Action - The maintenance of RHRS isolation from the RCS when RCS pressures are above the preset value.

b) Capability for test and calibration (IEEE-279 Section 4.10)

The above mentioned pressure interlock signals and logic will be tested on-line to the maximum extent possible without adversely affecting safety. This test will include the analog signal through to the train signal which activates the slave relay (the slave relay provides the final output signal the valve control circuit). This method is used since an actual actuation to permit

opening the valve could potentially leave only one remaining valve to isolate the low pressure RHRS from the RCS.

c) Multiple setpoints (IEEE-279 Section 4.15) - This requirement does not apply, as the setpoints are independent of mode of operation and are not changed.

Environmental qualification of the valves and wiring are discussed in Section 3.11.

7.6.2.2 Spent Fuel Pool Cooling and Cleanup System

Instrumentation for the Spent Fuel Pool Cooling and Cleanup Systems is provided for plant equipment protection and for the operator information about the system. The system is not a protection system as defined in IEEE-279. However, an analysis according to the applicable portion of IEEE-279 is provided for the safety-related portion of the system, spent fuel pool cooling.

a) Automatic initiation (IEEE-279 Section 4.1): there is no automatic initiation.

b) Single Failure Criterion (IEEE-279 Section 4.2, GDC 21, GDC 23, RG 1.53, BTP ICSB 18, IEEE-379).

   Compliance with a single failure criteria is accomplished by providing redundant instruments such as temperature elements, level switches and control. Failure of one channel will not affect the performance of the system.

c) Quality of components and module (IEEE-279 Section 4.3, Regulatory Guide 1.30).

   For discussion of Quality of components and module, refer to Section 7.3.2.2.3.

d) Equipment qualification (IEEE-279 Section 4.4, GDC 21, IEEE-323)

   Refer to Sections 3.10 and 3.11 for description of equipment qualification.

e) Channel integrity (IEEE-279 Section 4.5, Regulatory Guide 1.29, Regulatory Guide 1.100, IEEE-344, BTP ICSB 10)

   Type testing or analysis of components, separation of sensors and channels and qualification of cabling are utilized to ensure that the components and systems will maintain the functional capability required under applicable extreme conditions relating to environment, energy supply, malfunctions and accidents.

f) Channel independence (IEEE-279 Section 4.6 GDC 22, Regulatory Guide 1.75, IEEE-384).

   Channel independence is achieved by electrical and physical separation as described in Section 8.3.1.4.

g) Control and protection interaction (IEEE-279 Section 4.7, GDC-24)

   Refer to Section 7.3.2.2.7 for the discussion of control and protection function interaction.

h) Derivation of System Inputs (IEEE-279 Section 4.8)

System inputs are derived from direct measurement of the desired variables.

i) Capability for sensor check (IEEE-279 Section 4.9)

The sensors can be checked during normal operation.

j) Capability for test and calibration (IEEE-279 Section 4.10, GDC 21, GDC 40, Regulatory Guide 1.118, IEEE-338, or BTP ICSB 22).

The fuel pool cooling system is capable of being completely tested during normal plant operation in order to verify that each element of the system is capable of performing its intended functions.

k) Channel Bypass or Removal from Operation (IEEE-279 Section 4.11)

Equipment from one train may be removed from service without affecting plant operation.

l) Operating Bypasses (IEEE-279 Section 4.12)

Not Applicable. There are no operating bypasses in the fuel pool cooling system.

m) Indication of Bypasses (IEEE-279 Section 4.13) Regulatory Guide 1.47, BTP ICSB 21

Not applicable. There are no operating bypasses.

n) Access to Means for Bypassing (IEEE-279 Section 4.14)

Not applicable. There are no operating bypasses.

o) Multiple Setpoints (IEEE-279 Section 4.15)

Not Applicable. There are no multiple setpoints.

p) Completion of Protective Action Once it is Initiated

(IEEE-279 Section 4.16)

Not applicable. The system is manually operated.

q) Manual Initiation (IEEE-279 Section 4.17) Regulatory Guide 1.62

Cooling pump is started manually from the Unit 1 Control Room.

r) Access to Setpoint Adjustments, and Calibration and Test Point

(IEEE-279 Section 4.18) Regulatory Guide 1.105

Flow and temperature setpoint adjustment can be done at the process instrument cabinet and the level switch setpoint adjusting is done at the switch assembly by individually adjusting displacer position along the suspension cable.

s) Identification of Protective Actions (IEEE-279 Section 4.19)

Not applicable to this system.

t) Information Readout (IEEE-279 Section 4.20)

The status of all the pumps is indicated in the Control Room and locally. Flow discharge pressure is alarmed locally. Spent and new fuel temperature is indicated and alarmed in the Control Room. Fuel pool water level is indicated and alarmed in the Control Room and alarmed locally.

u) System Repair (IEEE-279 Section 4.21)

Replacement or repair of actuated components is accomplished as allowed by the Technical Specifications, Chapter 16.

v) Identification (IEEE-279 Section 4.22, IEEE-494)

Physical identification of fuel pool cooling system components (motor control centers, cables, cable trays, conduits, are described in Section 8.3.1.3).

7.6.2.3 Instrumentation and Control Power Supply System

There are two independent 480V AC power sources, each serving two inverters. Therefore, loss of either of the two 480 V AC power sources affect only two of the four inverters.

There are two independent batteries and battery chargers. Each battery is attached to a bus serving two inverters.

Since not more than two inverters are connected to the same bus, a loss of a single bus can only affect two of the four inverters.

Each inverter is independently connected to its respective instrument distribution panel so that the loss of an inverter cannot affect more than one of the four distribution panels.

Each inverter is also connected to a 120 VAC bypass power source and equipped with a static transfer switch. The static transfer switch will automatically align the output of the inverter to the bypass power source upon inverter failure, inverter over-current, and inverter low output voltage or by manual alignment. The static transfer switch has an auto re-transfer feature which returns the output to the inverter, once the inverter ouput has returned to normal operating voltage and current and remained within normal parameters for a predetermined time delay.

In addition, each of the four distribution panels is connected to a backup 120V AC power source. Each distribution panel can receive power from the 120V AC backup source under operator control. The transfer breakers/switches are mechanically interlocked to prevent paralleling the inverters with the backup source. Refer to Figure 7.6.1-4.

Therefore, no single failure in the instrumentation and control power supply system or its associated power supplied can cause a loss of power of more than one of the redundant loads.

The inverters are designed to maintain their outputs within acceptable limits. The loss of the AC or DC inputs are alarmed in the Control Room, as is the loss of an inverters output. There are no inverter breaker controls on the control board, as no manual transfers are necessary in the event of loss of the 480V AC preferred power source.

Physical separation and provisions to protect against fire are discussed in Chapter 8.

Based on the scope definitions presented in References 7.6.2-1 through 7.6.2-3, the criterion which is applicable to the instrumentation and control power supply system is IEEE Standard 308 (September 1971); for the availability of electric power sources, IEEE308 (October 1980) is applicable. The design is in compliance with IEEE Standard 308 (September 1971) and Regulatory Guide 1.6 and 1.32 (see Section 1.8). Availability of this system is continuously indicated by the operational status of the systems it serves and is verified by periodic testing performed on the served systems. The inverters have been seismically qualified as discussed in Section 3.10.

7.6.2.4 RHR Recirculation System Isolation Sump Valves Interlock

a) Initiation Circuit - the 2/4 low-low RWST level as shown on Figure 7.6.1-6, is the trip signal, which in coincidence with the "S" signal, provides the initiation function which would automatically open the containment sump isolation valves.

b) Logic - The logic function derived from the RWST level sensors and the "S" signal are depicted on Figure 7.6.1-5.

c) Bypass - The manual reset logic function is shown on Figure 7.6.1-5 and its purpose and action is described above in Section 7.6.1. As noted, the "S" signal is retained by sealing it in (i.e., it is latched) and is not removed by action of the main safety injection reset that is used by the operator per emergency procedures to block the "S" signal to certain other equipment prior to realignment for switchover to the recirculation mode following a postulated LOCA.

d) 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 bistables. The RWST level channel bistables are:

    1) Normally de-energized.

    2) De-energized on loss of power.

    3) Energized on low-low setpoint.

    Each level channel bistable 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 bistables receive an RWST level signal lower than the low-low level setpoint, following the generation of an "S" signal.

e) Sequence - This circuit is energized directly from the SSPS output cabinet and is not sequenced following an accident that requires its functioning.

f) 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.

g) 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 Sections 3.10 and 3.11. It is noted that there is functional diversity provided in that manual operation is available as a backup to the semi-automatic mode.

h) Actuated Devices - The actuated devices are the four motor control center starters, one for each of the motor operated sump valves, 8811 A&B and 8812 A&B.

7.6.2.5 RCS Pressure Control During Low Temperature Operation

Many criteria presented in IEEE 279-1971 and IEEE 338-1971 standards do not apply to the interlocks for RCS pressure control during low temperature operation, because the interlocks do not perform a protective function but rather provide automatic pressure control at low temperatures as backup to the operator. However, although IEEE-279 criteria do not apply, some advantages of the dependability and benefits of an IEEE-279 design have accrued by including selected elements as noted above in the protection sets and by organizing the control of two (of the three) PORV's into dual channels wherever practical. Either of the two PORV's 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 as shown in Figure 7.6.1-7.

2) Testing capability for elements of the interlocks within (not external to) the protection system is consistent with the testing principles and methods discussed in Section 7.2.2.2.3.10. It should be noted that there is an annunciator which provides an alarm when there is low auctioneered RCS temperature (see Section 5.2.2.11.2) coincident with a closed position of the motor operated (MOV) pressurizer relief isolation valves. This MOV is in the same fluid path as the PORV, with a separate MOV used and alarmed associated with the second PORV.

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 8.0.

4) Spurious operation at power is prevented by manual block switches provided in the permissive circuit for each PORV.

REFERENCES: SECTION 7.6

7.6.2-1 The Institute of Electrical and Electronic Engineers, Inc., "IEEE Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations," IEEE Standard 308-1971; IEEE 308-1980 for availability of electric power sources.

7.6.2-2 The Institute of Electrical and Electronic Engineers, Inc., "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations," IEEE Standard 279-1971.

7.6.2-3 The Institute of Electrical and Electronic Engineers, Inc., "IEEE Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection System," IEEE Standard 338-1971.

7.7 CONTROL SYSTEMS NOT REQUIRED FOR SAFETY

The general design objectives of the plant control systems are:

1. To establish and maintain power equilibrium between the primary and secondary system during steady state Unit operation.

2. To constrain operational transients so as to preclude Unit trip and reestablish steady state Unit operation.

3. To provide the reactor operator with monitoring instrumentation that indicates all required input and output control parameters of the systems and provides the operator the capability of assuming manual control of the system.

A comparison of the control systems not required for safety of a similar facility is contained in Table 7.1.1-1.

7.7.1 DESCRIPTION

The plant control systems described in this section perform the following functions:

Harris is designed to accept a step load increase or decrease of 10 percent and a ramp increase or decrease of 5 percent per minute within the load range of 15 percent to 100 percent without reactor trip, steam dump, or pressurizer relief actuation, subject to possible xenon limitations.

Maintains reactor coolant average temperature (T_{avg}) within prescribed limits by creating the bank demand signals for moving groups of rod cluster control assemblies during normal operation and operational transients. The T_{avg} control also supplies a signal to pressurizer water level control, and steam dump control.

1. Rod Control System - Provides for reactor power modulation by manual or automatic control of control rod banks in a preselected sequence and for manual operation of individual banks.

Systems for monitoring and indicating:

a. Provide alarms to alert the operator if the required core reactivity shutdown margin is not available due to excessive control rod insertion.

b. Display control rod position.

c. Provide alarms to alert the operator in the event of control rod deviation exceeding a preset limit.

The automatic rod control system is designed to maintain a programmed average temperature in the reactor coolant by regulating the reactivity within the core. The system is capable of restoring the average temperature to within ± 1.5°F of the programmed temperature following design load changes.

The programmed average temperature is a linear ramp from the no-load average temperature to the nominal full power average temperature based on the power level as sensed by turbine First Stage pressure. The Chapter 15 analysis assumes actual RCS average temperature is within a band of +6.0/-6.8°F about the program value, including instrument uncertainties (Reference 7.7.1-2), and accounting for the capability of the automatic rod control system. When automatic rod control is not in service, manual control of RCS indicated average temperature to the program value is accomplished by the operator, within a band determined to account for instrument uncertainties.

At low power levels prior to placing automatic rod control in service, indicated average temperature is controlled to within ± 2°F of the programmed average temperature calculated based on reactor power. During turbine roll and synchronization, indicated average temperature may be increased up to 4°F above the program value (while the Chapter 15 accident analysis accommodates a +6.5/-6.8°F band due to larger possible range of variation in the actual fluid conditions at low power conditions).

The rod control system is designed to automatically control the reactor in the power range between 15 and 100 percent of rated power for the following design transients:

a. ±10 percent step changes in load.

b. 5 percent/minute ramp loading and unloading.

2. Plant Control System Interlocks - Prevent further withdrawal of the control banks when signal limits are approached that indicate the approach to a DNBR limit or kW/ft. limit, and limit automatic turbine load increases to values for which the Nuclear Steam Supply System has been designed.

3. Pressurizer Pressure Control - Maintains or restores the pressurizer pressure 38 psi above to 50 psi below the design pressure (Reference 7.7.1-1) (which is within reactor trip and relief and safety valve actuation setpoint limits) following normal operational transients that

induce pressure changes by control (manual or automatic) of heaters and spray in the pressurizer. Provides steam relief by controlling the power operated relief valves. The above-noted +38/-50 psi tolerance conservatively bounds the± 33.4 psi result from Reference 7.7.1-2.

The pressurizer pressure control system maintains a pressure at the set value by four means:

a. Spray

b. Relief Valves

c. Proportional Heaters

d. Back-up Heaters

Together, the heaters, spray, and relief valves maintain the pressure at the setpoint value and prevent reactor trip as a result of pressure variations caused by operational transients.

4. Pressurizer Water Level Control - Establishes and maintains pressurizer water level within specified limits as a function of the average coolant temperature. Changes in level are caused by coolant density changes induced by loading, operational, and unloading transients. Level changes are produced by means of charging flow control (manual or automatic) as well as by manual selection of letdown orifices.

   Maintaining coolant level in the pressurizer within prescribed limits by actuating the charging and letdown system thus provides control of the reactor coolant water inventory.

   The water inventory in the Reactor Coolant System (RCS) is maintained by the Chemical and Volume Control System (CVCS). During normal plant operation, the pressurizer level is controlled by the charging flow which is controlled by the pressurizer level controller. The pressurizer water level is programmed as a function of the coolant average temperature. The pressurizer water level decreases as the load is reduced from full load. This decrease is the result of coolant contraction following a programmed coolant temperature reduction as the reactor power decreases. The programmed level is designed to match as nearly as possible the level changes resulting from the coolant temperature changes. To permit manual control of the pressurizer level during startup and shutdown operations, the charging flow can be manually regulated from the main control room.

5. Steam Generator Water Level Control - Establishes and maintains the steam generator water level within predetermined limits during normal operating transients.

   The Steam Generator Water Level Control System also restores the steam generator water level to within predetermined limits at Unit trip conditions. It regulates the feedwater flow rate such that, under operational transients, reactor coolant system water volume does not decrease below a minimum value. Steam generator water inventory control is manual or automatic through the use of feedwater control valves.

   The Harris Plant steam generator level control system utilizes a fixed reference level; that is, for all power levels there is a water level which is maintained. Each steam generator is equipped with a three-element feedwater controller (feedwater flow, steam flow, and water

level) which maintains a programmed water level on the secondary side of the steam generator during normal plant operation (See Figure 7.7.1-6). This controller continuously compares measured feedwater flow, steam flow, a compensated steam generator downcomer water level signal, and a fixed reference water level to regulate the main feedwater control valve position. Manual override of the steam generator level control system is also provided.

6. Steam Dump Control - Harris is designed to accept a 50 percent load rejection from full power without incurring reactor trip. Steam is dumped to the condenser and/or the atmosphere as necessary to accommodate excess power generation in the reactor during turbine load reduction transients.

   Ensures that stored energy and residual heat are removed following a reactor trip to bring the plant to equilibrium no-load conditions without actuation of the steam generator safety valves.

   Maintains the plant at no-load conditions and permits a manually controlled cooldown of the plant.

   The steam dump system comprises 14 valves which can bypass steam to the condenser and to the atmosphere. Included in the 14 valves are the eight atmospheric relief valves. Depending on the full power vessel average temperature, the total steam dump capacity is approximately 66 to 86 percent of the rated steam flow.

   The condenser and atmospheric steam dump valves are provided with the following signals:

   a. An on-off signal to solenoids in the air supply line determines whether or not air is supplied to the valve.

   b. An on-off signal to a solenoid (one per dump valve) bypasses the valve positioner and allows the dump valve to be rapidly tripped open.

   c. A modulate signal is sent to the valve positioner. When the positioner is not bypassed (that is, the dump valve is not tripped open), the dump valve position depends upon the magnitude of the modulating signal.

7. Incore Instrumentation - Provides information on the neutron flux distribution and on the core outlet temperatures at selected core locations.

7.7.1.1 Reactor Control Rod System

The Reactor Control Rod System enables the nuclear plant to follow load changes automatically including the acceptance of step load increases or decreases of 10 percent and ramp increases or decreases of 5 percent per minute within the load range of 15 percent to 100 percent without reactor trip, steam dump, or pressure relief valve actuation (subject to possible xenon limitations). The system is also capable of restoring coolant average temperature to within the programmed temperature deadband following a change in load. Manual control rod operation may be performed at any time within the range of defined insertion limits.

The Reactor Control Rod System controls the reactor coolant average temperature by regulation of control rod bank position. The reactor coolant loop average temperatures are determined from hot leg and cold leg measurements in each reactor coolant loop. There is an average coolant temperature (T_{avg}) computed for each loop, where:

$$T_{avg} = \frac{T_{hot} + T_{cold}}{2}$$

The error between the programmed reference temperature (based on turbine First Stage pressure) and the median of the T_{avg} measured temperatures (which is processed through a lead-lag compensation unit) from each of the reactor coolant loops constitutes the primary control signal as shown in general on Figure 7.7.1-1 and in more detail on the functional diagrams shown in Figure 7.2.1-1, Sheet 9. The system is capable of restoring coolant average temperature to the programmed value following a change in load. The programmed coolant temperature increases linearly with turbine load from zero power to the full power condition. The T_{avg} also supplies a signal to pressurizer level control, steam dump control, and rod insertion limit monitor.

The temperature channels needed to derive the temperature input signals for the Reactor Control Rod System are fed from protection channels via isolation amplifiers.

An additional control input signal is derived from the reactor power versus turbine load mismatch signal. This additional control input signal improves system performance by enhancing response and reducing transient peaks.

The core axial power distribution is controlled during load follow maneuvers by changing (a manual operator action) the combination of the boron concentration in the Reactor Coolant System (RCS) and control rod position. The main control board AFD (axial flux difference) meter (see Section 7.7.1.3.1) allows the operator to monitor AFD and compare the current value to the allowable operating band. Adding boron to the reactor coolant will reduce T_{avg} and cause the rods (through the Rod Control System) to move toward the top of the core. This action will reduce power peaks in the bottom of the core. Likewise, removing boron from the reactor coolant will move the rods further into the core to control power peaks in the top of the core.

7.7.1.2 Rod Control System

The Rod Control and Position Indication System receives rod speed and direction signals from the T_{avg} control system. The rod speed demand signal varies over the corresponding range of 3.75 to 45 in. per minute (6 to 72 steps/minute) depending on the magnitude of the input signal. Manual control is provided to move control banks (in overlap) in or out at a prescribed fixed speed.

When the turbine load reaches approximately 15 percent of rated load, the operator may select the "AUTOMATIC" mode, and rod motion is then controlled by the Reactor Control Rod System. A permissive interlock C-5 (see Table 7.7.1-1) derived from measurements of turbine First Stage pressure prevents automatic control when the turbine load is below 15 percent. In the "AUTOMATIC" mode, the rods are again withdrawn (or inserted) in a predetermined programmed sequence by the automatic programming with the control interlocks (see Table 7.7.1-1).

The shutdown banks are typically in the fully withdrawn position during normal operation and are moved to this position at a constant speed by manual control prior to criticality. A reactor trip signal causes them to fall by gravity into the core. There are three shutdown banks.

The control banks are the only rods that can be manipulated under automatic control. Each control bank is divided into two groups to obtain smaller incremental reactivity changes per step. All rod control cluster assemblies in a group are electrically paralleled to move simultaneously. There is individual position indication for each rod cluster control assembly.

Power-to-rod drive mechanisms is supplied by two motor generator sets operating from two separate 480 volt, three-phase buses. Each generator is the synchronous type and is driven by a 150 HP induction motor. The AC power is distributed to the rod control power cabinets through the two series connected reactor trip breakers.

The variable speed rod drive programmer affords the ability to insert small amounts of reactivity at low speed to accomplish fine control of reactor coolant average temperature about a small temperature deadband, as well as furnishing control at high speed. A summary of the rod cluster control assembly sequencing characteristics is given below.

a) Two groups within the same bank are stepped such that the relative position of the groups will not differ by more than one step.

b) The control banks are programmed such that withdrawal of the banks is sequenced in the following order: control bank A, control bank B, control bank C, and control bank D. The programmed insertion sequence is the opposite of the withdrawal sequence; i.e., the last control bank withdrawn (bank D) is the first control bank inserted.

c) The control bank withdrawals are programmed such that when the first bank reaches a preset position, the second bank begins to move out simultaneously with the first bank which continues to move toward its fully withdrawn position. When the second bank reaches a preset position, the third bank begins to move out, and so on. This withdrawal sequence continues until the Unit reaches the desired power level. The control bank insertion sequence is the opposite.

d) Overlap between successive control banks is adjustable between 0 to 50 percent (0 and 115 steps), with an accuracy of $\pm$ 1 step.

e) Rod speeds for either the shutdown banks or manual operation of the control banks are capable of being controlled between a minimum of 8 steps per minute and a maximum of 72 steps per minute.

7.7.1.3 Plant Control Signals for Monitoring and Indicating

7.7.1.3.1 Monitoring functions provided by the nuclear instrumentation system

The power range channels are used to measure power level, axial flux difference and radial flux tilt. These channels are capable of recording (via ERFIS) overpower excursions up to 200 percent of full power. Suitable alarms are derived from these signals as described below.

Basic power range signals are:

a) Total current from a power range detector (four signals from separate detectors); these detectors are vertical and have a total active length of approximately 10 ft.

b) Current from the upper half of each power range detector (four signals).

c) Current from the lower half of each power range detector (four signals).

Derived from these basic signals are the following including standard signal processing for calibration).

a) Indicated nuclear power (four signals).

b) Indicated axial flux difference (AFD), derived from upper half flux minus lower half flux (four signals).

Alarm functions derived are as follows:

1. Deviation (maximum minus minimum of four) in indicated nuclear power.

2. Upper radial tilt (maximum to average of four) on upper half currents.

3. Lower radial tilt (maximum to average of four) on lower half currents.

Nuclear power and AFD is selectable for recording. Indicators are provided on the main control board for nuclear power and for AFD.

The AFD deviation alarms are derived from the plant process computer which determines the 1 minute averages of the excore detector outputs to monitor flux in the reactor core and alerts the operator if alarm conditions exist. Various types of alarm messages are output. When using wide AFD bands (Siemens refers to as PDC-3 and Westinghouse refers to as relaxed axial offset control (RAOC)) an alarm message is output upon determining an AFD value which on two or more channels exceeds the prescribed AFD operating band alarm limit. The alarm limits are typically 2% less than the COLR limit to allow operator response time.

Additional background information on the Nuclear Instrumentation System can be found in Section 7.2.

7.7.1.3.2 Rod position monitoring

Two separate systems are provided to sense and display control rod position as described below:

1. Digital Rod Position Indication System - The digital rod position indication system measures the position of each control rod using a detector which consists of discrete coils mounted concentrically with the rod drive pressure housing. The coils are located axially along the pressure housing and magnetically sense the entry and presence of the rod drive shaft through its centerline. For each detector, the coils are interlaced into two data channels, and are connected to the containment electronics (Data A and B) by separate multi-conductor cables. By employing two separate channels of information, the digital rod position indication system can continue to function (at reduced accuracy)

when one channel fails. Multiplexing is used to transmit the digital position signals from the containment electronics to the main control board display unit.

The AEP-1 display unit contains a column of light-emitting diodes (LEDs) for each rod. At any given time, the one LED illuminated in each column shows the position for that particular rod. Since shutdown rods are typically fully withdrawn with the plant at power, their position is displayed every 6 steps only from rod bottom to 18 steps and from 210 steps to 228 steps. All intermediate positions of the rod are represented by a single "transition" LED. Each rod of the control banks has its position displayed every 6 steps throughout its range of travel.

Included in the system is a rod at bottom signal for each rod that operates a local alarm. Also, a control room annunciator is actuated when any shutdown rod or control bank A rod is at bottom.

2. Demand Position System - The demand position system counts pulses generated in the Rod Drive Control System to provide a digital readout of the demanded bank position.

   The demand position and digital rod position indication systems are separate systems, but safety criteria were not involved in the separation, which was a result only of operational requirements. Operating procedures require the reactor operator to compare the demand and indicated (actual) readings from the Rod Position Indication System so as to verify operation of the Rod Control System.

7.7.1.3.3 Control bank rod insertion monitoring

When the reactor is critical, the normal indication of reactivity status in the core is the position of the control bank in relation to reactor power (as indicated by the reactor coolant system loop ΔT) and coolant average temperature. These parameters are used to calculate insertion limits for the control banks. Two alarms are provided for each control bank.

1. The "low" alarm alerts the operator of an approach to the rod insertion limits requiring boron addition by following normal procedures with the CVCS.

2. The "low-low" alarm alerts the operator to take action to add boron to the RCS as directed by the emergency boration procedures.

The rod insertion limit alarms only provide alarms at the Technical Specification Core Operating Limit Report (COLR) rod insertion limit for banks C and D and only when the rods are moved in overlap sequence. The control bank rod insertion limit monitor low-low alarm setpoint and Technical Specification COLR rod insertion limit are identical only for D-Bank (at all power levels) and for C-Bank. The power level where the C bank COLR rod insertion limit and the low-low rod insertion limit alarm meet varies with the all rods out park position (44.6% for 225 steps, 43% for 222 steps, 46.2% for 228 steps, and 47.8% for 231 steps). The rod insertion limit monitor low and low-low alarm is set non-conservatively for A-Bank, B-Bank and C-Bank (power > above limits). This is inherent to the design. The low-low rod insertion limit alarms are the same as the Core Operating Limits Report (COLR) rod insertion limit only for control banks C and D and only when the system is operated in overlap mode. The low alarm will occur when the calculated position of D-Bank is 10 steps above the curve provided in the COLR. The low low alarm will occur for D Bank at the COLR limit. With %ΔT between 0% and the power levels

listed above for the various all rods out park positions, the C-Bank low and low-low alarms will occur simultaneously with the D-Bank alarms.

The purpose of the control bank rod insertion monitor is to given warning to the operator of excess 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 cold leg, which is a direct function of reactor power and T_{avg} , which is programmed as a function of power. The rod insertion monitor uses parameters for each control rod bank as follows:

$$Z_{LL} = A(\Delta T)_{auct} + B(T_{avg})_{auct} + C$$

where:

Z_{LL}	=	maximum permissible insertion limit for affected control bank
$(\Delta T)_{auct}$	=	median ΔT of all loops
$(T_{avg})_{auct}$	=	median T_{avg} of all loops
A,B,C,	=	Constants chosen to maintain $Z_{LL} \geq$ actual limit based on physics calculations

The control rod bank demand position (Z) is compared to Z_{LL} as follows:

If $Z - Z_{LL} \leq D$ setpoint, a low alarm is actuated.

If $Z - Z_{LL} \leq E$ setpoint, a low-low alarm is actuated.

Actuation of the low alarm alerts the operator of an approach to a reduced shutdown reactivity situation. Administrative procedures require the operator to add boron through the CVCS. Actuation of the low-low alarm normally requires the operator to initiate emergency boration procedures. Following a rapid power reduction, this alarm may be received and not be indicative of a reduced shutdown reactivity condition. This is primarily due to xenon not being at equilibrium for the new power level. In this situation normal boration procedures may be followed to restore the rods to above the insertion limits within two hours as required by the COLR. The value for "E" is chosen such that the low-low alarm would normally be actuated before the insertion limit is reached. The value for "D" is chosen to allow the operator to follow normal boration procedures. Figure 7.7.1-2 shows a block diagram representation of the control rod bank insertion monitor. The monitor is shown in more detail on the functional diagrams shown in Figure 7.2.1-1, Sheet 9. In addition to the rod insertion monitor for the control banks, the plant computer, which monitors individual rod positions, provides an alarm that is associated with the rod deviation alarm discussed in Section 7.7.1.3.4. An alarm is provided to warn the operator if any shutdown rod cluster control assembly leaves the fully withdrawn position.

Rod insertion limits are determined by:

1. Establishing the allowed rod reactivity insertion at full power consistent with the purposes given above.

2. Establishing the differential reactivity worth of the control rods when moved in normal sequence.

3. Establishing the change in reactivity with power level by relating power level to rod position.

4. Linearizing the resultant limit curve. All key nuclear parameters in this procedure are measured as part of the low power physics test program.

Any unexpected change in the position of the control bank under automatic control, or a change in coolant temperature under manual control, provides a direct and immediate indication of a change in the reactivity status of the reactor. In addition, samples are taken periodically of coolant boron concentration. Variations in concentration during core life provide an additional check on the reactivity status of the reactor, including core depletion.

7.7.1.3.4 Rod deviation alarm

The position of any control rod is compared to the position of other rods in the bank. A rod deviation alarm is generated by the digital rod position indication system if a present rod deviation limit is exceeded. The deviation alarm of a shutdown rod is based on a preset insertion limit being exceeded.

The demanded and measured rod position signals are also monitored by the plant computer which provides a visual printout and an audible alarm whenever an individual rod position signal deviates from the other rods in the bank by a preset limit. The alarm can be set with appropriate allowance for instrument error and within sufficiently narrow limits to preclude exceeding core design hot channel factors.

Figure 7.7.1-3 is a block diagram of the rod deviation comparator and alarm system implemented by the plant computer. Additionally, the digital rod position indication system contains rod deviation circuitry that detects and alarms on the following conditions:

When any two rods within the same control bank are misaligned by a preset distance (≥ 12 steps), and

When any shutdown rod is at or below 210 steps.

7.7.1.3.5 Rod bottom alarm

A rod bottom signal for the control rods in the digital rod position indication system is used to operate a control relay, which generates the "ROD BOTTOM ROD DROP" alarm.

7.7.1.4 Plant Control System Interlocks

The listing of the plant control system interlocks, along with the description of their derivations and functions, is presented in Table 7.7.1-1. The designation numbers for these interlocks are

preceded by "C." The development of these logic functions is shown in the functional diagrams (see Figure 7.2.1-1).

7.7.1.4.1 Rod stops

Rod stops are provided to prevent abnormal power conditions which could result from excessive control rod withdrawal initiated by either a control system malfunction or operator violation of administrative procedures.

Rod stops are the C-1, C-2, C-3, C-4, and C-5 control interlocks identified in Table 7.7.1-1. The C-3 rod stop derived from overtemperature delta temperature (OTΔT) and the C-4 rod stop derived from overpower delta temperature (OPΔT) are also used for turbine runback, which is discussed below.

7.7.1.4.2 Automatic turbine load runback

Automatic turbine load runback is initiated by an approach to an overpower or overtemperature condition. This will prevent high-power operation that might lead to an undesirable condition which, if reached, would be terminated by a reactor trip.

Turbine load reference reduction is initiated by either an overtemperature or overpower ΔT signal. Two-out-of-three 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 overpower condition.

For either condition in general

$$\Delta T_{rod\ stop} = \Delta T_{setpoint} - B_p$$

where:

B_p = a setpoint bias

where ΔT setpoint refers to the Overtemperature ΔT reactor trip value and the Overpower ΔT reactor trip value for the two conditions.

The turbine runback is continued until ΔT is equal to or less than $\Delta T_{rod\ stop}$.

This function serves to maintain an essentially constant margin to trip.

7.7.1.4.3 Turbine loading stop

An interlock (C-16) is provided to limit turbine loading during a rapid return to power transient when a reduction in reactor coolant temperature is used to increase reactor power (through the negative moderator coefficient). This interlock limits the reduction in coolant temperature so that it does not reach cooldown accident limits and preserves satisfactory steam generator

operating conditions. Subsequent automatic turbine loading can begin after the interlock has been cleared by an increase in coolant temperature which is accomplished by reducing the boron concentration in the coolant.

7.7.1.5 Pressurizer Pressure Control

The reactor coolant system pressure is controlled by using either the heaters (in the water region) or the spray (in the steam region) of the pressurizer plus steam relief for large transients. The electrical immersion heaters are located near the bottom of the pressurizer. A portion of the heater group is proportionally controlled to correct small pressure variations. These variations are caused by heat losses, including heat losses due to a small continuous spray. The remaining (back-up) heaters are turned on automatically when the pressurizer pressure controlled signal demands approximately 100 percent proportional heater power.

The spray nozzles are located in 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 condition, 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 the actuation of a high-pressure reactor trip for the above condition.

A block diagram of the Pressurizer Pressure Control System is shown on Figure 7.7.1-4.

7.7.1.6 Pressurizer Water Level Control

The pressurizer operates by maintaining a steam cushion over the reactor coolant. As the density of the reactor coolant varies with temperature, the steam water interface is adjusted to compensate for cooling density variations with relatively small pressure disturbances.

The water inventory in the RCS is maintained by the CVCS. 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 median average temperature (auctioneered) being used. The pressurizer water level decreases as the load is reduced from full load. This is a result of coolant contraction following programmed coolant temperature reduction from full power to low power. The programmed level is designed to match as nearly as possible the level changes resulting from the coolant temperature changes.

To control pressurizer water level during startup and shutdown operations, the charging flow is manually regulated from the Control Room. The letdown line isolation valves are closed on low pressurizer level.

A block diagram of the Pressurizer Water Level Control System is shown on Figure 7.7.1-5. Reference 7.7.1-3 documents a +5.0/-5.2% level span controller uncertainty, which is bounded by the ±6.75% uncertainty assumed for safety analyses.

7.7.1.7 Steam Generator Water Level Control

Each steam generator is equipped with a three-element feedwater flow controller which maintains a fixed reference water level. The three-element feedwater controller regulates the feedwater valve by continuously comparing the feedwater flow signal, the water level signal, the fixed reference level and the pressure compensated steam flow signal.

Continued delivery of feedwater to the steam generators is required as a sink for the heat stored and generated in the reactor following a reactor trip and turbine trip. An override signal closes all feedwater valves when the average coolant temperature is below a given temperature and the reactor has tripped. Manual override of the Feedwater Control System is available at all times.

When the nuclear plant is operating at very low power levels (as during startup), the steam and feedwater flow signals will not be usable for control. Therefore, a secondary automatic control system is provided for operation at low power. This system uses the steam generator water level and nuclear power signals in a feed-forward control scheme to position a bypass valve which is in parallel with the main feedwater regulating valve. Switchover from the Bypass Feedwater Control System (low power) to the Main Feedwater Control System is initiated by the operator.

A block diagram of the Steam Generator Water Level Control System is shown in Figure 7.7.1-6.

7.7.1.8 Steam Dump Control

The Steam Dump System is designed to accept a 50 percent load rejection from full power without tripping the reactor.

The Steam Dump System is able to accommodate this abnormal load rejection and to reduce the effects of the transient imposed upon the RCS. By bypassing main steam directly to the condenser and/or the atmosphere, an artificial load is thereby maintained on the RCS. The RCS 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 first stage pressure and the lead-lag compensated auctioneered median 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 First Stage pressure. It is provided to unblock the dump valves when the rate of load rejection exceeds a preset value corresponding to a 10 percent step load decrease or a sustained ramp load decrease of 5 percent per minute.

A second interlock is provided to unblock the atmospheric steam dump valves in case of a large load rejection. As above, the rate of decrease in the turbine load is determined. The valves are unblocked when the rate exceeds a value corresponding to a 40 percent step load decrease.

A block diagram of the Steam Dump System is shown on Figure 7.7.1-8.

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 the difference between the lead-lag compensated median T_{avg} and the reference T_{avg} which is based on turbine first stage pressure.

The T_{avg} signal is the same as that used in the RCS. 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 dumping. Since control rods are available in this situation, steam dumping terminates as the error comes within the maneuvering capability of the control rods.

7.7.1.8.2 Turbine trip steam dump controller

Following a turbine trip, the load rejection steam dump controller is defeated and the turbine trip steam dump controller becomes active. Since control rods are not available in this situation, the demand signal is the error signal between the lead-lag compensated median 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.

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 and reactor trip on load rejection.

7.7.1.9 Incore Instrumentation

The Incore Nuclear 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 7.7.1-9.

7.7.1.9.1 Thermocouples

Chromel-alumel thermocouples are threaded into guide tubes that penetrate the reactor vessel head through seal assemblies, and terminate at the exit flow end of the fuel assemblies. The thermocouples are provided with two primary seals, a conoseal and Grafoil seal from conduit to head. Thermocouple readings are monitored by one or more of the plant computer systems.

7.7.1.9.2 Moveable neutron flux detector drive system

Miniature fission chamber detectors can be remotely positioned in retractable guide thimbles to provide flux-mapping of the core. The stainless steel detector shell is welded to the leading end of a helical wrap drive cable and to a stainless steel sheathed coaxial cable. The retractable thimbles, into which the miniature detectors are driven, are pushed into the reactor core through conduits which extend from the bottom of the reactor vessel down through the concrete shield area and then up to a thimble seal table. Their distribution over the core is nearly uniform with about the same number of thimbles located in each quadrant.

The thimbles are closed at the leading ends, are dry inside, and serve as the pressure barrier between the reactor water pressure and the atmosphere. Mechanical seals between the retractable thimbles and the conduits are provided at the seal table. During reactor operation, the retractable thimbles are stationary. They are extracted downward from the core during refueling to avoid interference within the core. A space above the seal table is provided for the retraction operation.

The drive system for the insertion of the miniature detectors consists basically of drive assemblies, 5-path transfer assemblies, and 10-path transfer assemblies, as shown in Figure 7.7.1-9. 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 end 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. Each detector accesses thimble locations via the 5- and 10 path rotary assemblies.

7.7.1.9.3 Control and readout description

The control and readout system provides means for inserting the miniature neutron detectors into the reactor core and withdrawing the detectors while plotting neutron flux versus detector position. The control system is located in the Control Room. Limit switches in each transfer device provide feedback of path selection operation. Each gear box drives a resolver for position feedback. One 5-path transfer selector is provided for each drive unit to insert the detector in one of five functional modes of operation. One 10-path transfer is also provided for each drive unit that is then used to route a detector into any one of up to 10 selectable paths. A common path is provided to permit cross calibration of the detectors.

The Control Room contains the necessary equipment for control, position indication, and flux recording for each detector.

A "flux-mapping" consists, briefly, of selecting flux thimbles in given fuel assemblies at various core quadrant locations. The detectors are driven to the top of the core and the detector is stopped automatically after reaching the preset setpoint. An x-y plot (position versus flux level) is initiated with the slow withdrawal of the detectors through the core from the top to a point below the bottom. In a similar manner, other core locations are selected and plotted. Each detector provides axial flux distribution data along the center of a fuel assembly.

Data from the measured assemblies in various radial positions of the core is used to infer power in the non-measured assemblies, thus producing a flux map for the entire core.

The number and location of these thimbles have been chosen to permit measurement of local to average peaking factors to an accuracy of better than ± 5 percent (95 percent confidence). Measured nuclear peaking factors will be increased proportionally to allow for the proper accuracy. If the measured power peaking is larger than acceptable, reduced power capability will be indicated.

7.7.1.10 Deleted by Amendment No. 40.

7.7.1.11 Safety-related Instrumentation Freeze Protection

Freeze Protection for safety-related instrumentation at SHNPP consists of two systems: the Freeze Protection System and the Temperature Maintenance System.

7.7.1.11.1 Freeze Protection System

The Freeze Protection System is a non-Class 1E system. It is designed to protect preselected piping systems exposed to ambient temperatures between 40F and -2F. System controls incorporate ambient sensing controlled freeze protection panels with two thermostats connected in parallel. The thermostats are preset to turn on at 40F and off at 45F. A line sensing temperature device is added to those circuits where the piping or equipment design temperatures can be exceeded due to the heater cable characteristics. The device will interrupt the current at preset values (under the design temperatures for lines or equipment). Additionally, the freeze protection panels include the following alarms:

a) Under-Temperature Alarm (35F Ambient Sensing Thermostat)

b) Under Current Circuit Alarm

c) Under Voltage Alarm

d) Ground Fault Alarm

At the Waste Processing Control Room, a summary alarm indicates a freeze protection panel malfunction for any of the above condition.

As a substitute to heat tracing individual lines, unit space heaters are used for areas where the temperature can be controlled by a locally mounted ambient air sensing thermostat. The thermostats are preset to turn on at 51°F. A thermostat set at 40°F is provided to alarm if the surface temperature falls below 40°F.

7.7.1.11.2 Temperature maintenance system

The Temperature Maintenance System is a non-Class 1E system. It is designed to maintain temperatures within specified minimum and maximum limits. The following systems have temperature maintenance:

a) Caustic System

b) Waste Management System

c) Boron Recycle System

d) Hydrogen Analyzer System

e) Chemical and Volume Control System

f) Isokinetic Sampling System

System controls for temperature maintenance incorporate individually controlled circuits, each including a resistance temperature detector (RTD) and a thermocouple. The RTDs are used to control the current in the circuit at the panel. Current is interrupted when maximum temperature limits are reached. The thermocouples are used to monitor the surface temperatures of the equipment or lines being protected. Additionally, the temperature values are remotely recorded with a datalogger.

As a substitute to the individual heat trace circuit, ambient air unit heaters are used in areas where the temperature can be controlled by a locally mounted thermostat. This is used with systems with low boric acid concentration. For this application, two (2) ambient air unit heaters are used per controlled area. One controlled by a local thermostat and the other is controlled through a contactor circuit wired to a temperature maintenance panel and the corresponding RTD in order to maintain area temperature at, or above, 65°F.

7.7.1.11.3 System redundancy

Either partial or total redundance is provided for pre-selected systems. Redundancy for the Freeze Protection System is provided for a) systems which are critical to the safe operation of the plant, and b) systems which are essential for safe shutdown of the plant.

Redundancy in the Temperature Maintenance System is provided for the Waste Management System Boron Recycle System, Hydrogen Analyzer System, Chemical and Volume Control System, and the Isokinetic Sampling System. The redundancy is accomplished through local manual operation at the system panels or circuit power distribution boxes. Temperature maintenance of the hydrogen analyzer system is energized through the non-safety-related MCCs which are connected to the 480V ESF System (Section 8.3.1.1.2.3). This system is manually connected to Division A.

For areas controlled by ambient air unit heaters redundancy exist only for the alarm portion with manual capability to be connected to a primary/redundant heat tracing panel.

7.7.2 ANALYSIS

The plant control systems are designed to assure high reliability in any anticipated operational occurrences. Equipment used in these systems are designed and constructed with a high level of reliability.

Proper positioning of the control rods is monitored in the Control Room by bank arrangements of the individual position columns for each rod cluster control assembly (RCCA). A rod deviation alarm alerts the operator of a deviation of one RCCA from the other rods in that bank position. There are also insertion limit monitors with visual and audible annunciation. A rod

bottom alarm signal is provided to the Control Room for each RCCA. Four 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 RCCAs. Long-term regulation of core reactivity is accomplished by adjusting the concentration of boric acid in the reactor coolant. Short term reactivity control for power changes is accomplished by the plant control system which automatically moves RCCAs. This system uses input signals including neutron flux, coolant temperature, and turbine load.

The axial core power distribution is controlled by moving the control rods through changes in reactor coolant system boron concentration. Adding boron causes the rods to move out thereby reducing the amount of power in the bottom of the core, this allows power to redistribute toward the top of the core. Reducing the boron concentration causes the rods to move into the core, thereby reducing the power in the top of the core, the result redistributes power towards the bottom of the core.

The plant control systems will prevent an undesirable condition in the operation of the plant that, if reached, will be protected by reactor trip. The description and analysis of this protection is covered in Section 7.2. Worst case failure modes of the plant control systems are postulated in the analysis as initiating events of off-design operational transients and accidents covered in Chapter 15.0, such as the following:

a) Uncontrolled RCCA bank withdrawal from a subcritical or low power startup condition.

b) Uncontrolled RCCA bank withdrawal at power.

c) RCCA misalignment.

d) Loss of external electrical load and/or turbine trip.

e) Loss of non-emergency AC power to the station auxiliaries (station blackout).

f) Feedwater system malfunctions that result in a decrease in feedwater temperature.

g) Excessive increase in secondary steam flow.

h) Inadvertent opening of a steam generator relief or safety valve. These analyses show that a reactor trip setpoint is reached in time to protect the health and safety of the public under those postulated incidents and that the resulting coolant temperatures produce a DNBR 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 amplifiers contained in the protection channel. As such, a failure in the control circuitry does not adversely affect the protection channel. Test results have shown that a short circuit or the application (credible fault voltage from within the cabinets) of 118 volt

AC or 140 volt DC on the isolated output portion of the circuit (nonprotection side of the circuit) will not affect the input (protection) side of the circuit.

Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels are capable of providing the protective action even when degraded by a second random failure. This meets the applicable requirements of Section 4.7 of IEEE Standard 279-1971. All single power source, sensor, or impulse line failures result in plant conditions that are bounded by the analysis in Chapter 15 to include control systems failures resulting from high energy line break (HELB).

The pressurizer pressure channels needed to derive the control signals are electrically isolated from control.

The design criteria on the isolation devices in the Balance of Plant (BOP) Systems is based on actual mounting and wiring of the isolation relays within the Isolation Cabinets. The devices which are part of redundant safety channels and their respective BOP interfaces are located in individual freestanding isolation cabinets. The Isolation Cabinets are constructed to provide electrical isolation and physical independence between different train Class 1E circuits and between Class 1E and non-Class 1E Systems. Any circuit or component failure on one side of the isolation barrier will not produce a failure or malfunction on the other side.

The analysis of BOP control circuits shows that no credible faults will induce voltage transients exceeding the normal operating conditions of the isolation devices. The circuits are protected against contact arcing and contact welding as well as against coil failure so that the failure of the non-safety part of the isolation device would not result in degradation of Class 1E circuits. The power supplies were analyzed not to create overcurrent. Thus, the separation between safety groups and between safety and non-safety systems is achieved.

Electrical isolation is maintained by electro-mechanical plug-in type relays whose special construction provides an electrical isolation of 4000 V RMS between the input and output. Physical independence into Class 1E and non-class 1E sections is provided by means of a metal barrier. The relay sockets are installed on the isolation barrier which divides the isolation panels. DC relays are fed from the 125 VDC Class 1E buses (SA & SB) supplied from the station batteries. AC relays are fed from the 120 VAC uninterruptible power supply service buses. Separate feeders are provided for each isolation cabinet. Power fault annunciation for each cabinet indicates a loss of any one of the power supplies. The isolation cabinets are located in the RAB within controlled environmental conditions (Control Room Envelope). Normal conditions in this area will be maintained before, during, and following an accident. The application of the isolation devices is further discussed in Section 8.3.1.2.30.

7.7.2.2 Response Considerations of Reactivity

Reactor shutdown with control rods is completely independent of the control functions since the trip breakers interrupt power to the rod drive mechanisms regardless of existing control signals. The design is such that the system can withstand accidental withdrawal of control groups or unplanned dilution of soluble boron without exceeding acceptable fuel design limits. The design meets the requirements of the 1971 General Design Criteria 25.

No single electrical or mechanical failure in the Rod Control System could cause the accidental withdrawal of a single RCCA from the partially inserted bank at full power operation. The operator could deliberately withdraw a single RCCA in the control bank; this feature is necessary in order to retrieve a rod, should one be accidentally dropped. In the extremely unlikely event of simultaneous electrical failures which could result in single RCCA 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 RCCA by operator action, whether deliberate or by a combination of errors, would result in activation of the same alarm and the same visual indications.

Each bank of control and shutdown rods in the system is divided into two groups (group 1 and group 2) of up to four or five 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 7.7.2-1, which also shows that one group is always within one step (5/8 in.) 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 RCCA attached to the mechanism. Since the four stationary gripper, moveable gripper, and lift coils associated with the RCCA of a rod group are driven in parallel, any single failure which could cause rod withdrawal would affect a minimum of one group of RCCA. Mechanical failures are in the direction of insertion, or immobility.

Figure 7.7.2-2 illustrates the design features that assure that no single electrical failure could cause the accidental withdrawal of a single RCCA from the partially inserted bank at full power operation.

Figure 7.7.2-2 shows the typical parallel connections on the lift, movable and stationary coils. Failure of the stationary or movable circuits will result in dropping or preventing rod (or rods) motion, therefore the discussion of single failure will be addressed to the lift coil circuits: 1) due to the method of wiring the pulse transformers which fire the lift coil multiplex thyristors, three of the four thyristors in a rod group could remain turned off when required to fire, if for example the gate signal lead failed open at point X_1. Upon "up" demand, one rod in group 1 and four rods in group 2 would withdraw. A section 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; and 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 16 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 MIL-HBD-217A. These wire failures would have to be accompanied by failure, or disregard, of the indications mentioned above. The probability of this occurrence is, therefore, too low to have any significance.

In order for the operator to erroneously withdraw a single rod cluster control assembly, the operator would have to improperly set the bank selector switch, the lift coil disconnect switches, and the in-hold-out switch. In addition, the three indications would have to be disregarded or ineffective. Such series of errors would require a complete lack of understanding and

administrative control. A probability number cannot be assigned to a series of errors such as these.

The Rod Position Indication System provides direct visual displays of each control rod assembly position. The plant computer alarms for deviation of rods from their banks. In addition, a rod insertion limit monitor provides an audible and visual alarm to warn the operator of an approach to an abnormal condition due to dilution. The low-low insertion limit alarm alerts the operator to follow emergency 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 main control board. The main control board position readouts, one for each rod, give the plant operator the actual position of the rod in steps. The indications are grouped by banks (e.g., Control Bank A, Control Bank B, etc.) to indicate to the operator the deviation of one rod with respect to other rods in a bank. This serves as a means to identify rod deviation.

The plant computer monitors the actual position of all rods. Should a control rod be misaligned from the other rods in that bank by more than 12 steps 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 deviation occur, the comparator output will operate a bistable unit to actuate a main control board annunciator. This alarm will alert the operator to a power imbalance caused by a misaligned rod. By use of individual rod position readouts, the operator can determine the deviating control rod and take corrective action. The design of the plant control system meets the requirements of General Design Criteria 23.

Upper and lower flux deviation and auto defeat annunciators ALB-13/5-3 and ALB-13/5-4 are screened through a time delay circuit in annunciator Cabinet No. 2 to prevent spurious nuisance alarms. The flux deviation alarm limit is reached for very short time periods due to nuclear instrumentation system process noise. Such flux deviations do not represent a sustained condition requiring operator action. If a sustained flux deviation condition exists the annunciator will actuate. The time delay setting is no longer than 1.5 minutes.

Refer to Section 4.3 for additional information on response considerations due to reactivity.

7.7.2.3 Step Load Changes Without Steam Dump

The plant control system restores equilibrium conditions, without a trip, following a plus or minus 10 percent step change in load demand, over the 15 to 100 percent power range for automatic control. Steam dump is blocked for load decrease less than or equal to 10 percent. A load demand greater than full power is prohibited by the turbine control load limit devices.

The plant control system minimizes the reactor coolant average temperature deviation during the transient within a given value and restores average temperature to the programmed setpoint. Excessive pressurizer pressure variations are prevented by using spray and heaters and power relief valves in the pressurizer.

The control system limits nuclear power overshoot to acceptable values following a 10 percent increase in load to 100 percent.

7.7.2.4 Loading and Unloading

Ramp loading and unloading of 5 percent per minute can be accepted over the 15 to 100 percent power range under automatic control without tripping the plant. The function of the control system is to maintain the coolant average temperature as a function of turbine-generator load.

The coolant average temperature increases during loading and causes a continuous insurge to the pressurizer as a result of coolant expansion. The sprays limit the resulting pressure increase. Conversely, as the coolant average temperature is decreasing during unloading, there is a continuous outsurge from the pressurizer resulting from coolant contraction. The pressurizer heaters limit the resulting system pressure decrease. The pressurizer water level is programmed such that the water level is above the setpoint for heater cut out during the loading and unloading transients. The primary concern during loading is to limit the overshoot in nuclear power and to provide sufficient margin in the Overtemperature ΔT setpoint.

The automatic load controls are designed to adjust the unit generation to match load requirements within the limits of the unit capability and licensed rating.

During rapid loading transients, a drop in reactor coolant temperature is sometimes used to increase core power. This mode of operation is applied when the control rods are not inserted deep enough into the core to supply all the reactivity requirements of the rapid load increase (the boron control system is relatively ineffective for rapid power changes). The reduction in temperature is initiated by continued turbine loading past the point where the control rods are completely withdrawn from the core. The temperature drop is recovered and nominal conditions restored by a boron dilution operation.

Excessive drops in coolant temperature are prevented by interlock C-16. This interlock circuit monitors the median coolant temperature indications and the programmed reference temperature which is a function of turbine First Stage pressure and causes a turbine loading stop when the decreased temperature reaches the setpoints.

The core axial power distribution is controlled during the reduced temperature return to power by placing the control rods in the manual mode when the $\Delta\Phi$ operating limits are approached. Placing the rods in manual will stop further changes in $\Delta\Phi$ and it will also initiate the required

drop in coolant temperature. Normally power distribution control is not required during a rapid power increase and the rods will proceed, under the automatic rod control system, to the top of the core. The bite position, as discussed in Chapter 4, is re-established at the end of the transient by decreasing the coolant boron concentration.

7.7.2.5 Load Rejection Furnished by Steam Dump System

When a load rejection occurs, if the difference between the required temperature setpoint of the RCS 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 flow reduces proportionally as the control rods act to reduce the average coolant temperature. The artificial load is, therefore, removed as the coolant average temperature is restored to its programmed equilibrium value.

The dump valves are modulated by the reactor coolant average temperature signal. The required number of steam dump valves can be tripped quickly to stroke full open or modulate, depending upon the magnitude of the temperature error signal resulting from loss of load.

7.7.2.6 Turbine-Generator Trip With Reactor Trip

Whenever the turbine-generator unit trips at an operating power level above 10 percent 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 steam generator safety valve setpoint. The thermal capacity of the RCS is greater than that of the secondary system, and because the full load average temperature is greater than the no-load temperature, a heat sink is required to remove heat stored in the reactor coolant to prevent actuation of steam generator safety valves for a trip from full power. This heat sink is provided by the combination of controlled release of steam to the condenser and by makeup of feedwater to the steam generators.

The Steam Dump System is controlled from the reactor coolant average temperature signal whose setpoint values are programmed as a function of turbine load. Actuation of the steam dump is rapid to prevent actuation of the steam generator safety valves. With the 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.

The feedwater flow is cut off following a reactor trip 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 heaters. However, if the heaters become uncovered following the trip, the CVCS 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 reactivity shutdown margin.

REFERENCES: SECTION 7.7:

7.7.1-1 Letter from G. Percival (Westinghouse) to S. Zimmerman (CP&L), "Instrumentation Uncertainty Safety Evaluation," CQL-88-639, dated 11-17-88.

7.7.1-2 "Westinghouse Improved Thermal Design Procedure Instrument Uncertainty Methodology for Carolina Power & Light Harris Nuclear Plant (for Uprate to 2912.4 MWT-NSSS Power and Replacement Steam Generator)", WCAP-12340, Rev. 1 (Proprietary) and WCAP-12341, Rev. 1 (Non-Proprietary).

7.7.1-3 "Westinghouse Pressurizer Water Level Control System Uncertainty Methodology for Harris Nuclear Plant (Uprate to 2912.4 MWT-NSSS Power)", WCAP-15239, Rev. 0 (Proprietary) and WCAP-15240, Rev. 0 (Non-Proprietary).

TABLE	TITLE
7.1.0-1	LISTING OF APPLICABLE CRITERIA FOR INSTRUMENTATION AND CONTROL SYSTEM
7.1.1-1	PLANT COMPARISON FOR NSSS DESIGN
7.1.1-2	PLANT COMPARISON FOR BALANCE OF PLANT DESIGN
7.2.1-1	LIST OF REACTOR TRIPS
7.2.1-2	PROTECTION SYSTEM INTERLOCKS
7.2.1-3	REACTOR TRIP SYSTEM INSTRUMENTATION
7.2.2-1	DELETED BY AMENDMENT NO. 48
7.3.1-1	SYSTEM RESPONSIBILITIES
7.3.1-2	INSTRUMENTATION OPERATING CONDITION FOR ENGINEERED SAFETY FEATURES
7.3.1-3	INSTRUMENT OPERATING CONDITIONS FOR ISOLATION FUNCTIONS
7.3.1-4	INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM
7.3.1-5	ESF ACTUATION SYSTEMS - SAFETY INJECTION SIGNAL(S)
7.3.1-6	ESF ACTUATION SYSTEMS - CONTAINMENT SPRAY ACTUATION SIGNAL (CSAS)
7.3.1-7	ESF ACTUATION SYSTEMS - CONTAINMENT ISOLATION PHASE - A (T)
7.3.1-8	ESF ACTUATION SYSTEMS - CONTAINMENT ISOLATION PHASE - B (P)
7.3.1-9	ESF ACTUATION SYSTEMS CONTAINMENT VENTILATION ISOLATION SIGNAL (CVIS)
7.3.1-10	ESF ACTUATION SYSTEMS - MAIN STEAM ISOLATION SIGNAL (MSIS)
7.3.1-11	ESF ACTUATION SYSTEMS - FEEDWATER ISOLATION SIGNAL (MFI)
7.3.1-12	ESF AND SUPPORTING SYSTEM ACTUATION INSTRUMENTATION
7.3.2-1	ENGINEERED SAFETY FEATURES - STATUS INDICATOR LIGHTS
7.4.1-1	MONITORING INSTRUMENTS FOR SAFE SHUTDOWN
7.4.1-2	INSTRUMENTATION AND CONTROL AUXILIARY CONTROL PANEL (ACP)
7.5.1-1	CONTROL ROOM INDICATORS AND/OR RECORDS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS-CONTAINMENT SPRAY AND CONTAINMENT COOLING SYSTEM
7.5.1-2	CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS-AUXILIARY FEEDWATER SYSTEM
7.5.1-3	CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION

TABLE	TITLE
	II, III AND IV EVENTS-EMERGENCY POWER SYSTEM
7.5.1-4	CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS-SERVICE WATER SYSTEM
7.5.1-5	CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS-CONTROL ROOM EMERGENCY FILTRATION SYSTEM
7.5.1-6	CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS-REACTOR AUXILIARY BUILDING EMERGENCY EXHAUST SYSTEM
7.5.1-7	CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS-FUEL HANDLING BUILDING EMERGENCY EXHAUST SYSTEM
7.5.1-8	CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS-FUEL HANDLING SPENT FUEL PUMP ROOM VENTILATION SYSTEM
7.5.1-9	CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS-REACTOR COOLANT SYSTEM
7.5.1-10	CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS-CONTAINMENT SYSTEM
7.5.1-11	CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS - MAIN STEAM SUPPLY SYSTEM
7.5.1-12	CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS-REFUELING WATER STORAGE TANK
7.5.1-13	CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS-COMPONENT COOLING WATER SYSTEM
7.5.1-14	CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION-NUCLEAR INSTRUMENTATION
7.5.1-15	REACTOR CONTROL SYSTEM
7.5.1-16	ANNUNCIATOR LIGHT BOXES
7.7.1-1	PLANT CONTROL SYSTEM INTERLOCKS
7.7.1-2	DELETED BY AMENDMENT NO. 40

TABLE 7.1.0-1 LISTING OF APPLICABLE CRITERIA FOR INSTRUMENTATION AND CONTROL SYSTEM

CRITERIA	TITLE	CONFORMANCE DISCUSSED IN SECTION
1. 10 CFR Part 50		
a. 10 CFR 50.34	Contents of Application: Technical Information	
b. 10 CFR 50.36	Technical Specifications	16.1, 16.2
c. 10 CFR 50.55a	Codes and Standards	3.1, 3.9, 3.10, 3.11
2. General Design Criteria (GDC),Appendix A to 10 CFR Part 50.		See Section 3.1 for discussion of each Design Criteria
GDC 1	Quality Standards and Records	3.1, 7.2.2, 7.4.2
GDC 2	Design Bases for Protection Against Natural Phenomena	3.1, 3.10, 3.11, 7.2.2, 7.2.1
GDC 3	Fire Protection	3.1, 9.5.1, 7.4.2
GDC 4	Environmental and Missile Design Bases	3.1, 3.11, 7.2.2, 7.4.2
GDC 10	Reactor Design	3.1.4, 7.2.2, 7.4.2
GDC 13	Instrumentation and Control	7.2.1, 7.3.1, 7.3.2, 7.4.2
GDC 15	Reactor Coolant System Design	3.1, 7.2.2
GDC 17	Electric Power Systems	3.1, 8.3, 7.3.2
GDC 19	Control Room	3.1, 6.4, 9.4, 7.4.1, 7.4.2, 7.3.1, 12.3.4
GDC 20	Protection System Functions	3.1, 1.1.2, 7.2.2, 7.3.2, 7.3.1, 7.4.2
GDC 21	Protection Systems Reliability and Testability	3.1, 7.1.2, 7.2.2, 7.3.2, 7.3.1, 7.4.2, 7.6.2
GDC 22	Protection System Independence	3.1, 7.1.2, 7.2.2, 7.3.2, 7.3.1, 7.4.1, 7.4.2
GDC 23	Protection System Failure Modes	3.1, 7.2.2, 7.3.2,7.3.1, 7.4.2, 7.6.2
GDC 24	Separation of Protection and Control Systems	3.1, 7.2.2, 7.3.2, 7.3.1, 7.4.2, 7.6.2
GDC 25	Protection System Requirements for Reactivity Control Malfunctions	3.1, 7.3.2, 7.7.2
GDC 26	Reactivity Control System Redundancy and Capability	3.1, 7.7.2, 7.4.2, 4.6, 9.3.4
GDC 27	Combined Reactivity Control Systems Capability	3.1, 2.3.1, 7.3.1, 7.3.2, 7.4.2
GDC 28	Reactivity Limits	3.1, 7.3.1, 7.3.2
GDC 29	Protection Against Anticipated Operational Occurrences	3.1, 7.2.2
GDC 30	Quality of Reactor Coolant Pressure Boundary	3.1, 7.7
GDC 33	Reactor Coolant Makeup	3.1, 7.4.2
GDC 34	Residual Heat Removal	3.1, 7.4.2
GDC 35	Emergency Core Cooling	3.1, 7.3.2
GDC 37	Testing of Emergency Core Cooling System	3.1, 7.3.2

TABLE 7.1.0-1 LISTING OF APPLICABLE CRITERIA FOR INSTRUMENTATION AND CONTROL SYSTEM

CRITERIA	TITLE	CONFORMANCE DISCUSSED IN SECTION
GDC 38	Containment Heat Removal	3.1, 7.3.1, 7.3.2
GDC 40	Testing of Containment Heat Removal System	3.1, 7.3.2, 7.6.2
GDC 41	Containment Atmosphere Cleanup	3.1, 7.3.2
GDC 43	Testing of Containment Atmosphere	3.1, 7.3.2
GDC 44	Cooling Water	3.1, 7.3.2
GDC 46	Testing of Cooling Water System	3.1, 7.3.2
GDC 55	Reactor Coolant Pressure Boundary Penetrating Containment	3.1, 6.2.4
GDC 56	Primary Containment Isolation	3.1, 6.2.4, 7.3.1, 7.3.2
GDC 57	Closed Systems Isolation Valves	3.1, 6.2.4, 7.3.1, 7.3.2
GDC 60	Control of Releases of Radioactive Materials to the Environment	3.1, 9
GDC 63	Monitoring Fuel and Waste Storage	3.1, 7.6
GDC 64	Monitoring Radioactivity Releases	3.1, 12.3
3. Institute of Electrical and Electronics Engineers (IEEE) Standards		
IEEE Std. 279 (ANSI N42.7)	Criteria for Protection Systems for Nuclear Power Generating Stations	7.1, 7.2, 7.3, 7.6, 7.4, 7.5, 7.7
IEEE Std 308	Criteria for Class IE Electric Systems for Nuclear Power Generating Stations	7.3.2, 7.6, 8.3.1.2, 7.4.2, 7.6.2, 8.3.1
IEEE Std 317	Electric Penetration Assemblies in Containment Structures for Nuclear Power Generating Stations	3.8, 7.1.2, 8.3.1.2
IEEE Std 323	Qualifying Class IE Equipment for Nuclear Power Generating Stations	1.8 (RG 1.89) 3.11, 8.3.1.2 7.3.2, 7.4.1, 7.4.2, 7.6.2
IEEE Std 336 (ANSI N45.2.4)	Installation, Inspection and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations	7.1.2, 8.3.1.2, 7.4.2
IEEE Std 338	Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems	1.8, 7.1.2.18, 7.2.2.2, 7.2.3 7.3.2.2.10, 7.6.2.2.j), 7.6.2 8.3.1.2.27
IEEE Std 344 (ANSI N41.7)	Guide for Seismic Qualification of Class I Electrical Equipment for Nuclear Power Generating Stations	3.10, 7.1.2.7, 8.3.1.2, 7.3.2, 7.4.1, 7.4.2, 7.6.2
IEEE Std 352	General Principles for Reliability Analysis of Nuclear Power Generating Stations Protection Systems	7.3.2
IEEE Std 379 (ANSI N41.2)	Guide for the Application of the Single Failure Criterion to Nuclear Power Generating Station Protection Systems	7.1.2.7, 8.3.1.2, 7.3.2, 7.6.2
IEEE Std 383 (ANSI N41.10)	IEEE Standard for Type Test of Class 1E Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations	8.1.4, 9.5.1, 8.3.1
IEEE Std 384 (ANSI N41.14)	Criteria for Separation of Class IE Equipment and Circuits	1.8, 7.1.2, 8.3.1.2
IEEE Std 494	Method for Identification of Documents Related to Class 1E Equipment and Systems for Nuclear Power Generating Stations	7.3.2, 7.6.2

TABLE 7.1.0-1 LISTING OF APPLICABLE CRITERIA FOR INSTRUMENTATION AND CONTROL SYSTEM

CRITERIA	TITLE	CONFORMANCE DISCUSSED IN SECTION
IEEE Std 387	Criteria for Diesel-Generator Units applied as Standby Power Supplies for Nuclear Power Generating Stations	8.3.1
IEEE Std 420	Trial-Use for Class 1E Control Switchboards for Nuclear Power Generating Stations	8.1.4
4. Regulatory Guides (RG)		See Section 1.8 for discussion of each Regulatory Guide 1.75
RG 1.6	Independence Between Redundant Standby (Onsite) Power Sources and Between Their Distribution Systems	1.8, 7.6
RG 1.7	Control of Combustible Gas Concentrations in Containment	7.3.1
RG 1.11	Instrument Lines Penetrating Primary Reactor Containment	1.8, 6.2.4, 7.3.1 Note: Only lines covered are containment pressure sensing system. No automatic or remote isolation valves.
RG 1.89	Qualification of Class 1E Equipment for Nuclear Power Plants	See Section 3.11, 7.1.2, 7.4.2
RG 1.22	Periodic Testing of Protection System Actuation Functions	1.8, 7.1.2, 7.2.2, 7.3.2
RG 1.29	Seismic Design Classification	1.8, 3.10, 7.2.1, 7.3.2, 7.4.2 7.6.2
RG 1.30	Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment	1.8, 17.1, 7.3.2, 7.4.2
RG 1.32	Use of IEEE Std 308 "Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations	1.8, 8.3.1.2, 7.3.2, 7.4.2
RG 1.40	Qualification Tests of Continuous - Duty Motors Installed Inside the Containment of Water-Cooled Nuclear Power Plants	3.1, 8.3.1.2, 14.2
RG 1.47	Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems	Use in conjunction with Position 1.8, RG 1.17, 7.3.2, 7.1.2, 7.4.1, 7.4.2, 7.5.1, 7.5.2, 7.6.2
RG 1.53	Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems	1.8, 7.1.2, 7.4.2, 7.6.2
RG 1.62	Manual Initiation of Protection Actions	1.8, 7.3.2, 7.2.1, 7.3.2, 7.4.2, 7.6.2
RG 1.63	Electric Penetration Assemblies in Containment Structures for Water-Cooled Nuclear Power Plant	1.8, 8.3.1, 7.1.2, 7.4.2
RG 1.68	Preoperational and Initial Startup Test Program for Water-Cooled Power Reactors	1.8, 14.0, 7.1.2
RG 1.70	Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants Rev. 2	1.8, 7.4.2
RG 1.73	Qualification Tests of Electric Valve Operators Installed Inside the Containment of Nuclear Power Plants	1.8
RG 1.75	Physical Independence of Electrical Systems	1.8, 7.2.1, 7.3.1.4, 8.3.1.2, 7.1.2
RG 1.78	Assumptions for Evaluating the Habitability of Nuclear Power Plant Control Room During a Postulated Hazardous Chemical Release	1.8, 7.3.1, 9.4.1
RG 1.12	Instrumentation for Earthquakes	1.8, 3.7.4
RG 1.45	Reactor Coolant Pressure Boundary Leakage Detection Systems	1.8

TABLE 7.1.0-1 LISTING OF APPLICABLE CRITERIA FOR INSTRUMENTATION AND CONTROL SYSTEM

CRITERIA	TITLE	CONFORMANCE DISCUSSED IN SECTION
RG 1.67	Installation of Overpressure Protection Devices	1.8
RG 1.80	Preoperational Testing of Instrument Air	1.8, 7.1.2
RG 1.97	Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident	1.8, 7.5.1.8
RG 1.100	Seismic Qualification of Electrical Equipment for Nuclear Power Plants	1.8, 3.10, 8.3.1.2, 7.1.2, 7.3.2
RG 1.105	Instrument Spans and Setpoints	1.8, 7.3.1, 7.3.2, 7.1.2, 7.3.2, 7.6.2
RG 1.106	Thermal Overload Protection for Electric Motors on Motor-Operated Valves	1.8, 8.3.1.2, 7.1.2.1.5, 7.3.2
RG 1.108	Periodic Testing of Diesel Generator Units used as Onsite Electric Power Systems for Nuclear Power Plants	1.8, 8.3.1, 14.2
RG 1.118	Periodic Testing of Electrical Power and Protection Systems	1.8, 7.1.2.17, 7.3.2.2.10, 7.6.2.2.j), 8.3.1.2.20, 13.5.1.3.e), 7.6.2
RG 1.120	Fire Protection Guidelines for Nuclear Power Plants	1.8, 9.5.1
RG 1.21	Measuring, Evaluating and Reporting Radioactivity in Solid Wastes and Releases of Radioactive Materials in Liquid and Gaseous Effluents from Light Water-Cooled NPP (Rev. 1)	1.8, 11.5.1
RG 1.38	Quality Assurance Requirements for Packaging, Shipping, Receiving, Storage and Handling of Items for Water Cooled Nuclear Power Plants (Rev. 2)	1.8, 9.12, 17.3
RG 1.41	Preoperational Testing of Redundant On-Site Electric Power Systems to Verify Proper Group Assignments	7.3.2, 14.2.7
RG 1.60	Design Response Spectra for Seismic Design of Nuclear Power Plants	1.8, 3.7.1
RG 1.92	Combining Modal Responses and Spatial Components in Seismic Response Analysis (Rev. 1)	1.8, 3.7.2.1, 3.7.3.7, 3.9A
RG 1.137	Fuel Oil System for Standby Diesel Generator	1.8, 9.5.4.1
RG 1.139	Guidance for Residual Heat Removal (Rev. 0)	1.8, 5.4, 7.3, 7.4, 7.6, 10.4, 14.2
RG 1.141	Containment Isolation Provisions for Fluid Systems (Rev. 0)	1.8, 6.2, 7.3
RG 1.123	Quality Assurance Requirements for Control or Procurement of Items and Services for Nuclear Power Plants (Rev. 1)	1.8, 17.3
RG 1.68.3	Preoperational Testing of Instrument and Air Control Systems	7.1.2.12
5. Branch Technical Positions (BTP) 1CSB		
BTP ICSB 1	Backfitting of the Protection and Emergency Power Systems of Nuclear Reactors	7.6.2, 7.3.2
BTP ICSB 9	Definition and Use of "Channel-Calibration" Technical Specifications	16, 7.3.2, 7.6.2
BTP ICSB 10	Electrical and Mechanical Equipment Seismic Qualification Program	3.10, 7.3.2, 7.6.2
BTP ICSB 13	Design Criteria for Auxiliary Feedwater Systems	7.3.2

TABLE 7.1.0-1 LISTING OF APPLICABLE CRITERIA FOR INSTRUMENTATION AND CONTROL SYSTEM

CRITERIA	TITLE	CONFORMANCE DISCUSSED IN SECTION
BTP ICSB 14	Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors	15.2, 15.3
BTP ICSB 18 (PSB)	Application of the Single Failure Criterion to Manually Controlled Electrically Operated Valves	7.3.2, 16, 7.6.2
BTP ICSB 20	Design of Instrumentation and Controls Provided to Accomplish Change over from Injection to Recirculation Mode	6.3.2, 7.3.2
BTP ICSB 21	Guidance for Application of Reg. Guide 1.47	7.1.2, 7.3.2, 7.5.1, 7.6.2
BTP ICSB 22	Guidance for Application of Reg. Guide 1.22	7.1.2, 7.2.2, 7.3.2, 7.6.2
BTP ICSB 23	Qualification of Safety-Related Display Instrumentation for Post-Accident Condition Monitoring and Safe Shutdown	7.3.2
BTP ICSB 24	Testing of Reactor Trip System and Engineered Safety Feature Actuation System Sensor Response Times	7.2.2, 7.3.2
BTP ICSB 25	Guidance for the Interpretation of General Design Criterion 37 for Testing the Operability of the Emergency Core Cooling System as a Whole	3.1, 6.3.4
BTP ICSB 27	Design Criteria for Thermal Overload Protection for Motors of Motor-Operated Valves	8.3.1.2

TABLE 7.1.1-1 PLANT COMPARISON FOR NSSS DESIGN

	REACTOR TRIP SYSTEM	FUNCTIONAL DIFFERENCES BETWEEN SHNPP AND SOUTH TEXAS PROJECT
1.	Turbine trip on Reactor Protection System Actuation	SHNPP turbine is tripped on Safety Injection. SI is actuated among other signals by low steamline pressure signal. South Texas Project (STP) turbine is tripped on either Safety Injection or excessive cooldown protection. The SHNPP steamline protection system and the South Texas Project (STP) excessive cooldown protection both accomplish the same function although the initiating signals may have different derivations. In any case, Chapter 15 analyses do not take credit for turbine trip on safety injection or excessive cooldown.
2.	Reactor trip on Turbine stop valve closure	SHNPP requires closure of all four valves for reactor trip, while South Texas Project requires closure of two out of four stop valves for reactor trip. This trip is an anticipatory trip not taken credit for in the Chapter 15 analysis.
3.	Pressurizer high level water detection	SHNPP uses three channels, South Texas Project uses four channels. However, the Chapter 15 analyses do not take credit for this function.
4.	Pressurizer pressure detection (high and low)	SHNPP uses three channels, South Texas Project uses four channels. SHNPP's three channels are used for protection. There are two completely separate channels for control purposes. Therefore, a postulated single failure of one of the protection channels would not prevent actuation of this function.
5.	Interlock P-15 [Neutron flux power range below setpoint] or P4 (Reactor tripped)	South Texas Project uses interlocks as permissive condition to allow feedwater and turbine generator trip, S.I., and Steam Line Isolation as part of the excessive cooldown protection. SHNPP does not need this interlock. The SHNPP steamline break protection system performs the same safety function as the STP excessive cooldown protection, but does not utilize the P-15 interlock. Permissive P-4 is used at SHNPP for SI Block Logic, Turbine Trip and closes the main feedwater regulating valves on low T_{avg}.
6.	Low Feedwater Flow	SHNPP has a low feedwater reactor trip; South Texas Project does not. Although the low feedwater flow reactor trip would serve to trip the reactor for a loss of feedwater event, it is not taken credit for in the Chapter 15 analysis. Therefore, Chapter 15 shows that the low-low steam generator level reactor trip is adequate protection for loss of feedwater transients.
	ENGINEERED SAFETY FEATURES ACTUATION SYSTEM	
1.	Emergency Core Cooling System	South Texas Project safety injection initiation occurs on Low-low compensated cold while SHNPP does not use this initiating signal. Safety injection actuation from this signal (low-low compensated T_{cold}) would occur during the main steamline rupture analysis presented in Chapter 15. During the main steamline rupture a low steamline pressure signal is reached within the first few seconds of the transient. Using this signal to actuate SI provides adequate protection in the event of a postulated steamline rupture.

TABLE 7.1.1-1 PLANT COMPARISON FOR NSSS DESIGN

REACTOR TRIP SYSTEM	FUNCTIONAL DIFFERENCES BETWEEN SHNPP AND SOUTH TEXAS PROJECT
2. Feedwater Isolation Initiation	South Texas Project feedwater isolation occurs on: a .Low compensated T cold interlocked with P15 b .High feedwater flow interlocked with P15 These conditions are not applicable to SHNPP, and no credit is taken for it in the Chapter 15 analyses. Feedwater Isolation is initiated by SI signal and/or P-14 Steam Generator Hi-Hi Level.
3. Main Steam Line Isolation Initiation	Main steamline isolation initiation on SHNPP occurs upon high steam pressure rate below P-11 and Low Steamline Pressure above P-11 while on South Texas Project it occurs on any function that initiates Safety Injection. Steamline isolation, as in safety injection actuation can be actuated from any of several signals for SHNPP. These signals can be derived from: a .Low steam pressure. b .Hi-Hi containment pressure. c. High steam pressure rate. d. Manual actuation. In accidents where mitigation depends on steamline isolation, the STP steamline isolation would have one advantage over SHNPP pertaining to the containment analysis following a secondary side split break. Since steamline isolation would occur on Hi containment pressure for STP (instead of Hi-Hi containment pressure for SHNPP), blowdown from all steam generators would be terminated sooner, therefore decreasing the mass/energy released into Containment. However, the SHNPP containment analysis showed that its protection systems are adequate to mitigate the consequences of a break inside Containment. Therefore, no safety problems exist due to the SHNPP steamline isolation logic.

TABLE 7.1.1-1 PLANT COMPARISON FOR NSSS DESIGN

REACTOR TRIP SYSTEM	FUNCTIONAL DIFFERENCES BETWEEN SHNPP AND SOUTH TEXAS PROJECT
4. Auxiliary Feedwater Pump Starting	SHNPP has two motor driven and one turbine driven AFW pumps. a .Motor driven pump starting occurs on SHNPP upon loss of offsite power and loss of both main feedwater pumps in addition to the start signals that are the same on South Texas Project (i.e. low-low level in any Steam Generator and Safety Injection Signal). South Texas Project pump initiation circuit includes a manual reset block control on low-low steam generator level while SHNPP does not use this type of control. It is not necessary to block the auxiliary pump start signal on SHNPP because the turbine driven pump on SHNPP is not started automatically on a low-low level in one steam generator. b. Turbine-driven pump starting occurs on SHNPP upon low-low level in two out of three steam generators or loss of offsite power. Although it would be true that actuation of the turbine driven pump on the same signal as the motor driven pump would provide more heat removal capability for heat up accidents (such as loss of feedwater and feedline rupture) it was demonstrated in Chapter 15 of the SHNPP FSAR that adequate heat removal capability was supplied by the SHNPP auxiliary feedwater pump actuation system. South Texas Project turbine-driven pump initiation occurs on the same signal as the motor-driven pumps: a .Safety injection signal b .low-low level in any steam generator.
Auxiliary Feedwater Isolation	SHNPP auxiliary feedwater line automatically isolates on steamline isolation and high steamline differential pressure, South Texas Project does not. For SHNPP, there are three auxiliary feedwater pumps which supply the steam generators through piping whose discharge is interconnected by headers. For STP, the supply is through auxiliary feedwater dedicated piping to each steam generator.
CONTROL SYSTEMS NOT REQUIRED FOR SAFETY	
1. Steam Generator Water Level Control System	Main Feedwater Pump speed is controlled on South Texas Project, whereas control on SHNPP is by position of feedwater F/W bypass valve as well as by F/W control valve. Both ways of controlling steam generator water level are acceptable. Chapter 15 analyses for SHNPP and STP show that for feedwater malfunction transients, all acceptance criteria are met.
2. Steam Dump Control System	The C8 control interlock, which blocks steam dump on 2/4 turbine stop valves closed on South Texas Project, will block steam dump on 4/4 turbine stop valves closed on SHNPP. In any case, no credit is taken in the Chapter 15 accident analysis.

TABLE 7.1.1-2

PLANT COMPARISON FOR BALANCE OF PLANT DESIGN

	DIFFERENCES BETWEEN SHNPP AND WATERFORD 3 (NON-NSSS)	ATTENDANT EFFECTS OF DIFFERENCES ON SAFETY-RELATED SYSTEMS
Systems required for Safe Shutdown	Functionally no difference	No response required
Safety-Related Display Instrumentation	Functionally no difference except for the Bypass and Inoperable Status Indication which is non-safety	The Bypass and Inoperative status indication on the Shearon Harris Nuclear Power Plant is designed in conformance with Regulatory Guide 1.47 requirements. The system provides indication during a bypass or inoperable related on SHNPP condition on any part of the safety related Engineered Safety Feature Systems. These indications are provided on a system level as described in FSAR Section 7.5.1.9. The actuating contacts for these lights, coming from the ESF systems are isolated. Proper isolation devices are provided between the bypass indicating light (Non-Safety) and all safety related contacts to assure that any adverse effect on the lights cannot propagate to the plant safety systems. Isolation devices are in accordance with Regulatory Guide 1.75. The bypass and inoperable status panels (two channels) on SHNPP serve primarily as augmented operator indication in addition to other safety related Class 1E indications associated with each equipment (i.e. motor indicating lights, valve position lights, etc).
Other Systems Required for Safety	a. Systems that are common have no functional differences. The following SHNPP systems are not addressed in Waterford 3: -Diesel Fuel Oil System (See Section 7.3) -Radiation Monitoring (See Section 7.6 and Chapter 11)	Diesel Fuel Oil System and Radiation Monitoring on Waterford 3, were basically similar in function to the systems provided on SHNPP. However, SHNPP FSAR describes the systems in more detail. There is no effect in any way associated with the safety-related systems.
	b. SHNPP does address the following systems as part of ESFAS containment ventilation isolation subsystem in Section 7.3 -Containment Purge Isolation -Containment Vacuum Relief	The Containment Purge Isolation as described in FSAR Section 9.4.7.2.2 and Containment Vacuum Relief as described in FSAR Section 7.3.1.5.12 are actuated by contacts completely independent from any other safety-related systems. The instrument and controls are physically and electrically separated into two channels. The redundancy and independence provided in each system give full assurance that no adverse effect can be propagated to any safety-related systems.

TABLE 7.2.1-1 LIST OF REACTOR TRIPS

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 setting; manual block and automatic reset of low setting by P-10
2. Intermediate range neutron flux (anticipatory)	1/2	Manual block permitted by P-10	Manual block and automatic reset
3. Source range neutron flux (anticipatory)	1/2	Manual block permitted by P-6, interlocked with P-10	Manual block and automatic reset. Automatic block above P-10 (High voltage removed from detector)
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	2/3	No interlocks	
7. Overpower ΔT	2/3	No interlocks	
8. Pressurizer low pressure	2/3	Interlocked with P-7	Blocked below P-7
9. Pressurizer high pressure	2/3	No interlocks	
10 .Pressurizer high water level	2/3	Interlocked with P-7	Blocked below P-7
11. Low reactor coolant flow	a .2/3 in 2/3 loops	Interlocked with P-7	
	b. 2/3 in any loop	Interlocked with 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 undervoltage	2/3 loops	Interlocked with P-7	Low voltage permitted below P-7

TABLE 7.2.1-1 LIST OF REACTOR TRIPS

Reactor Trip	Coincidence Logic	Interlocks	Comments
13. Reactor coolant pump underfrequency	2/3 loops	Interlocked with P-7	Underfrequency on 2 motors will trip all reactor coolant pump breakers and cause reactor trip; blocked below P-7
14 .Low feedwater flow	1/2 in any loop	No interlocks	1/2 steam/feedwater flow mismatch in coincidence with 1/2 low steam generator water level
15 .Low-low steam generator water level	2/3 in any loop	No interlocks	
16. Safety injection signal	Coincident with actuation of safety injection	No interlocks	(See Section 7.3 for engineered safety features actuation conditions)
17. Turbine Trip (anticipatory			
a. Trip fluid pressure	2/3	Interlocked with P-7	Blocked below P-7
b. Turbine throttle valve close	4/4	Interlocked with P-7	Blocked below P-7
18. Manual	1/2	No interlocks	
19. General Warning Alarm Trip	Coincident Occurrence in Both Trains of any of the Conditions Listed in Paragraph 7.2.1.1.2.9	None	None

TABLE 7.2.1-2

PROTECTION SYSTEM INTERLOCKS

Designation	Derivation	Function
I POWER ESCALATION PERMISSIVES		
P-6	Presence of P-6: 1/2 neutron flux (intermediate range) above setpoint	Allows manual block of source range reactor trip
	Absence of P-6: 2/2 neutron flux (intermediate range) below setpoint	Defeats the block of source range reactor trip
P-10	Presence of P-10: 2/4 neutron flux (power range) above setpoint	Allows manual block of power range (low setpoint) reactor trip
		Allows manual block of intermediate range reactor trip and intermediate range rod stops (C-1)
	Absence of P-10: 3/4 neutron flux (power range) below setpoint	Defeats the block of power range (low setpoint) reactor trip
		Defeats the block of intermediate range reactor trip and intermediate range rod stops (C-1)
		Input to P-7
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 first stage pressure below setpoint (from P-13)	Block reactor trip on: Low reactor coolant flow in more than one loop, undervoltage, turbine trip pressurizer low pressure, and pressurizer high level blocks RCP breaker trip on underfrequency
P-8	Absence of P-8: 3/4 neutron flux (power range) below setpoint	Blocks reactor trip on low reactor coolant flow in a single loop
P-13	2/2 turbine first stage pressure below setpoint	Input to P-7

TABLE 7.2.1-3

REACTOR TRIP SYSTEM INSTRUMENTATION

Reactor Trip Signal	Range	Trip Accuracy[1]
1 .Power range high neutron flux	1 to 120% full power	
2 .Intermediate range high neutron flux	8 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	+15% of full power	
5 .Power range high negative neutron flux rate	-15% of full power	
6 .Overtemperature ΔT	T_H 530 to 650°F	
	T_C 510 to 630°F	
	T_{AV} 530 to 630°F	
	P_{PRZR} 1700 to 2500 psig	
	F(Δφ)-50 to + 50%	
	T Setpoint 0 to 150% RTP	
7. Overpower ΔT	T_H 530 to 650°F	
	T_C 510 to 630°F	
	T_{AV} 530 to 630°F	
	ΔT Setpoint 0 to 150% RTP	
8. Pressurizer low pressure	1700 to 2500 psig	
9. Pressurizer high pressure	1700 to 2500 psig	
10. Pressurizer high water level	Entire distance between taps (0 to 100% span)	
11. Low reactor coolant flow	0 to 120% of rated flow	
12. Reactor coolant pump undervoltage	0 to 100% rated voltage	
13. Reactor coolant pump underfrequency	50 to 60 Hz	
14. Low feedwater flow[2]	0 to 120% Maximum	
15. Low-low steam generator water level	Total distance between narrow range steam generator level taps (0 to 100% span)	
16. Turbine trip from low hydraulic fluid pressure	200 to 3000 psig	

[1] See discussion in Section 7.2.1.2.6.b.
[2] 1/2 steam/feedwater flow mismatch in coincidence with 1/2 low steam generator water level.

TABLE 7.3.1-1

SYSTEM RESPONSIBILITIES

System	System Classification	Mechanical System Responsibilities	FSAR Section Discussing Mechanical System	ESFAS Logic (Figure No.)	DBA Required Action(1)
Emergency Core Cooling	ESF	Westinghouse	6.3	-	1,2,3,4
Containment Isolation	ESF	Ebasco	6.2.4	7.3.1-5 7.3.1-6	1,2,3,4
Main Steam Isolation	ESF	Westinghouse	10.3	7.3.1-7	2,3,4
Main Feedwater Isolation	ESF	Ebasco	10.4	7.3.1-8	2,3,4
Containment Spray	ESF	Ebasco	6.5.2	7.3.1-3	1,3,4
Containment Cooling	ESF	Ebasco	6.2.2	7.3.1-4	1,2,3,4
Auxiliary Feedwater	ESF	Ebasco	10.4.9	7.3.1-9 7.3.1-10	6
Combustible Gas Control	non-safety-related	Westinghouse/Ebasco	6.2.5	-	7
Emergency Power Supply	ESF Support	Ebasco	8.3.1	8.3.1-1	6
Emergency Service Water System	ESF Support	Ebasco	9.2.1	7.3.1-15	6
Component Cooling Water	ESF Support	Ebasco/Westinghouse	9.2.2	-	6
120V Uninterruptible AC System	ESF Support	Ebasco	8.3.1	-	6
Safety Related 125V DC Power System	ESF Support	Ebasco	8.3.2	-	6
Control Room Ventilation	ESF Support	Ebasco	9.4.1	7.3.1-17	6
RAB ESF Equipment Cooling	ESF Support	Ebasco	9.4.5	7.3.1-18	6
Diesel Generator Building Ventilation	ESF Support	Ebasco	9.4.5	7.3.1-19	6
Essential Switchgear Room Cooling	ESF Support	Ebasco	9.4.5	7.3.1-21	6
Electrical Equipment Protection Room HVAC	ESF Support	Ebasco	9.4.5	7.3.1-20	6
Emergency Exhaust Systems	ESF	Ebasco	6.5.1	7.3.1-11 through 7.3.1-14	1,3,5
Spent Fuel Pool Pump Ventilation	ESF Support	Ebasco	9.4.2	7.3.1-22	6
Containment Vacuum Relief	ESF Support	Ebasco	6.2.1.1.3.4	7.3.1-23	1,2,3,4
Fuel Oil Transfer House Ventilation	ESF Support	Ebasco	9.4.5.2.4	7.3.1-24	6
Emergency Service Water Intake Structure Ventilation	ESF Support	Ebasco	9.4.5.2.6	7.3.1-25	6
Diesel Fuel Oil System	ESF Support	Ebasco	9.5.4	7.3.1-26	6

(1) Legend
1. Loss of coolant accident
2. Steam generator tube rupture

TABLE 7.3.1-1 (Continued)

3. Secondary system break (inside Containment)
4. Secondary system break (outside Containment)
5. Fuel handling accident
6. Any of the above
7. Beyond Design Basis Accidents

TABLE 7.3.1-2

INSTRUMENTATION OPERATING CONDITION FOR ENGINEERED SAFETY FEATURES

No.	Functional Unit	No. of Channels	No. of Channels to Trip	Location***
1.	Safety Injection			
	a. Manual	2	1	3
	b. High containment pressure (Hi-1)	3	2	2
	c. Low compensated steam line pressure	9 (3/steam line)	2/3 in any steam line	2
	d. Pressurizer low pressure*	3	2	1
2.	Containment Spray			
	a. Manual**	2	1	3
	b. Containment pressure HI-3	4	2	2

* Permissible bypass if reactor coolant pressure is less than 2,000 psig.

**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.

***Sensor Location Code

1. Inside Containment

2. Outside Containment - Reactor Auxiliary Building

3. Control Room

TABLE 7.3.1-3

INSTRUMENT OPERATING CONDITIONS FOR ISOLATION FUNCTIONS

No.	Functional Unit	No. of Channels	No. of Channels to Trip	Location***
1.	Containment Isolation			
	a. Safety injection (Phase A)	See items 1(a) through 1(d) of Table 7.3.1-2		
	b. Containment pressure HI-3 (Phase B)	See item 2(b) of Table 7.3.1-2		
	c. Manual			
	Phase A	2	1	3
	Phase B	See item 2(a) of Table 7.3.1-2		
2.	Steam Line Isolation			
	a. High steam line pressure rate	9 (3/steamline)	2/3 in any steamline	3
	b. Containment pressure HI-2	3	2	3
	c. Low steamline pressure	9 (3/steamline)	2/3 in any steamline	3
	d. Manual	2	1	3
3.	Feedwater Line Isolation			
	a. SG hi-hi water level (P-14)	12 (4/SG)	2/4 of any SG	3
	b. Safety injection	See item 1 (a through d) of Table 7.3.1-2		
	c. Low T_{avg} and reactor trip (P4)	3	2	3
	d. Manual (component level)			
4.	Containment Ventilation Isolation			
	a. Safety injection	See item 1(a) and 1(d) of Table 7.3.1-2		
	b. Containment radiation	4	2	3
	c. Manual containment spray actuation	See item 2(a) of Table 7.3.1-2		
	d. Manual containment phase A isolation	2	1	3
5.	Control Room Isolation			
	a. Safety injection	See items 1(a) through 1(d) of Table 7.3.1-2		
	b. Control room air intake radiation (normal OAI, north and south emergency OAIs)	2/Intake	1/Intake	3
	c. Manual (component level)			
	d. Control room air intake smoke (normal OAI)	2/Intake	1/Intake	3
6.	FHB Ventilation Isolation			
	a. Spent fuel pool radiation (north and south networks)	4 (3 detectors/channel) per train 2 trains	1 (1 of 3 detectors) per train	4
	b. Manual (component level)			
7.	RAB Ventilation Isolation			
	a. Safety injection	See items 1(a) through 1(d) of Table 7.3.1-2		
	b. Manual (component level)			
	c. Control room air intake radiation (normal OAI, north and south emergency OAIs)	2/Intake	1/Intake	3
	d. Control room intake smoke (normal OAI)	2/Intake	1/Intake	3
8	Auxiliary Feedwater Isolation			
	a. Differential pressure between steamlines coincident with MSIV closure signal	3/Stealmine	2/Steamline indicating that its pressure is low in comparison to other 2 lines	3
	b. Manual (component level)			

TABLE 7.3.1-3 (Continued)

*** Actuating Logic Location Code
3. Control Room
4. Fuel Handling Building

TABLE 7.3.1-4

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Designation	Input	Function Performed
P-4	Reactor tripped	Presence of P-4 signal activates turbine trip
		Presence of P-4 signal closes main feedwater regulating valves on T_{avg} below setpoint
		Presence of P-4 signal prevents opening of main feedwater regulating valves which are closed by SI or high SG water level
		Presence of P-4 signal allows manual reset/block of the automatic reactuation of safety injection
		Absence of P-4 signal defeats the manual reset/block, allowing for automatic reactuation of safety injection
P-11	2/3 pressurizer pressure below setpoint (Presence of P-11 signal permits function shown. Absence of high pressurizer pressure signal defeats function shown and provides confirmatory opening of actuator valves.)	Allows manual block of SI on low pressurizer pressure
		Blocks automatic operation of the pressurizer power operated relief valves and accumulator discharge valves. Allows manual block of safety injection and steamline isolation actuation signals on low steam line pressure. This same blocking action enables steamline isolation actuation which could result from a high rate of decrease of steam pressure.
P-12	2/3 T_{avg} below low-low setpoint (Presence of P-12 signal permits functions shown. Absence of signal defeats functions shown.)	Blocks steam dump except for cooldown condenser dump valves.
		Manual bypass of steam dump block for the cooldown valves only
P-14	2/4 Steam Generator Water Level above setpoint in any steam generator	Trips turbine and all main feedwater pumps, and closes main and bypass feedwater control valves for all steam generators on high-high level signal

TABLE 7.3.1-5 ESF ACTUATION SYSTEMS-SAFETY INJECTION SIGNAL(S)

EQUIPMENT IDENTIFICATION	SERVICE	ACTUATION CHANNEL	ACTION	REFERENCE FIGURE NUMBER	SCHEMATIC/LOGIC NUMBER
APCH (1A-SA)	Charging/Safety Injection Pump A	A	Start Note 1	6.3.4-3	NSSS - CSIP1A
APCH (1B-SB)	Charging/Safety Injection Pump B	B	Start Note 1	6.3.4-3	NSSS - CSIP1B
APCH (1C-SAB)	Charging/Safety Injection Pump C	A&B	Start Note 1	6.3.4-3	NSSS - CSIP1C
APCH (1A-SA)	Residual Heat Removal Pump A	A	Start Note 1	5.4.7-1	NSSS - RHRP1A
APCH (1B-SB)	Residual Heat Removal Pump B	B	Start Note 1	5.4.7-1	NSSS - RHRP1B
APCC (1A-SA)	Component Cooling Pump A	A	Start Note 1	9.2.2-1	NSSS - CCP1A
APCC (1B-SB)	Component Cooling Pump B	B	Start Note 1	9.2.2-1	NSSS - CCP1B
APCC (1C-SAB)	Component Cooling Pump C	A&B	Start Note 1	9.2.2-1	NSSS - CCP1C
2CS-V585SA-1	Charging/Safety Injection Minimum Flow Isolation	A	Close	9.3.4-3	NSSS - 1-8106
2CS-V600SB-1	Charging/Safety Injection Pump A Min. Flow Isolation	B	Close	9.3.4-3	NSSS - 1-8109A
2CS-V602SB-1	Charging/Safety Injection Pump B Min. Flow Isolation	B	Close	9.3.4-3	NSSS - 1-8109B
2CS-V601SB-1	Charging/Safety Injection Pump C Min. Flow Isolation	B	Close	9.3.4-3	NSSS - 1-8109C
2SI-V537SA-1	S.I. Accumulator A Discharge	A	Open	6.3.2-2	NSSS - 1-8808A
2SI-V536SB-1	S.I. Accumulator B Discharge	B	Open	6.3.2-2	NSSS - 1-8808B
2SI-V535SA-1	S.I. Accumulator C Discharge	A	Open	6.3.2-1	NSSS - 1-8803C
2SI-V506SA-1	Boron Injection Tank Outlet Isolation		Open	6.3.2-1	NSSS - 1-8801A
2SI-V505SB-1	Boron Injection Tank Outlet Isolation	A	Open	6.3.2-1	NSSS - 1-8801B
2CS-V610SA-1	Charging Pump to Reactor Coolant System Isolation	B	Close	6.3.4-3	NSSS - 1-8107
2CS-V609SB-1	Charging Pump to Reactor Coolant System Isolation	A	Close	6.3.4-3	NSSS - 1-8108
2CS-V757SA-1	CVCS Miniflow Isolation	B	Open/Close Note 6		
2CS-V759SB-1	CVCS Miniflow Isolation	A	Open/Close Note 6		
2CS-L523SA-1	RWST to Charging Pumps	A	Open	9.3.4-3	NSSS-1-LCV-115B
2CS-L522SB-1	RWST to Charging Pumps	B	Open	9.3.4-3	NSSS-1-LCV-115D
2CS-L520SA-1	Volume Control Tank Outlet Isolation	A	Close	9.3.4-3	NSSS-1-LCV-115C
2CS-L521SB-1	Volume Control Tank Outlet Isolation	B	Close	9.3.4-3	NSSS-1-LCV-115E
3CC-L1SA-1	CCW to Failed Fuel Detector Isolation	A	Close	9.2.2-4	NSSS-1-LCV670
3CC-L2SB-1	CCW to Failed Fuel Detector Isolation	B	Close	9.2.2-4	NSSS-1-LCV676
3CC-D547SA-1	Sample Coolers CCW Isolation	A	Close	9.2.2-4	CAR-2166-B-430-SH31.64
3CC-D54SB-1	Sample Coolers CCW Isolation	B	Close	9.2.2-4	CAR-2166-B-430-SH31.64
AH-1 (1A-SB)	Safety Related Containment Fan Cooler	B	Start Note 1,4	6.2.2-3	CAR-2166-B-430-SH31.64
AH-1 (1B-SB)	Safety Related Containment Fan Cooler	B	Start Note 1,4	6.2.2-3	CAR-2166-B-430-SH31.64
AH-2 (1A-SA)	Safety Related Containment Fan Cooler	A	Start Note 1,4	6.2.2-3	CAR-2166-B-430-SH31.64
AH-2 (1B-SA)	Safety Related Containment Fan Cooler	A	Start Note 1,4	6.2.2-3	CAR-2166-B-430-SH31.64

TABLE 7.3.1-5 ESF ACTUATION SYSTEMS-SAFETY INJECTION SIGNAL(S)

EQUIPMENT IDENTIFICATION	SERVICE	ACTUATION CHANNEL	ACTION	REFERENCE FIGURE NUMBER	SCHEMATIC/LOGIC NUMBER
AH-3 (1A-SA)	Safety Related Containment Fan Cooler	A	Start Note 1,4	6.2.2-3	CAR-2166-B-430-SH31.64
AH-3 (1B-SA)	Safety Related Containment Fan Cooler	A	Start Note 1,4	6.2.2-3	CAR-2166-B-430-SH31.64
AH-4 (1A-SB)	Safety Related Containment Fan Cooler	B	Start Note 1,4	6.2.2-3	CAR-2166-B-430-SH23.8
AH-4 (1B-SB)	Safety Related Containment Fan Cooler	B	Start Note 1,4	6.2.2-3	CAR-2166-B-430-SH23.8
2BD-P6SB-1	Steam Generator 1A Blowdown Isolation Valve	B	Close	10.1.0-6	CAR-2166-B-430-SH23.9
2BD-V11SA-1	Steam Generator 1A Blowdown Isolation Valve	A	Close	10.1.0-6	CAR-2166-B-430-SH23.9
2BD-P7SB-1	Steam Generator 1B Blowdown Isolation Valve	B	Close	10.1.0-6	CAR-2166-B-430-SH23.10
2BD-V15SA-1	Steam Generator 1B Blowdown Isolation Valve	A	Close	10.1.0-6	CAR-2166-B-430-SH23.10
2BD-P8SB-1	Steam Generator 1C Blowdown Isolation Valve	B	Close	10.1.0-6	NSSS - 1-8811B
2BD-V19SA-1	Steam Generator 1C Blowdown Isolation Valve	A	Close	10.1.0-6	NSSS - 1-8811A
2S1-V57OSB-1	Containment Sump to RHRP-B Isol Valve	B	Open Note 5		NSSS - 1-8812B
2S1-V571SA-1	Containment Sump to RHRP-A Isol Valve	A	Open Note 5		NSSS - 1-8812A
2S1-V572SB-1	Containment Sump to RHRP-B Isol Valve	B	Open Note 5		NSSS-1-LCV-115B
2S1-V573SA-1	Containment Sump to RHRP-A Isol Valve	A	Open Note 5		NSSS-1-LCV-115D
2SP-V12OSA-1	Steam Generator 1A Sampling Isolation	A	Close	10.1.0-6	CAR-2166-B-430-SH25.7
2SP-V 9OSB-1	Steam Generator 1A Sampling Isolation	B	Close	10.1.0-6	CAR-2166-B-430-SH25.13
2SP-V 91SB-1	Steam Generator 1A Sampling Isolation	B	Close	10.1.0-6	CAR-2166-B-430-SH25.13
2SP-V121SA-1	Steam Generator 1B Sampling Isolation	A	Close	10.1.0-6	CAR-2166-B-430-SH25.7
2SP-V 85SB-1	Steam Generator 1B Sampling Isolation	B	Close	10.1.0-6	CAR-2166-B-430-SH25.8
2SP-V 86SB-1	Steam Generator 1B Sampling Isolation	B	Close	10.1.0-6	CAR-2166-B-430-SH25.8
2SP-V122SA-1	Steam Generator 1C Sampling Isolation	A	Close	10.1.0-6	CAR-2166-B-430-SH25.7
2SP-V 80SB-1	Steam Generator 1C Sampling Isolation	B	Close	10.1.0-6	CAR-2166-B-430-SH25.8
2SP-V 81SB-1	Steam Generator 1C Sampling Isolation	B	Close	10.1.0-6	CAR-2166-B-430-SH25.8
3SW-B5SA-1	Normal Service Water Header "A" Isolation Valve	A	Close	9.2.1-1	CAR-2166-G-425SO1
3SW-B65B-1	Normal Service Water Header "B" Isolation Valve	B	Close	9.2.1-1	CAR-2166-G-425SO1
3SW-B85A-1	S.W. Return Header to Cooling Tower Isolation Valve	A	Close	9.2.1-1	CAR-2166-G-425SO1
3SW-B13SA-1	S.W. Return Header "A" to Cooling Tower Isolation Valve	A	Close	9.2.1-1	CAR-2166-G-425SO1
3SW-B14SB-1	S.W. Return Header "B" to Cooling Tower Isolation Valve	B	Close	9.2.1-1	CAR-2166-G-425SO1
3SW-B237SA-1	CVCS Chillers Service Water Inlet Isolation Valve	A	Close	9.2.1-1	CAR-2166-G-425SH.30.3
3SW-B238SB-1	CVCS Chillers Service Water Inlet Isolation Valve	B	Close	9.2.1-1	CAR-2166-G-425SH.30.3
3SW-B266SA-1	CVCS Chillers Service Water Outlet Isolation Valve	A	Close	9.2.1-1	CAR-2166-B-430SH.30.3
3SW-B267SB-1	CVCS Chillers Service Water Outlet Isolation Valve	B	Close	9.2.1-1	CAR-2166-B-430SH.30.3
(1A-SA)	Emergency Service Water Pump A	A	Start Note 1	9.2.1-1	CAR-2166-G-425SO2

TABLE 7.3.1-5 ESF ACTUATION SYSTEMS-SAFETY INJECTION SIGNAL(S)

EQUIPMENT IDENTIFICATION	SERVICE	ACTUATION CHANNEL	ACTION	REFERENCE FIGURE NUMBER	SCHEMATIC/LOGIC NUMBER
(1B-SB)	Emergency Service Water Pump B	B	Start Note 1	9.2.1-1	CAR-2166-G-425SO2
(1A-SA)	Service Water Booster Pump A	A	Start Note 1	9.2.1-1	CAR-2166-G-425SO2
(1B-SB)	Service Water Booster Pump B	B	Start Note 1	9.2.1-1	CAR-2166-G-425SO2
3SW-B15SA-1	Service Water Return Header A to Aux. Reservoir Isolation		Open	9.2.1-1	CAR-2166-G-425SO1
3SW-B16SB-1	Service Water Return Header B to Aux. Reservoir Isolation	B	Open	9.2.1-1	CAR-2166-G-425SO1
3CX-V2280SA-1	Chilled Water Normal Makeup Isol Valve System A	A	Close Note 7	9.2.8-3	CAR-2166-B-430SH31.82G
3CX-V2281SB-1	Chilled Water Normal Makeup Isol Valve System A	B	Close Note 7	9.2.8-3	CAR-2166-B-430SH31.82G
3CX-V2282SA-1	Chilled Water Normal Makeup Isol Valve System B	A	Close Note 7	**	CAR-2166-B-430SH31.82H
3CX-V2283SB-1	Chilled Water Normal Makeup Isol Valve System B	B	Close Note 7	**	CAR-2166-B-430SH31.82H
3CH-B3SA-1	ESF Chilled Water System “A” Isolation	A	Close	-	CAR-2166-B-430SH31.82B
3CH-B4SB-1	ESF Chilled Water System “A” Isolation	B	Close	-	CAR-2166-B-430SH31.82B
3CX-B4SA-1	ESF Chilled Water System “A” Isol	A	Close	-	CAR-2166-B-430SH31.82B
3CX-B3SB-1	ESF Chilled Water System “A” Isol	B	Close	-	CAR-2166-B-430SH31.82B
3CH-B2SA-1	ESF Chilled Water System “A” Isol	A	Close	-	CAR-2166-B-430SH31.82B
3CH-B1SB-1	ESF Chilled Water System “A” Isol	B	Close	-	CAR-2166-G-430SH31.82B
3CX-B2SA-1	ESF Chilled Water System “A” Isol	A	Close	-	CAR-2166-G-430SH31.82B
3CX-B1SB-1	ESF Chilled Water System “A” Isol	B	Close	-	CAR-2166-G-430SH31.82B
WC-2(1A-SA)	ESF Water Chiller A	B	Start Note 1	9.2.8-3	CAR-2166-B-430SH31.82A
WC-2(1B-SB)	ESF Water Chiller B	A	Start Note 1	**	CAR-2166-B-430SH31.83A
AH-15(1A-SA)	Control Room HVAC Normal Supply Fan	B	Start Note 1	9.4.1-1	CAR-2166-B-440SH31.121
AH-15(1A-SB)	Control Room HVAC Normal Supply Fan	A	Start Note 1	9.4.1-1	CAR-2166-B-440SH31.121
3CZ-B1SA-1	Control Room HVAC Normal Intake Valve	B	Close Note 3	9.4.1-1	CAR-2166-B-430SH31.120
3CZ-B2SB-1	Control Room HVAC Normal Intake Valve	A	Close Note 3	9.4.1-1	CAR-2166-B-430SH31.120
3CZ-B3SA-1	Control Room HVAC Normal Exhaust Valve	B	Close Note 3	9.4.1-1	CAR-2166-B-430SH31.122
3CZ-B4SB-1	Control Room HVAC Normal Exhaust Valve	A	Close Note 3	9.4.1-1	CAR-2166-B-430SH31.122
ES-1(1A-NSS)	Control Room HVAC Purge Exhaust Fan	B	Stop Note 3	9.4.1-1	CAR-2166-B-430SH31.123
ES-1(1B-NSS)	Control Room HVAC Purge Exhaust Fan	A	Stop Note 3	9.4.1-1	CAR-2166-B-430SH31.123
3CZ-B13SA-1	Control Room HVAC Purge Exhaust Valve	B	Close Note 3	9.4.1-1	CAR-2166-B-430SH31.123
3CZ-B14SB-1	Control Room HVAC Purge Exhaust Valve	A	Close Note 3	9.4.1-1	CAR-2166-B-430SH31.123
3CZ-B17SA-1	Control Room HVAC Purge Makeup Valve	B	Close Note 3	9.4.1-1	CAR-2166-B-430SH31.120
3CZ-B18SB-1	Control Room HVAC Purge Makeup Valve	A	Close Note 3	9.4.1-1	CAR-2166-B-430SH31.120
3CZ-D16SA-1	Control Room HVAC Post Accident Return Branch Damper	B	Close Note 3	9.4.1-1	CAR-2166-B-430SH31.122

TABLE 7.3.1-5 ESF ACTUATION SYSTEMS-SAFETY INJECTION SIGNAL(S)

EQUIPMENT IDENTIFICATION	SERVICE	ACTUATION CHANNEL	ACTION	REFERENCE FIGURE NUMBER	SCHEMATIC/LOGIC NUMBER
3CZ-D11SB-1	Control Room HVAC Post Accident Return Branch Damper	A	Close Note 3	9.4.1-1	CAR-2166-B-430SH31.122
R-2(1A-SA)	Control Room HVAC Emergency Filtration Unit Fan	B	Start Note 1	9.4.1-1	CAR-2166-B-430SH31.130
R-2(1B-SB)	Control Room HVAC Emergency Filtration Unit Fan	B	Start Note 1	9.4.1-1	CAR-2166-B-430SH31.130
1A-SA	Emergency Diesel Generator	A	Start	N/A	CAR-2166-G-427
1B-SB	Emergency Diesel Generator	B	Start	N/A	CAR-2166-G-427
1A-SA	Auxiliary Feedwater Pump	A	Start Note 1	10.1.0-3&4	CAR-2166-B-430SH31.181
1B-SB	Auxiliary Feedwater Pump	B	Start Note 1	10.1.0-3&4	CAR-2166-B-430SH31.181
1A-SA	Emergency Intake Screen Wash Pump	A	Start Note 1	N/A	CAR-2166-B-430SH31.183
1B-SB	Emergency Intake Screen Wash Pump	B	Start Note 1	N/A	CAR-2166-B-430SH31.183
1A-SA	Emergency Intake Traveling Screen	A	Start Note 1	N/A	CAR-2166-B-430SH31.237A
1B-SB	Emergency Intake Traveling Screen	B	Start Note 1	N/A	CAR-2166-B-430SH31.237B
1A-SA	Emergency Service Water Strainer	A	Start Note 2	N/A	CAR-2166-B-430SH31.85
1B-SB	Emergency Service Water Strainer	B	Start Note 2	N/A	CAR-2166-B-430SH31.85
E-86(1A-SA)	Diesel Generator Room Exhaust Fan	A	Start Note 1	9.4.5-2	CAR-2166-B-430SH31.85
E-86(1C-SB)	Diesel Generator Room Exhaust Fan	B	Start Note 1	9.4.5-2	CAR-2166-B-430SH31.85
E-85(1A-SA)	Fuel Oil Transfer Pump House Exhaust Fan	A	Start Note 1	9.4.5-2	CAR-2166-B-430SH31.85
E-85(1C-SB)	Fuel Oil Transfer Pump House Exhaust Fan	B	Start Note 1	9.4.5-2	CAR-2166-G-427
S-64(1X-SA)	R.A.B. Pipe Tunnel Ventilation Fan	A	Start Note 1	9.4.3-2	CAR-2166-G-427
S-65(1X-SB)	R.A.B. Pipe Tunnel Ventilation Fan	B	Start Note 1	9.4.3-2	CAR-2166-B-430SH31.181
AH-5(1A-SA)	RHR Pump Air Handling Unit	A	Start Note 1	9.4.3-1	CAR-2166-B-430SH31.181
AH-5(1B-SB)	RHR Pump Air Handling Unit	B	Start Note 1	9.4.3-1	CAR-2166-B-430SH31.183
AH-6(1A-SA)	CCW Pump Air Handling Unit	A	Start Note 1	9.4.3-1	CAR-2166-B-430SH31.183
AH-6(1B-SB)	CCW Pump Air Handling Unit	B	Start Note 1	9.4.3-1	CAR-2166-B-430SH31.237A
AH-7(1B-SB)	CCW Pump Air Handling Unit	B	Start Note 1	9.4.3-1	CAR-2166-B-430SH31.85
AH-9(1A-SA)	Charging Pump Air Handling Unit	A	Start Note 1	9.4.3-1	CAR-2166-B-430SH31.85
AH-9(1B-SB)	Charging Pump Air Handling Unit	B	Start Note 1	9.4.3-1	CAR-2166-B-430SH31.85
AH-10(1A-SA)	Charging Pump Air Handling Unit	A	Start Note 1	9.4.3-1	CAR-2166-B-430SH31.85
AH-10(1B-SB)	Charging Pump Air Handling Unit	B	Start Note 1	9.4.3-1	CAR-2166-B-430SH31.85
AH-92(1A-SA)	MCC 1A35 & 1B35 Air Handling Unit	A	Start Note 1	-	CAR-2166-B-430SH31.85A3
AH-92(1B-SB)	MCC 1A35 & 1B35 Air Handling Unit	B	Start Note 1	-	CAR-2166-B-430SH31.85A3
AH-93(1X-SA)	Rod Cabinet Air Handling Unit	A	Start Note 1	-	CAR-2166-B-430SH31.85A1
AH-11(1A-SA)	Mechanical Penetration Area Air Handling Unit	A	Start Note 1	9.4.3-1	CAR-2166-B-430SH31.85
AH-11(1B-SB)	Mechanical Penetration Area Air Handling Unit	B	Start Note 1		CAR-2166-B-430SH31.85

TABLE 7.3.1-5 ESF ACTUATION SYSTEMS-SAFETY INJECTION SIGNAL(S)

EQUIPMENT IDENTIFICATION	SERVICE	ACTUATION CHANNEL	ACTION	REFERENCE FIGURE NUMBER	SCHEMATIC/LOGIC NUMBER
AH-19(1A-SA)	Aux. Feedwater Pump & HVAC Chiller Air Handling Unit	A	Start Note 1	9.4.3-2	CAR-2166-B-430SH31.85
AH-19(1B-SB)	Aux. Feedwater Pump & HVAC Chiller Air Handling Unit	B	Start Note 1	9.4.3-2	CAR-2166-B-430SH31.85
AH-20(1A-SA)	Aux. Feedwater Pump & HVAC Chiller Air Handling Unit	A	Start Note 1	9.4.3-2	CAR-2166-B-430SH31.85
AX-20(1B-SB)	Aux. Feedwater Pump & HVAC Chiller Air Handling Unit	B	Start Note 1	9.4.3-2	CAR-2166-B-430SH31.85
AH-23(1X-SA)	Mech. & Electrical Penetration Area Air Handling Unit	A	Start Note 1	9.4.3-1	CAR-2166-B-430SH31.85
AH-24(1X-SA)	Electrical Penetration Area Air Handling Unit	A	Start Note 1	9.4.3-2	CAR-2166-B-430SH31.85
AH-25(1X-SB)	Electrical Penetration Area Air Handling Unit	B	Start Note 1	9.4.3-2	CAR-2166-B-430SH31.85
AH-26(1A-SA)	HV Equipment Room #2 Air Handling Unit	A	Start Note 1	9.4.3-1	CAR-2166-B-430SH31.85
AH-26(1B-SB)	HV Equipment Room #1 Air Handling Unit	B	Start Note 1	9.4.3-1	CAR-2166-B-430SH31.85
AH-28(1A-SA)	Mechanical Penetration Area Air Handling Unit	A	Start Note 1	9.4.3-1	CAR-2166-B-430SH31.85
AH-28(1B-SB)	Boron Inj. Tank Area Air Handling Unit	B	Start Note 1	9.4.3-1	CAR-2166-B-430SH31.85
AH-29(1X-SB)	Secondary WPB Evap. Access Aisle Air Handling Unit	B	Start Note 1	9.4.3-6	CAR-2166-B-430SH31.85
AH-8(1X-SB)	Service Water Booster Pump Area Air Handling Unit	B	Start Note 1	9.4.3-1	CAR-2166-B-430SH31.85
AH-12(1A-SA)	Switchgear Room “A” Supply Fan	A	Start Note 3	9.4.5-1	CAR-2166-B-430SH31.73A
3CZ-B5SA-1	Electric Equipment Protection Room Ventilation Isolation Vlv	A	Close Note 3	9.4.5-1	CAR-2166-B-430SH31.30A
3CZ-B6SB-1	Electric Equipment Protection Room Ventilation Isolation Vlv	B	Close Note 3	9.4.5-1	CAR-2166-B-430SH31.30A
3CZ-B7SA-1	Electric Equipment Protection Room Ventilation Isolation Vlv	A	Close Note 3	9.4.5-1	CAR-2166-B-430SH31.29
3CZ-B8SB-1	Electric Equipment Protection Room Ventilation Isolation Vlv	B	Close Note 3	9.4.5-1	CAR-2166-B-430SH31.29
3AV-D3SA-1	RAB Normal Ventilation Branch Isol. Dampers	A	Close	9.4.3-2	-
3AV-D4SB-1	RAB Normal Ventilation Branch Isol. Dampers	B	Close	9.4.5-1	-
3AV-D5SA-1	RAB Normal Ventilation Branch Isol. Dampers	A	Close	9.4.5-1	-
3AV-D6SB-1	RAB Normal Ventilation Branch Isol. Dampers	B	Close	9.4.5-1	-
3AV-D7SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D8SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D9SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-2	-
3AV-D10SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-2	-
3AV-D11SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D12SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-

TABLE 7.3.1-5 ESF ACTUATION SYSTEMS-SAFETY INJECTION SIGNAL(S)

EQUIPMENT IDENTIFICATION	SERVICE	ACTUATION CHANNEL	ACTION	REFERENCE FIGURE NUMBER	SCHEMATIC/LOGIC NUMBER
3AV-D13SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D14SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D15SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D16SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D17SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D18SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D19SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D20SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D21SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D22SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D23SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D24SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D25SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D26SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D27SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D28SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D29SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D30SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D31SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D32SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D33SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D34SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D35SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D36SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D37SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D38SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D52SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D53SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D58SB-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D59SA-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D62SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D63SA-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D66SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D67SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D70SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-

TABLE 7.3.1-5 ESF ACTUATION SYSTEMS-SAFETY INJECTION SIGNAL(S)

EQUIPMENT IDENTIFICATION	SERVICE	ACTUATION CHANNEL	ACTION	REFERENCE FIGURE NUMBER	SCHEMATIC/LOGIC NUMBER
3AV-D71SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D74SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D75SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D78SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D79SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
3AV-D82SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-1	-
3AV-D83SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-1	-
AV-D86SA-1	RAB Normal Ventilation. Branch Isol. Dampers	A	Close	9.4.3-2	CAR-2166-B-430SH31.35D
AV-D87SB-1	RAB Normal Ventilation. Branch Isol. Dampers	B	Close	9.4.3-2	CAR-2166-B-430SH31.350
AH-16(1A-SA)	Electric Equipment Protection Room Ventilation Supply Fan	A	Start Note 1	9.4.5-1	CAR-2166-B-430SH31.30A
AH-16(1B-SB)	Electric Equipment Protection Room Ventilation Supply Fan	B	Start Note 1	9.4.5-1	CAR-2166-B-430SH31.30A
E-10 (1A-SA)	Electric Equipment Protection Room Ventilation Exhaust Fan	A	Stop Note 3	9.4.5-1	CAR-2166-B-430SH31.29
E-10 (1B-SB)	Electric Equipment Protection Room Ventilation Exhaust Fan	B	Stop Note 3	9.4.5-1	CAR-2166-B-430SH31.29
E-17 (1X-NNS)	RAB Normal Exhaust Fan	A&B	Stop	9.4.3-2	CAR-2166-B-430SH31.35P
E-18 (1X-NNS)	RAB Normal Exhaust Fan	A&B	Stop	9.4.3-2	CAR-2166-B-430SH31.35Q
E-19 (1X-NNS)	RAB Normal Exhaust Fan	A&B	Stop	9.4.3-2	CAR-2166-B-430SH31.35R
E-20 (1X-NNS)	RAB Normal Exhaust Fan	A&B	Stop	9.4.3-2	CAR-2166-B-430SH31.35S
E-6 (1A-SA)	RAB Emergency Exhaust Fan	A	Start Notes 1,3	9.4.3-2	CAR-2166-B-430SH31.33
E-6 (1B-SB)	RAB Emergency Exhaust Fan	B	Start Notes 1,3	9.4.3-2	CAR-2166-B-430SH31.33A
S-3 (1A-NNS)	RAB Normal Supply Fan	A&B	Stop	9.4.3-2	CAR-2166-B-430SH31.37J
S-3 (1B-NNS)	RAB Normal Supply Fan	A&B	Stop	9.4.3-2	CAR-2166-B-430SH31.37J
1A-SA	Emergency Load Sequencer Panel A	A	Start	N/A	CAR-2166-G-509501C
1B-SB	Emergency Load Sequencer Panel B	B	Start	N/A	CAR-2166-G-509502
E-61 (1A-SA)	Diesel Generator Bldg. Exhaust Fan	A	Start Note 1	9.4.5-2	CAR-2166-B-430SH31.180A
E-61 (1B-SB)	Diesel Generator Bldg. Exhaust Fan	B	Start Note 1	9.4.5-2	CAR-2166-B-430SH31.180B
3AF-F1SA-1	AFW TO STM. GEN. 1A REG. VALVE	A OR B	OPEN	10.1.0-03	2166-G-427
3AF-F3SA-1	AFW TO STM. GEN. 1B REG. VALVE	A OR B	OPEN	10.1.0-03	2166-G-427
3AF-F2SA-1	AFW TO STM. GEN. 1C REG. VALVE	A OR B	OPEN	10.1.0-03	2166-G-427
2SP-V405SA-1	Cont. Atmos. Rad. Monitor Isol.	A	Close		
2SP-V304SA-1	Cont. Atmos. Sys. Cont. Isol.	A	Close		
2SP-V302SB-1	Cont. Atmos. Sys. Cont. Isol.	B	Close		

TABLE 7.3.1-5 ESF ACTUATION SYSTEMS-SAFETY INJECTION SIGNAL(S)

EQUIPMENT IDENTIFICATION	SERVICE	ACTUATION CHANNEL	ACTION	REFERENCE FIGURE NUMBER	SCHEMATIC/LOGIC NUMBER
2SP-V303SB-1	Cont. Atmos. Sys. Cont. Isol.	B	Close		
2SP-V305SA-1	Cont. Atmos. Sys. Cont. Isol.	A	Close		
AH-85(1A-SA)	D.G. Elect. Equip. Air Handling Unit	A	Start Note 1	9.4.5-2	CAR-2166-B-430SH31.182A
AH-85(1C-SB)	D.G. Elect. Equip. Air Handling Unit	B	Start Note 1	9.4.5-2	CAR-2166-B-430SH31.182B
1A1A-SA	6.9 KV Emer. Bus 1A-SA to Transf. 1A1	A	Open Note 1		
1B1A-SB	6.9 KV Emer. Bus 1B-SB to Transf. 1B1	B	Open Note 1		

Note 1: Equipment started via the emergency load sequencer of its respective safety train.
Note 2: Equipment indirectly started as slave of other equipment actuated by the safety signal.
Note 3: Equipment operations are initiated via the control room isolation signal.
Note 4: One fan per unit started as selected by lead fan selector switch.
Note 5: Valves open on SIAS coincident with RWST Lo-Lo Level
Note 6: Valves open/close on "S" coincident with RCS pressure.
Note 7: These valves are wired to close upon a SIAS; however, they are not credited for an active safety function (Ref. EC 51444).
* For NSSS supplied equipment the number is the valve number from which the schematic/logic can be found.
** Only train A is shown in Figure 9.2.8-3 as a representative.

TABLE 7.3.1-6

ESF ACTUATION SYSTEMS
CONTAINMENT SPRAY ACTUATION SIGNAL (CSAS)

EQUIPMENT IDENTIFICATION	SERVICE	ACTUATION CHANNEL	ACTION	REFERENCE FIGURE NUMBER	SCHEMATIC/LOGIC NUMBER
1A-SA	Containment Spray Pump A	A	Start	6.2.2-1	CAR-2166-G-423
1B-SB	Containment Spray Pump B	B	Start	6.2.2-1	CAR-2166-G-423
3CT-V21SA-1	Containment Spray Header A Isolation Valve	A	Open	6.2.2-1	CAR-2166-G-423
3CT-V43SB-1	Containment Spray Header B Isolation Valve	B	Open	6.2.2-1	CAR-2166-G-423
3CT-V85SA-1	Containment Spray Chemical Addition A Valve	A	Open	6.2.2-1	CAR-2166-G-423
3CT-V88SB-1	Containment Spray Chemical Addition B Valve	B	Open	6.2.2-1	CAR-2166-G-423
1A-SA	Emergency Load Sequencer Panel A	A	Start Note 1	N/A	CAR-2166-SK-E-463
1A-SB	Emergency Load Sequencer Panel B	B	Start Note 1	N/A	CAR-2166-SK-E-463

Notes:
1. The containment spray pumps will be started via the emergency load sequencer during an accident condition whenever the sequencer is operated and CSAS exists.

TABLE 7.3.1-7 ESF ACTUATION SYSTEMS-CONTAINMENT ISOLATION PHASE-A (T)

EQUIPMENT IDENTIFICATION	SERVICE	ACTUATION CHANNEL	ACTION	REFERENCE FIGURE NUMBER	SCHEMATIC/LOGIC NUMBER
2CS-V518SB-1	Letdown Line Isolation Valve	B	Close	9.3.4-1	NSSS 1-8152
2CS-V511SA-1	Letdown Line Isolation Valve	A	Close	9.3.4-1	NSSS 1-8149A
2CS-V512SA-1	Letdown Line Isolation Valve	A	Close	9.3.4-1	NSSS 1-8149B
2CS-V513SA-1	Letdown Line Isolation Valve	A	Close	9.3.4-1	NSSS 1-8149C
2SI-V554SB-1	Accumulator Fill Line Isolation	B	Close	6.3.2-2	NSSS 1-8860
2SI-V530SB-1	Nitrogen Supply Accumulator Tank Header Isolation	B	Close	6.3.2-2	NSSS 1-8880
2SI-V555SA-1	Accumulator Test Line to R.W.S.T. Isolation	A	Close	6.3.2-2	NSSS 1+8871
2SI-V550SB-1	Accumulator Test Line to R.W.S.T. Isolation	B	Close	6.3.2-2	NSSS 1-8961
2RC-D525SB-1	Pressurizer Relief Tank Spray Isolation	B	Close	5.1.2-2	NSSS 1-8028
2RC-D528SA-1	Pressurizer Relief Tank Nitrogen Supply Supply Isolation	A	Close	5.1.2-2	NSSS 1-8047
2RC-D529SB-1	Pressurizer Relief Tank Nitrogen Supply Supply Isolation	B	Close	5.1.2-2	NSSS 1-8033
2WL-D650SB-1	R.C. Drain Tank Pump Discharge	B	Close	-	NSSS 1-7136
2WG-D590SA-1	R.C. Drain Tank Gas Sample and Hydrogen Makeup	A	Close	-	NSSS 1-7126
2WG-D291SB-1	R.C. Drain Tank Gas Sample and Hydrogen Makeup	B	Close	-	NSSS 1-7150
2WL-L600SA-1	R.C. Drain Tank Pump Discharge	A	Close	-	NSSS 1-LCY-1003
2CS-V516SA-1	R.C. Pump Seal Water Return Isolation	A	Close	9.3.4-1	NSSS 1-8112
2CS-V517SB-1	R.C. Pump Seal Water Return Isolation	B	Close	9.3.4-1	NSSS 1-8100
2CC-V182SB-1	Excess Letdown Heat Exchanger Cooling Water Return	B	Close	9.2.2-3	NSSS 1-9486
2CC-V172SB-1	Excess Letdown Heat Exchanger Cooling Water Supply	B	Close	9.2.2-3	NSSS 1-9485
2SW-B88SAB-1	Containment Fan Cooler Normal Service Water Supply	A&B	Close	9.2.1-1	CAR-2166-B-430-SH21.7
2SW-B89SA-1	Containment Fan Cooler Normal Service Water Return	A	Close	9.2.1-1	CAR-2166-B-430-SH21.7
2SW-B90SB-1	Containment Fan Cooler Normal Service Water Return	B	Close	9.2.1-1	CAR-2166-B-430-SH21.7
2MS-V122SAB-1	Main Steam Sampling Isolation Valve Stm Gen. 1A	A&B	Close	10.1.0-1	CAR-2166-B-430-SH25.9
2MS-V124SAB-1	Main Steam Sampling Isolation Valve Stm Gen. 1B	A&B	Close	10.1.0-1	CAR-2166-B-430-SH25.9
2MS-V126SAB-1	Main Steam Sampling Isolation Valve Stm Gen. 1C	A&B	Close	10.1.0-1	CAR-2166-B-430-SH25.9
2SP-V2SA-1	Pressurizer Steam Space Sample Isolation Valve	A	Close	9.3.2-1	CAR-2166-B-430SH25.3
2SP-V12SA-1	Pressurizer Liquid Space Sample Isolation Valve	A	Close	9.3.2-1	CAR-2166-B-430SH25.3
2SP-V23SA-1	RCS Hot Leg Loops 2&3 Sample Isolation Valve	A	Close	9.3.2-1	CAR-2166-B-430SH25.3
2SP-V116SA-1	SIS Accumulator Sample Isolation Valve	A	Close	9.3.2-1	CAR-2166-B-430SH25.3
2SP-V1 SB-1	Pressurizer Steam Space Sample Isolation	B	Close	9.3.2-1	CAR-2166-B-430SH25.1

TABLE 7.3.1-7 ESF ACTUATION SYSTEMS-CONTAINMENT ISOLATION PHASE-A (T)

EQUIPMENT IDENTIFICATION	SERVICE	ACTUATION CHANNEL	ACTION	REFERENCE FIGURE NUMBER	SCHEMATIC/LOGIC NUMBER
2SP-V11 SB-1	Pressurizer Liquid Space Sample Isolation	B	Close	9.3.2-1	CAR-2166-B-430SH25.1
2SP-V111SB-1	RCS Hot Leg Loops 2&3 Sample Isolation Valve	B	Close	9.3.2-1	CAR-2166-B-430SH25.2
2SP-V113SB-1	SIS Accumulator 1A Sample Isolation Valve	B	Close	9.3.2-1	CAR-2166-B-430SH25.2
2SP-V114SB-1	SIS Accumulator 1B Sample Isolation Valve	B	Close	9.3.2-1	CAR-2166-B-430SH25.1
2SP-V115SB-1	SIS Accumulator 1C Sample Isolation Valve	B	Close	9.3.2-1	CAR-2166-B-430SH25.1
2MD-V36SA-1	Containment Sump Pump Discharge Isolation	A	Close	9.3.3-2	CAR-2166-B-430SH30.1
2MD-V77SB-1	Containment Sump Pump Discharge Isolation	B	Close	9.3.3-2	CAR-2166-B-430SH30.1
2IA-V192SA-1	Containment Building Instrument Air Isolation	A	Close	9.3.2-1	CAR-2166-B-430SH30.3
AH-37 (1A-NSS)	Non-Nuclear Safety Containment Fan Cooler	A&B	Stop	6.2.2-3	CAR-2166-B-430SH31.64A
AH-37 (1B-NSS)	Non-Nuclear Safety Containment Fan Cooler	A&B	Stop	6.2.2-3	CAR-2166-B-430SH31.64A
AH-38 (1A-NSS)	Non-Nuclear Safety Containment Fan Cooler	A&B	Stop	6.2.2-3	CAR-2166-B-430SH31.64A
AH-38 (1A-NSS)	Non-Nuclear Safety Containment Fan Cooler	A&B	Stop	6.2.2-3	CAR-2166-B-430SH31.64A
AH-39 (1B-NSS)	Non-Nuclear Safety Containment Fan Cooler	A&B	Stop	6.2.2-3	CAR-2166-B-430SH31.64A
AH-39 (1B-NSS)	Non-Nuclear Safety Containment Fan Cooler	A&B	Stop	6.2.2-3	CAR-2166-B-430SH31.64A
2FP-B1SA-1	Fire Protection-Containment Water Sprinkler Isolation	A	Close	9.5.1-4	Delete Manual Value
2CT-V25SA-1	Containment Spray Header Recirculation Isolation	A	Close	6.2.2-1	CAR-2166-B-430SH30.3
2CT-V49SB-1	Containment Spray Header Recirculation Isolation	B	Close	6.2.2-1	CAR-2166-G-423
2CT-V8SA-1	Containment Spray Eductor Test Valve Isolation	A	Close	6.2.2-1	CAR-2166-G-423
2CT-V145SB-1	Containment Spray Eductor Test Valve Isolation	B	Close	6.2.2-1	CAR-2166-G-423
2SP-V300SA-1	Containment H2 Sampling System A Cont. Isolation	A	Close	-	-
2SP-V308SB-1	Containment H2 Sampling System A Cont. Isolation	B	Close	-	-
2SP-V309SB-1	Containment H2 Sampling System A Cont. Isolation	B	Close	-	-
2SP-V348SA-1	Containment H2 Sampling System A Cont. Isolation	A	Close	-	
2SP-V349SA-1	Containment H2 Sampling System A Cont. Isolation	A	Close	-	
2SP-V301SA-1	Cont. H2 Sampling System A Cont. Iso.	A	Close	-	-
2SP-V314SB-1	Containment H2 Sampling System B Isolation	B	Close	-	N/A
2SP-V315SB-1	Containment H2 Sampling System B Isolation	B	Close	-	N/A
2AF-V162SAB-1	Hydrazine to AFW Steam Generator 1A/Disabled	M	LC		
2AF-V163SAB-1	Ammonia to AFW Steam Generator 1A/Disabled	M	LC		
2AF-V164SAB-1	Hydrazine to AFW Steam Generator 1B/Disabled	M	LC		
2AF-V165SAB-1	Ammonia to AFW Steam Generator 1B/Disabled	M	LC		
2AF-V166SAB-1	Hydrazine to AFW Steam Generator 1C/Disabled	M	LC		
2AF-V167SAB-1	Ammonia to AFW Steam Generator 1C/Disabled	M	LC		
2SP-V408SB-1	PASS Isolation	B	Close		
2SP-V409SA-1	PASS Isolation	A	Close		
2SP-V406SB-1	PASS Isolation	B	Close		
2SP-V407SA-1	PASS Isolation	A	Close		

TABLE 7.3.1-7 ESF ACTUATION SYSTEMS-CONTAINMENT ISOLATION PHASE-A (T)

EQUIPMENT IDENTIFICATION	SERVICE	ACTUATION CHANNEL	ACTION	REFERENCE FIGURE NUMBER	SCHEMATIC/LOGIC NUMBER
1A-SA	Containment Spray Pump Interlock Trip	A	Stop Note 1	6.2.2-1	-
1B-SB	Containment Spray Pump Interlock Trip	B	Stop Note 1	6.2.2-1	-
2SP-V448SA-1	Containment Atmos. Mon. System A Cont. Iso.	A	Close	-	
2SP-V449SB-1	Containment Atmos. Mon. System A Cont. Iso.	A	Close	-	
2SP-V450SA-1	Containment Atmos. Mon. System A Cont. Iso.	A	Close	-	
2SP-V451SB-1	Containment Atmos. Mon. System A Cont. Iso.	A	Close	-	

Notes:
1. Interlock applicable only when the recirculation valve of its respective safety train is open.

TABLE 7.3.1-8

ESF ACTUATION SYSTEMS-CONTAINMENT ISOLATION PHASE-B (P)

EQUIPMENT IDENTIFICATION	SERVICE	ACTUATION CHANNEL	ACTION	REFERENCE FIGURE NUMBER	SCHEMATIC/LOGIC NUMBER
2CC-V169SA-1	Reactor Coolant Pump Cooling Water Supply	A	Close	9.2.2-3	NSSS 1-9480A
2CC-V170SB-1	Reactor Coolant Pump Cooling Water Supply	B	Close	9.2.2-3	NSSS 1-94808
2CC-V183SB-1	Reactor Coolant Pump Cooling Water Return	B	Close	9.2.2-3	NSSS 1-9482
2CC-V184SA-1	Reactor Coolant Pump Cooling Water Return	A	Close	9.2.2-3	NSSS 1-9481
2CC-V190SB-1	R.C. Pump Thermal Barrier Cooling Water Return	B	Close	9.2.2-3	NSSS 1-9484
2CC-V191SA-1	R.C. Pump Thermal Barrier Cooling Water Return	A	Close	9.2.2-3	NSSS 1-9483

TABLE 7.3.1-9

ESF ACTUATION SYSTEMS
CONTAINMENT VENTILATION ISOLATION SIGNAL (CVIS)

EQUIPMENT IDENTIFICATION	SERVICE	ACTUATION CHANNEL	ACTION	REFERENCE FIGURE NUMBER	SCHEMATIC/LOGIC NUMBER
2CB-B1SA-1	Containment Relief Valve	A	Close	6.2.2-3	CAR-2166-B-430SH31.17
2CB-B2SB-1	Containment Relief Valve	B	Close	6.2.2-3	CAR-2166-B-430SH31.18
3CB-D1SA-1	Containment Relief Damper	A	Close	6.2.2-3	CAR-2166-B-430SH31.17
3CB-D2SB-1	Containment Relief Damper	B	Close	6.2.2-3	CAR-2166-B-430SH31.18
2CP-B1SA-1	Normal Containment Purge Inlet Isolation Valve	A	Close	6.2.2-3	CAR-2166-B-430SH31.210
2CP-B2SB-1	Normal Containment Purge Inlet Isolation Valve	B	Close	6.2.2-3	CAR-2166-B-430SH31.190
2CP-B5SA-1	Normal Containment Purge Outlet Isolation Valve	A	Close	6.2.2-3	CAR-2166-B-430SH31.210
2CP-B6SB-1	Normal Containment Purge Outlet Isolation Valve	B	Close	6.2.2-3	CAR-2166-B-430SH31.210
2CP-B3SA-1	Containment Preentry Purge Inlet Isolation Valve	A	Close	6.2.2-3	CAR-2166-B-430SH31.210
2CP-B4SB-1	Containment Preentry Purge Inlet Isolation Valve	B	Close	6.2.2-3	CAR-2166-B-430SH31.209
2CP-B7SA-1	Containment Preentry Purge Outlet Isolation Valve	A	Close	6.2.2-3	CAR-2166-B-430SH31.210
2CP-B8SB-1	Containment Preentry Purge Outlet Isolation Valve	A	Close	6.2.2-3	CAR-2166-B-430SH31.210
AH-82(1A-NNS)	Normal Containment Purge Fan	A and B	Stop	6.2.2-3	CAR-2166-B-430SH31.190
AH-82(1B-NNS)	Normal Containment Purge Fan	A and B	Stop	6.2.2-3	CAR-2166-B-430SH31.190

TABLE 7.3.1-10

ESF ACTUATION SYSTEMS
MAIN STEAM ISOLATION SIGNAL (MSIS)

EQUIPMENT IDENTIFICATION	SERVICE	ACTUATION CHANNEL	ACTION	REFERENCE FIGURE NUMBER	SCHEMATIC/LOGIC NUMBER
2MS-V1SAB-1	Main Isolation Valve - Steam Generator 1A	A&B	Close	10.1.0-1	CAR-2166-B-430SH8.8
2MS-V2SAB-1	Main Isolation Valve - Steam Generator 1B	A&B	Close	10.1.0-1	CAR-2166-B-430SH8.9
2MS-V3SAB-1	Main Isolation Valve - Steam Generator 1C	A&B	Close	10.1.0-1	CAR-2166-B-430SH8.10
2MS-F1SAB-1	Main Isolation Valve - Steam Generator 1A	A&B	Close	10.1.0-1	CAR-2166-B-430SH8.8
2MS-F2SAB-1	Main Isolation Valve - Steam Generator 1B	A&B	Close	10.1.0-1	CAR-2166-B-430SH8.9
2MS-F3SAB-1	Main Isolation Valve - Steam Generator 1C	A&B	Close	10.1.0-1	CAR-2166-B-430SH8.10
2MS-V59SAB-1	Main Steam Line Drain Isolation Valve Steam Generator 1A	A&B	Close	10.1.0-1	CAR-2166-B-430SH8.7
2MS-V60SAB-1	Main Steam Line Drain Isolation Valve Steam Generator 1B	A&B	Close	10.1.0-1	CAR-2166-B-430SH8.7
2MS-V61SAB-1	Main Steam Line Drain Isolation Valve Steam Generator 1C	A&B	Close	10.1.0-1	CAR-2166-B-430SH8.7

TABLE 7.3.1-11

ESF ACTUATION SYSTEMS
FEEDWATER ISOLATION SIGNAL (MFI)

EQUIPMENT IDENTIFICATION	SERVICE	ACTUATION CHANNEL	ACTION	REFERENCE FIGURE NUMBER	SCHEMATIC/LOGIC NUMBER
2FW-V26SAB-1	Feedwater Isolation Valve Steam Generator 1A	A&B	Close	10.1.0-3	CAR-2166-G-424
2FW-V27SAB-1	Feedwater Isolation Valve Steam Generator 1B	A&B	Close	10.1.0-3	CAR-2166-G-424
2FW-V28SAB-1	Feedwater Isolation Valve Steam Generator 1C	A&B	Close	10.1.0-3	CAR-2166-G-424
FCV-1FW-478SAB	Feedwater Control Valve Steam Generator 1A	A&B	Close	10.1.0-3	CAR-2166-G-424
FCV-1FW-488SAB	Feedwater Control Valve Steam Generator 1B	A&B	Close	10.1.0-3	CAR-2166-G-424
FCV-1FW-498SAB	Feedwater Control Valve Steam Generator 1C	A&B	Close	10.1.0-3	CAR-2166-G-424
FCV-1FW-479SAB	Feedwater Control Bypass Valve Steam Generator 1A	A&B	Close	10.1.0-3	CAR-2166-G-424
FCV-1FW-489SAB	Feedwater Control Bypass Valve Steam Generator 1B	A&B	Close	10.1.0-3	CAR-2166-G-424
FCV-1FW-499SAB	Feedwater Control Bypass Valve Steam Generator 1C	A&B	Close	10.1.0-3	CAR-2166-G-424
2FW-V89SAB-1	Hydrazine to Feedwater Steam Generator 1A/Disabled	M	L.C.		
2FW-V90SAB-1	Ammonia to Feedwater Steam Generator 1A/Disabled	M	L.C.		
2FW-V91SAB-1	Hydrazine to Feedwater Steam Generator 1B/Disabled	M	L.C.		
2FW-V92SAB-1	Ammonia to Feedwater Steam Generator 1B/Disabled	M	L.C.		
2FW-V93SAB-1	Hydrazine to Feedwater Steam Generator 1C/Disabled	M	L.C.		
2FW-V94SAB-1	Ammonia to Feedwater Steam Generator 1C/Disabled	M	L.C.		

TABLE 7.3.1-12

ESF AND SUPPORTING SYSTEM ACTUATION INSTRUMENTATION

System Variable	System Ranges	System Accuracies	System Response Times	System Actuation Setpoint
Pressurizer Pressure	1700 to 2500 psig	*±1.5% of span	2.0 seconds	
Containment Pressure				
- HI-1	0 to 55 psig	*±1.09% of full scale	2.0 seconds	3.0 psig
- HI-2	0 to 55 psig	*±1.09% of full scale	2.0 seconds	3.0 psig
- HI-3	0 to 55 psig	*±1.82% of full scale	2.0 seconds	10.0 psig
Steam Line Pressure	0 to 1300 psig	*±1.5% of span	2.0 seconds	601 psig
Steam Line Differential Pressure	0 to 1300 psig	*±2.11% of span	2.0 seconds	100 psi
Reactor Coolant Temperature T_{AVG}	530 to 630F	+2F	6.0 seconds	
Auxiliary Feedwater Actuation (Steam Generator Level)	0-100%	2.3% of span	2.0 seconds	
Primary Loop Flow	0-120% flow	±2.75% of span	1.0 seconds	
Feedwater Flow	0-5 MPPH	±2.52% of span	2.0 seconds	
RWST Water Level			Manual Actuation	
Containment Hydrogen	grab sample			4 v/o
Containment Radiation	See Table 12.3.4-1			
ESF Bus Primary Undervoltage	6.9 kV	±2%	1.26 Seconds**	80%
Fuel Handling Radiation			5 seconds (includes monitor, logic and dampers)	

* System Accuracy = $\frac{STS\ Trip\ Setpoint - STS\ Allowable\ Value}{Span}$

**Includes 1.2 seconds nominal time delay for associated time delay relay and 0.06 second maximum time delay of UV relay at 90% of voltage setpoint.

TABLE 7.3.2-1

ENGINEERED SAFETY FEATURES
STATUS INDICATOR LIGHTS

FUNCTION	INDICATION
Low-Low T_{avg}	A each channel T each channel P output of 2/3 logic
Pressurizer Water Level	A each channel (common window for all three) T each channel
Pressurizer Pressure	Same as pressurizer water level
P-11	T each channel; pressurizer pressure A P-11 status (converse of 2/3 high pressurizer pressure)
Pressurizer Safety Injection Block	P both trains blocked (allowed if pressurizer pressure is low)
Hi Steam Line D/P	T each of 9 channels A 3 windows, indicating P1, P2, P3 low
Hi Steam Line Pressure Rate	T each of 6 channels A annunciates high pressure rate in each of 3 steamlines
Low Steam Line Pressure	T each of 3 channels A one annunciator for all three
Steam Line Safety Injection Block	P both trains blocked (permitted by P-11)
Containment Pressure	A annunciator for Hi-1, Hi-2 and Hi-Hi containment pressure T each channel
Safety Injection Blocked	P permitted after time delay and receipt of P-4 (Reactor Trip)
Steam Line Stop Valves Closed	A common window for all three
Spray Actuation and Phase B Isol.	A window for each
Steam Generator Water Level	T each channel (Low-Low and High-High) A each generator, 2/3 logic (Low-Low), 2/4 logic (High-High)
Refueling Water Storage Tank Level	T each channel (Low-Low) A each channel, 1/4 logic (alert), 2/4 logic (actuation)
ATWS Panel Armed (C-20)	P armed when power above C-20
Containment Spray Bypassed	P each channel
Solid State Logic Protection System	A train in test (each train)
Safeguards Test Cabinet	A train in test (actuation) (each train)

Legend:

A Actuation signal lights

T Trip status lights

P Permissive status lights

TABLE 7.4.1-1 MONITORING INSTRUMENTS FOR SAFE SHUTDOWN

System Parameter	Local	Indication ACP	Indication MCB	ACP & MCB Indicator Range
Auxiliary Feedwater & Steam Relief System				
Auxiliary Feedwater Pump A Suction Pressure	PI-2251A	PI-2250A2	PI-2250A1	0-200 psig
Auxiliary Feedwater Pump B Suction Pressure	PI-2251B	PI-2250B2	PI-2250B1	0-200 psig
Auxiliary Feedwater Turbine Driven Pump Suction Pressure	PI-2271	PI-2270.2	PI-2270.1	0-200 psig
Auxiliary Feedwater Pump A Discharge Pressure	PI-2151A	PI-2150A2	PI-2150A1	0-2000 psig
Auxiliary Feedwater Pump B Discharge Pressure	PI-2151B	PI-2150B2	PI-2150B1	0-2000 psig
Auxiliary Feedwater Turbine Driven Pump Discharge Pressure	PI-2171	PI-2170.2	PI-2170.1	0-2000 psig
Auxiliary Feedwater Flow to Steam Generator 1A	-	FI-2050A2	FI-2050A1	0-266 KPPH
Auxiliary Feedwater Flow to Steam Generator 1B	-	FI-2050B2	FI-2050B1	0-266 KPPH
Auxiliary Feedwater Flow to Steam Generator 1C	-	FI-2050C2	FI-2050C1	0-266 KPPH
Auxiliary Feedwater Turbine Inlet Steam Pressure	PI-0431	PI-0430.2	PI-0430.1	0-1500 psig
Auxiliary Feedwater Turbine Inlet Pump Discharge Differential	-	PDI-2180.2	PDI-2180.1	0-100 psid
Auxiliary Feedwater Turbine Speed	SI-2180	SI-2180.2	SI-2180.1	0-6000 rpm
Condensate Storage Tank Level	LI-9011	LI-9010A2	LI-9010A1	0-100 %
Condensate Storage Tank Level	-	LI-9010B2	LI-9010B1	0-100 %
Main Steam Supply System				
Steam Generator 1A Level	LI-0477A LI-0477B	LI-0477.2	LI-0477.1	0-100%
Steam Generator 1B Level	LI-0487A LI-0487B	LI-0487.2	LI-0487.1	0-100 %
Steam Generator 1C Level	LI-0497A LI-0497B	LI-0497.2	LI-0497.1	0-100 %
Steam Generator 1A Pressure	PI-0474A	PI-0474.2	PI-0474.1	0-1300 psig
Steam Generator 1B Pressure	PI-0485A	PI-0484.2	PI-0485	0-1300 psig
Steam Generator 1C Pressure	PI-0496A	PI-0496.2	PI-0496.1	0-1300 psig
Main Steam Header Pressure	PI-0464B	PI-0464A2	PI-0464A1	0-1300 psig
Boric Acid System				
Emergency Boration Flow	FI-0110A	-	FI-0110	0-200 gpm
Make-up Water Flow	-	-	FIS-0114	0-160 gal.
Boric Acid Tank Level	-	-	LI-106	0-100%
Boric Acid Tank Level	-	LI-0161.2	LI-0161.1	0-100%

TABLE 7.4.1-1 MONITORING INSTRUMENTS FOR SAFE SHUTDOWN

System Parameter	Local	Indication ACP	Indication MCB	ACP & MCB Indicator Range
Chemical and Volume Control System (CVCS)				
Volume Control Tank Pressure	-	PI-0117.2	PI-0117.1	30 Hg-vac.100 psig
Volume Control Tank Temperature	-	TI-0116.2	TI-0116.1	50-300 F
Charging Header Flow	FI-0122B	FI-0122A2	FI-0122A1	0-150 gpm
Chemical and Volume Control System (CVCS)				
CHRG SI Pump A Current	-	-	EI-0221	0-100 amps
CHRG SI Pump B Current	-	-	EI-0222	0-100 amps
CHRG SI Pump C Current Train A	-	-	EI-0223	0-100 amps
CHRG SI Pump C Current Train B	-	-	EI-0224	0-100 amps
RCP 1A Seal Water Injection Flow	FI-0130B	-	FI-0130A	0-20 gpm
RCP 1B Seal Water Injection Flow	FI-0127B	-	FI-0127A	0-20 gpm
RCP 1C Seal Water Injection Flow	FI-0124B	-	FI-0124A	0-20 gpm
RCP 1A Seal Differential Pressure	PI-0156B	PI-0156A2	PI-0156A1	0-400 psid
RCP 1B Seal Differential Pressure	PI-0155B	PI-0155A2	PI-0155A1	0-400 psid
RCP 1C Seal Differential Pressure	PI-0154B	PI-0154A2	PI-0154A1	0-400 psid
Reactor Coolant System (RCS)				
RCS Hot Leg Temperature Loop 1	-	TI-0413.2	TI-0413.1	0-700 F
RCS Hot Leg Temperature Loop 2	-	TI-0423.2	TI-0423.1	0-700 F
RCS Cold Leg Temperature Loop 1	-	TI-0410.2	TI-0410.1	0-700 F
RCS Cold Leg Temperature Loop 2	-	TI-0420.2	TI-0420.1	0-700 F
RCS Pressure	PI-404	PI-0402.2	PI-0402.1	0-3000 psig
	PI-405	PI-0403.2	PI-0403.1	0-3000 psig
Pressurizer Level		LI-0459A2	LI-0459A1	0-100%
			LI-0460	0-100%
		LI-0461.2	LI-0461.1	0-100%
Pressurizer Pressure		-	PI-0444	1700-2500 psig
		PI-0445.2	PI-0445.1	1700-2500 psig
		PI-0455.2	PI-0455.1	1700-2500 psig
		-	PI-0456	1700-2500 psig
		-	PI-0457	1700-2500-pisg
Pressurizer Vapor Temperature	-	TI-0454.2	TI-0454.1	100-700F
Pressurizer Relief Tank Pressure	-	PI-0472.2	PI-0472.1	0-120 psig
Pressurizer Relief Tank Temperature	-	TI-0471.2	TI-0471.1	50-350 F
Pressurizer Relief Tank Level	-	LI-0470.2	LI-0470.1	0-100 %
Pressurizer Liquid Temperature	-	TI-0453.2	TI-0453.1	100-700 F
RCP 1A Ammeter			EI-160	0-800 Amps
RCP 1B Ammeter			EI-161	0-800 Amps

TABLE 7.4.1-1 MONITORING INSTRUMENTS FOR SAFE SHUTDOWN

System Parameter	Local	Indication ACP	Indication MCB	ACP & MCB Indicator Range
RCP 1C Ammeter			EI-162	0-800 Amps
Residual Heat Removal System (RHRS)				
RHR Heat Exchanger 1A Flow	-	FI-0605A2	FI-0605A1	0-5000 gpm
RHR Heat Exchanger 1B Flow	-	FI-0605B2	FI-0605B1	0-5000 gpm
RHR Pump 1A Motor Ammeter	-	-	EI-0610A1	0-600 amp
RHR Pump 1B Motor Ammeter	-	-	EI-0610B1	0-600 amp
RHR Pump 1A Discharge Pressure	PI-5451A	-	PI-0600A	0-700 psig
Residual Heat Removal System (RHRS)				
RHR Pump 1B Discharge Pressure	PI-5451B	-	PI-0600B	0-700 psig
Component Cooling Water System (CCWS)				
Component Cooling Surge Tank Level	LI-0670B	LI-0670A2	LI-0670A1	0-100 %
	LI-0676B	LI-0676A2	LI-0676A1	0-100 %
CCW Heat Exchanger 1A Outlet Temperature	-	TI-0674.2	TI-0674.1	0-200 F
CCW Heat Exchanger 1B Outlet Temperature	-	TI-0675.2	TI-0675.1	0-200 F
CCW Heat Exchanger 1A Discharge Pressure	-	-	PI-0649	0-200 psig
CCW Heat Exchanger 1B Discharge Pressure	-	-	PI-0650	0-200 psig
CCW Heat Exchanger 1A Outlet Flow	-	FI-0652.2	FI-0652.1	0-15000 gpm
CCW Heat Exchanger 1B Outlet Flow	-	FI-0653.2	FI-0653.1	0-15000 gpm
Residual Heat Exchanger 1A Outlet Flow	FI-0688B	FI-0688A2	FI-0688A1	0-9000 gpm
Residual Heat Exchanger 1B Outlet Flow	FI-0689B	FI-0689A2	FI-0689A1	0-9000 gpm
Service Water System (SWS)				
Normal SW Pumps Chamber Level	-	-	LI-9300.1	0-100 %
SW Header A Flow	-	FI-9101A2	FI-9101A1	0-25000 gpm
SW Header B Flow	-	FI-9101B2	FI-9101B1	0-25000 gpm
Emergency SW Pump 1A Discharge Pressure	PI-9102A	PI-9101A2	PI-9101A1	0-200 psig
Emergency SW Pump 1B Discharge Pressure	PI-9102B	PI-9101B2	PI-9101B1	0-200 psig
SW To Turbine Building	-	FI-9301.2	FI-9301.1	0-13500 gpm
Normal SW Pumps Discharge Header Pressure	PI-9301A	PI-9302.2	PI-9302.1	0-150 psig
	PI-9301B			
Electrical				
Emergency Bus 1A-SA, V	-	EI-6956A2	EI-6956A1	0-9000 V
Emergency Bus 1B-SB, V	-	EI-6956B2	EI-6956B1	0-9000 V
Standby Diesel Generator 1A-SA, MW	-	EI-6957A2	EI-6957A1	0-9.6 Mw
Standby Diesel Generator 1B-SB, MW	-	EI-6957B2	EI-6957B1	0-9.6 Mw
Battery 1A-SA, V	-	EI-6961A2	EI-6961A1	0-150 V

TABLE 7.4.1-1 MONITORING INSTRUMENTS FOR SAFE SHUTDOWN

System Parameter	Local	Indication ACP	Indication MCB	ACP & MCB Indicator Range
Battery 1B-SB, V	-	EI-6961B2	EI-6961B1	0-150 V
Auxiliary Bus 1A, V	-	-	EI-560	0-9000 V
Auxiliary Bus 1B, V	-	-	EI-563	0-9000 V
Auxiliary Bus 1C, V	-	-	EI-562	0-9000 V
Auxiliary Bus 1D, V	-	-	EI-561	0-9000 V
Auxiliary Bus 1E, V	-	-	EI-564	0-9000 V
Battery A1 amp	-	EI-6963A2	EI-6963A1	± 600 amp
Battery B1 amp	-	EI-6963B2	EI-6963B1	± 600 amp
Diesel Generator				
Diesel Generator Day Tank 1A-SA	LI-2461A1	-	LI-2461A	0-100%
Diesel Generator Day Tank 1B-SB	LI-2461B1	-	LI-2461B	0-100%
Nuclear Instrumentation				
Source Range Readout	-	-	NI-31B	10^{0}-10^{6} cps
		-	NI-31D	-.5 - +5 dpm
		-	NI-32B	10^{0}-10^{6} cps
		-	NI-32D	-.5 - +5 dpm
Intermediate Range	-	-	NI-35B	10^{-11}-10^{3} amps
	-	-	NI-35D	-.5 - +5 dpm
			NI-36B	10^{-11}-10^{3} amps
			NI-36D	-.5 - +5 dpm
Source Range IE Readout		NI-60A2	NI-60A1	10^{-1}-10^{6} cps
		NI-60B2	NI-60B1	10^{-3}-200 pcnt
		-	NI-61A	10^{-1}-10^{6} cps
		-	NI-61B	10^{-3}-200 pcnt

TABLE 7.4.1-2 INSTRUMENTATION AND CONTROL AUXILIARY CONTROL PANEL (ACP)

Service	Instrument Tag No.	Safety Train	Range
INDICATORS			
SERVICE WATER SYSTEM (SW)			
SW Flow to Turbine Building	FI-9301.2	Non-Safety	0-13500 gpm
SW Pumps Discharge Header Pressure	PI-9302.2	Non-Safety	0-150 psig
SW Header A Flow	FI-9101A2	SA	0-25000 gpm
SW Header B Flow	FI-9101B2	SB	0-25000 gpm
Emergency SW Pump Discharge Header A Pressure	PI-9101A2	SA	0-200 psig
Emergency SW Pump Discharge Header B Pressure	PI-9101B2	SB	0-200 psig
COMPONENT COOLING WATER SYSTEM (CCW)			
CCW Heat Exchanger 1A Outlet Flow	FI-0652.2	Non-Safety	0-15000 gpm
CCW Heat Exchanger 1B Outlet Flow	FI-0653.2	Non-Safety	0-15000 gpm
CCW Surge Tank Level	LI-0670A2	SA	0-100 %
CCW Surge Tank Level	LI-0676A2	SB	0-100 %
CCW Heat Exchanger 1A Outlet Temperature	TI-0674.2	SA	0-200 F
CCW Heat Exchanger 1B Outlet Temperature	TI-0675.2	SB	0-200 F
Residual Heat Exchanger 1A Outlet Flow	FI-0688A2	Non-Safety	0-7000 gpm
Residual Heat Exchanger 1B Outlet Flow	FI-0689A2	Non-Safety	0-7000 gpm
RESIDUAL HEAT REMOVAL SYSTEM (RHR)			
Residual Heat Exchanger 1A Flow	FI-0605A2	Non-Safety	0-5000 gpm
Residual Heat Exchanger 1B Flow	FI-0605B2	Non-Safety	0-5000 gpm
INSTRUMENT AIR SYSTEM			
Instrument Air Pressure	PI-9751.2	Non-Safety	0-150 psig
CHEMICAL AND VOLUME CONTROL SYSTEM (CVCS)			
Letdown Heat Exchanger Outlet Temperature	TI-0144.2	Non-Safety	50-200°F
Letdown Heat Exchanger Flow	FI-0150.2	Non-Safety	0-200 gpm
Letdown Heat Exchanger Pressure	PI-0145.2	Non-Safety	0-600 psig
Volume Control Tank Level	LI-0115.2	Non-Safety	0-100%
Volume Control Tank Temperature	TI-0116.2	Non-Safety	50-300°F
Volume Control Tank Pressure	PI-0117.2	Non-Safety	-30"Hg-100 psig
Charging Header Flow	FI-0122A2	Non-Safety	0-150 gpm
Regenerative Heat Exchanger Letdown Temperature	TI-0140.2	Non-Safety	100-600°F
RCP 1 Seal 1 Pressure	PI-0156A2	Non-Safety	0-400 psid
RCP 2 Seal 1 Pressure	PI-0155A2	Non-Safety	0-400 psid
RCP 3 Seal 1 Pressure	PI-0154A2	Non-Safety	0-400 psid
Boric Acid Tank Level	LI-0161.2	SB	0-100%
REACTOR COOLANT SYSTEM (RCS)			
RC Loop 1 Cold Leg Temperature	TI-0410.2	SB	0-700°F
RC Loop 1 Hot Leg Temperature	TI-0413.2	SA	0-700°F
RC Loop 2 Cold Leg Temperature	TI-0420.2	SB	0-700°F
RC Loop 2 Hot Leg Temperature	TI-0423.2	SA	0-700°F
Pressurizer Relief Tank Temperature	TI-0471.2	Non-Safety	50-350°F
RCS Wide Range Pressure	PI-0402.2	SA	0-3000 psig
RCS Wide Range Pressure	PI-0403.2	SB	0-3000 psig
Pressurizer Relief Tank Level	LI-0470.2	Non-Safety	1-100%
Pressurizer Relief Tank Pressure	PI-0472.2	Non-Safety	0-120 psig
Pressurizer Pressure	PI-0445.2	Non-Safety	1700-2500 psig
Pressurizer Pressure	PI-0455.2	Non-Safety	1700-2500 psig
Pressurizer Surge Line Temperature	TI-0450.2	Non-Safety	100-700°F
Pressurizer Liquid Temperature	TI-0453.2	Non-Safety	100-700°F

TABLE 7.4.1-2 INSTRUMENTATION AND CONTROL AUXILIARY CONTROL PANEL (ACP)

Service	Instrument Tag No.	Safety Train	Range
Pressurizer Vapor Temperature	TI-0454.2	Non-Safety	100-700°F
REACTOR COOLANT SYSTEM (RCS) (Cont'd)			
Pressurizer Water Level	LI-0459A2	SA	0-100%
Pressurizer Water Level	LI-0461.2	SA	0-100%
Spray Line Temperature RC Loop 1	TI-0451.2	Non-Safety	100-700°F
Spray Line Temperature RC Loop 2	TI-0452.2	Non-Safety	100-700°F
MAIN STEAM SYSTEM			
Steam Generator 1A Pressure (Loop 1)	PI-0474.2	SB	0-1300 psig
Steam Generator 1B Pressure (Loop 2)	PI-0484.2	SB	0-1300 psig
Steam Generator 1C Pressure (Loop 3)	PI-0496.2	SB	0-1300 psig
Steam Generator 1A Wide Range Level	LI-0477.2	SA	0-100%
Steam Generator 1B Wide Range Level	LI-0487.2	SB	0-100%
Steam Generator 1C Wide Range Level	LI-0497.2	SA	0-100%
Steam Header Pressure	PI-0464A2	Non-Safety	0-1300 psig
AUXILIARY FEEDWATER SYSTEM			
Auxiliary Feedwater Pump A Suction Pressure	PI-2250A2	SA	0-200 psig
Auxiliary Feedwater Pump B Suction Pressure	PI-2250B2	SB	0-200 psig
Auxiliary Feedwater Turbine Driven Pump Suction Pressure	PI-2270.2	SB	0-200 psig
Auxiliary Feedwater Turbine Steam Pressure	PI-0430.2	SB	0-1500 psig
Auxiliary Feedwater Pump A Discharge Pressure	PI-2150A2	SA	2000 psig
Auxiliary Feedwater Pump B Discharge Pressure	PI-2150B2	SB	2000 psig
Auxiliary Feedwater Turbine Drive Pump Discharge Pressure	PI-2170.2	SB	2000 psig
Auxiliary Feedwater Turbine Pump Differential Pressure	PDI-2180.2	SB	0-100 psid
Auxiliary Feedwater Flow to Steam Generator 1A	FI-2050A2	SA	0-266 kpph
Auxiliary Feedwater Flow to Steam Generator 1B	FI-2050B2	SB	0-266 kpph
Auxiliary Feedwater Flow to SteamGenerator 1C	FI-2050C2	SA	0-266 kpph
Auxiliary Feedwater Turbine Speed	SI-2180.2	SB	0-6000 rpm
Condensate Storage Tank Level	LI-9010A2	SA	0-100 %
Condensate Storage Tank Level	LI-9010B2	SB	0-100 %
ELECTRICAL SYSTEM			
Emergency Bus 1A-SA Voltage	EI-6956A2	SA	0-9 kv
Emergency Bus 1B-SB, Voltage	EI-6956B2	SB	0-9 kv
Emergency Diesel Generator 1A-SA, MW	EI-6957A2	SA	0-9.6 Mw
Emergency Diesel Generator 1B-SB, MW	EI-6957B2	SB	0-9.6 Mw
Battery 1A-SA Voltage	EI-6961A2	SA	0-150 V
Battery 1B-SB Voltage	EI-6961B2	SB	0-150 V
Battery 1A-SA amp	EI-6963A2	SA	±600 amp
Battery 1B-SB amp	EI-6963B2	SB	±600 amp
NUCLEAR INSTRUMENTATION SYSTEM			
Source Range	NI-60A2	SA	10^{-1} – 10^{6} cps
	NI-60B2	SA	10^{-3} – 200 pcnt
CONTAINMENT SPRAY SYSTEM			
Refueling Water Storage Tank Level	LI-7110	Non-safety	0-100 pcnt
HVAC SYSTEM			
Control Room to Outside Differential Pressure	PDI-7838A2	SA	0-1 in. wc.
Control Room Temperature	TI-7837A2	SA	0-100 F

TABLE 7.4.1-2 INSTRUMENTATION AND CONTROL AUXILIARY CONTROL PANEL (ACP)

Service	Instrument Tag No.	Safety Train	Range
Control Room AH-15 (1A-SA) Electric Heating Coil Outlet Temperature	TI-7835A2	SA	0-100 F
Control Room Temperature	TI-7837B2	SB	0-100 F
Control Room AH-15 (1B-SB) Electric Heating Coil Outlet Temperature	TI-7835B2	SB	0-100 F
Control Room to Outside Differential Pressure	PDI-7838B2	SB	0-1 in. wc.
INDICATING LIGHTS			
Reactor Support Cooling Fan S-4 (1A-SA)	2681.2	SA	-
Primary Shield Cooling Fan S-2 (1A-SA)	2665.2	SA	-
Reactor Support Cooling Fan S-4 (1B-SB)	2682.2	SB	-
Primary Shield Cooling Fan S-2 (1B-SB)	2666.2	SB	-
Normal SW Pump A Discharge Valve	2185.2	Non-Safety	-
Normal SW Pump B Discharge Valve	2186.2	Non-Safety	-
SW Booster Pump A	2233.2	SA	-
SW HDR A Return to Aux. Res. 3SW-B15SA	2286.2	SA	-
SW Booster B	2234.2	SB	-
SW HDR B Return to Aux. Res. 3SW-B16SB	2287.2	SB	-
Emergency SW Intake Valves Auxiliary Reservoir 3SW-B1-SA and Main Reservoir 3SW-B3-SA	2217.2	SA	-
Emergency SW Intake Valves Auxiliary Reservoir 3SW-B2-SB and Main Reservoir 3SW-B4-SB	2218.2	SB	-
Pressurizer Spray Valve IRC-P525SN and IRC - P526SN	159.3	Non-Safety	-
Start up Transformer 1A-Y Breaker - 101	1659.2	Non-Safety	-
Start up Transformer 1B-Y Breaker - 121	1660.2	Non-Safety	-
Emergency Diesel Generator 1A-SA, Breaker-106 Status	1702.2	SA	-
Emergency Diesel Generator 1B-SB, Breaker-126 Status	1750.2	SB	-
Aux Bus ID to Emergency Bus 1A-SA, Breaker-105 Status	1727.2	SA	-
Aux Bus IE to Emergency Bus 1B-SB, Breaker-125 Status	1752.2	SB	-
Aux Bus ID to Emergency Bus 1A-SA, Breaker-104 Status	1633.2	Non Safety	-
Aux Bus IE to Emergency Bus 1B-SB, Breaker-124 Status	1634.2	Non Safety	-
SW Return Headers A Isolation Valve 3-SW-B13-SB	2280.2	SB	-
SW Common Return Headers Isolation Valve 3-SW-B8-SA	2284.2	SA	-
SW Return Header B Isolation Valve 3-SW-B14-SB	2282.2	SB	-
SW Header A Inlet Isolation Valve 3-SW-B5-SA	2207.2	SA	-
SW Header B Inlet Isolation Valve 3-SW-B6-SB	2208.2	SB	-
Main Steam Power Operated Relief Valves PCV-308A-SA, PCV-308B-SB, and PCV-308C-SA	1254.2	SA	-
Auxiliary Feedwater Pump 1A-SA Discharge Valve PCV-2150A-SA	1941.2	SA	-
Auxiliary Feedwater Pump 1B-SB Discharge Valve PCV-2150B-SB	1942.2	SB	-
Auxiliary Feedwater Motor Pump Regulator Valves FCV-2051A- SA FCV-2051B- SA FCV-2051C-SA	1944.2	SA	-
Auxiliary Feedwater Turbine Pump Regulator Valves FCV-2071A-SB FCV-2071B-SB FCV-2071C-SB	1950.2	SB	-
CONTROLLERS			

TABLE 7.4.1-2 INSTRUMENTATION AND CONTROL AUXILIARY CONTROL PANEL (ACP)

Service	Instrument Tag No.	Safety Train	Range
RESIDUAL HEAT REMOVAL SYSTEM (RHRS)			
Residual Heat Exchanger 1A Bypass Auto/Manual Station	FK-0605A2	Non-Safety	0-100 pct
RHR Letdown Manual Station	HC-0142.2	Non-Safety	0-100 pct
Residual Heat Exchanger 1B Bypass Auto/Manual Station	FK-0605B2	Non-Safety	0-100 pct
Residual Heat Exchanger 1A Outlet Manual Station	HC-0603A2	Non-Safety	0-100 pct
Residual Heat Exchanger 1B Outlet Manual Station	HC-0603B2	Non-Safety	0-100 pct
CHEMICAL AND VOLUME CONTROL (CVCS)			
Seal Water Flow Manual Station	HC-0186.2	Non-Safety	0-100 pct
Charging Header Flow Auto/Manual Station	FK-0122.2	Non-Safety	0-100 pct
Demineralizer Inlet Temperature Auto/Manual Station	TK-0381A2	Non-Safety	0-100 pct
Letdown Low Pressure Auto/Manual Station	PK-0145.2	Non-Safety	0-100 pct
PRESSURIZER			
Pressurizer Spray Auto/Manual Station	PK-0444C2	Non-Safety	0-100 pct
Pressurizer Pressure Master Control Auto/Manual Station	PK-0444A2	Non-Safety	0-100 pct
Pressurizer Spray Auto/Manual Station	PK-0444D2	Non-Safety	0-100 pct
Pressurizer Level Control Auto/Manual Station	LK-0459F2	Non-Safety	0-100 pct
MAIN STEAM SYSTEM			
Steam Header Pressure Auto/Manual Station	PK-0464.2	Non-Safety	0-100 pct
Steam Power Operated Relief Valve Auto/Manual Station	PK-0308A2	SA	0-100 pct
Steam Power Operated Relief Valve Auto/Manual Station	PK-0308B2	SB	0-100 pct
Steam Power Operated Relief Valve Auto/Manual Station	PK-0308C2	SA	0-100 pct
Feedwater Bypass Manual Station	FK-0479.2	Non-Safety	0-100 pct
Feedwater Bypass Manual Station	FK-0489.2	Non-Safety	0-100 pct
Feedwater Bypass Manual Station	FK-0499.2	Non-Safety	0-100 pct
AUXILIARY FEEDWATER SYSTEM			
Auxiliary Feedwater Turbine Driven Pump to Steam Generator A	FK-2071A2	SB	0-100 pct
Auxiliary Feedwater Turbine Driven Pump to Steam Generator B	FK-2071B2	SB	0-100 pct
Auxiliary Feedwater Turbine Driven Pump to Steam Generator C	FK-2071C2	SB	0-100 pct
Auxiliary Feedwater Turbine Control Auto/Manual Station	PDK-2180.2	SB	0-100 pct
Auxiliary Feedwater Motor Driven Pumps to Steam Generator A Valve	FK-2051A2	SA	0-100 pct
Auxiliary Feedwater Motor Driven Pumps to Steam Generator B Valve	FK-2051B2	SA	0-100 pct
Auxiliary Feedwater Motor Driven Pumps to Steam Generator C Valve	FK-2051C2	SA	0-100 pct
CONTROL SWITCHES			
SERVICE WATER SYSTEM (SW)			
Normal SW Pump 1A-NNS	2181.2	Non-Safety	-
Normal SW Pump 1B-NNS	2182.2	Non-Safety	-
Emergency SW Pump 1A-SA	2211.2	SA	-
Emergency SW Pump 1B-SB	2212.2	SB	-
COMPONENT COOLING WATER (CCW)			
CCW Pump 1A-SA	941.2	SA	-
CCW Pump 1B-SB	942.2	SB	-

TABLE 7.4.1-2 INSTRUMENTATION AND CONTROL AUXILIARY CONTROL PANEL (ACP)

Service	Instrument Tag No.	Safety Train	Range
CCW Pump 1C-SAB	943.2	SA	-
CCW Pump 1C-SAB	944.2	SB	-
RESIDUAL HEAT REMOVAL SYSTEM (RHRS)			
RHR Pump 1A-SA Minimum Flow Valve (FCV-602-A) 2RH-F511SA	323.2	SA	-
RHR Pump 1B-SB Minimum Flow Valve (FCV-602-B) 2RH-F510SB	324.2	SB	-
RHR to CVCS Charging Pumps Suction Valve 2RH-V507SA	329.2	SA	-
RHR to CVCS Charging Pumps Suction Valve 2RH-V506SB	330.2	SB	-
RHR Pump 1A-SA	321.2	SA	-
RHR Pump 1B-SB	322.2	SB	-
RHR Loop 1 Supply from RCS Loop 1 Isolation Valve 1RH-V503SA	325.2	SA	-
RHR Loop 3 Supply from RCS Loop 3 Isolation Valve 1RH-V501SA	326.2	SA	-
RESIDUAL HEAT REMOVAL SYSTEM (RHRS) (Cont'd)			
RHR Loop 1 Supply from RCS Loop 1 Isolation Valve 1RH-V502SB	327.2	SB	-
RHR Loop 3 Supply from RCS Loop 3 Isolation Valve 1RH-V500SB	328.2	SB	-
SAFETY INJECTION SYSTEM (SIS)			
RHR Loop 1 Low Head Injection to Cold Legs Valve 2SI-V579SA	444.2, 457.2(*)	SA	-
RHR Loop 2 Low Head Injection to Cold Legs Valve 2SI-V578SB	445.2, 457.4(*)	SB	-
CHEMICAL AND VOLUME CONTROL SYSTEM (CVCS)			
Letdown Line Supply Isolation Valve LCV-459	250.2	Non-Safety	-
Letdown Line Supply Isolation Valve LCV-460	251.2	Non-Safety	-
Boric Acid Tank to Charging Pump Valve 2CS-V586SB	268.2	SB	-
RCS Normal Charging Line Valve 2CS-V502SN	282.2	Non-Safety	-
RCS Alternate Charging Line Valve 2CS V503SN	283.2	Non-Safety	-

(*Switch 444.2 and 445.2 has "grey and white striped tee" handle.)

Letdown Orifice Isolation Valve 2CS-V511SA	284.2	SA	-
Charging Safety Injection Pump 1A-SA	221.2	SA	-
Charging Safety Injection Pump 1B-SB	222.2	SB	-
Boric Acid Transfer Pump 1A-SA	229.2	SA	-
Letdown Orifice Isolation Valve 2CS-V512SA	285.2	SA	-
Charging Safety Injection Pump 1C-SAB	223.2	SA	-
Charging Safety Injection Pump 1C-SAB	224.2	SB	-
Boric Acid Transfer Pump 1B-SB	230.2	SB	-
Letdown Orifice Isolation Valve 2CS-V513SA	286.2	SA	-
Letdown to Demineralizer or Volume Control Tank 2CS-M510SN	246.2	Non-Safety	-
PRESSURIZER			
Pressurizer Heater Back-up Group A	152.2	Non-Safety	-
Pressurizer Heater Back-up Group B	153.2	Non-Safety	-

TABLE 7.4.1-2 INSTRUMENTATION AND CONTROL AUXILIARY CONTROL PANEL (ACP)

Service	Instrument Tag No.	Safety Train	Range
Pressurizer Power Relief Valve (PCV-445-A) 1RC-P527SA	157.2	SA	-
Pressurizer Power Relief Valve (PCV-445-B) 1RC-P528SN	158.2	Non-Safety	-
Pressurizer Power Relief Valve (PCV-445-B) 1RC-P529SB	156.2	SB	-
Pressurizer Power Relief Isolation Valve (8000 A) 2RC-V526SN	160.2	Non-Safety	-
Pressurizer Power Relief Isolation Valve (8000 B) 2RC-V527SN	161.2	Non-Safety	-
Pressurizer Power Relief Isolation Valve (8000 C) 2RC-V528SN	162.2	Non-Safety	-
Pressurizer Relief Tank Nitrogen Supply Isolation Valve (8047) 2RC-D528SA	170.2	SA	-
Pressurizer Relief Tank Nitrogen Supply Isolation Valve (8033) 2RC-D529SB	169.2	SB	-
Pressurizer Relief Tank Primary Water Supply Isolation Valve (8028) 2RC-D528SB	165.2	SB	-
Pressurizer Relief Tank Primary Water Supply Isolation Valve (8030) 5RC-D526	166.2	Non-Safety	-
MAIN STEAM			
Main Steam Isolation Valve 2-MS-V1-SAB	1001.2	SA/SB	-
Main Steam Isolation Valve 2-MS-V2-SAB	1003.2	SA/SB	-
Main Steam Isolation Valve 2-MS-V3-SAB	1005.2	SA/SB	-
Steam Dump Interlock	854.2	SA	-
Steam Dump Mode Selector	853.2	Non-Safety	-
Steam Dump Interlock	855.2	SB	
Main Steam Power Operated Relief Valve 2MS-P20-SA-1 Alternate Servo Control Power Switch	1256.2		
AUXILIARY FEEDWATER SYSTEM			
Auxiliary Feedwater Turbine Driven Pump Steam Isolation Valve B 2MS-V8SA	1975.2	SA	-
Auxiliary Feedwater Turbine Driven Pump Steam Isolation Valve C 2MS-V9SB	1974.2	SB	-
Auxiliary Feedwater Turbine Stop Valve	1976.2	SB	-
Turbine Driven Auxiliary Feedwater Pump Isolation Valve A 2AF-V116SA	1933.2	SA	-
Turbine Driven Auxiliary Feedwater Pump Isolation Valve B 2AF-V117SA	1934.2	SA	-
Motor Driven Auxiliary Feedwater Pump Isolation Valve A 2AF-V10SB	1930.2	SB	-
Auxiliary Feedwater Motor Driven Pump Isolation Valve B 2AF-V195SB	1931.2	SB	-
Auxiliary Feedwater Motor Driven Pump A	1921.2	SA	-
Turbine Driven Auxiliary Feedwater Pump Isolation Valve C 2AF-V118SA	1935.2	SA	-
Auxiliary Feedwater Motor Driven Pump B	1922.2	SB	-
Motor Driven Auxiliary Feedwater Pump Isolation Valve C 2AF-V23SB	1932.2	SB	-
SW to Auxiliary Feedwater Pump 1A-SA Supply Valve 3 SW-B74SA	2262.2	SA	-

TABLE 7.4.1-2 INSTRUMENTATION AND CONTROL AUXILIARY CONTROL PANEL (ACP)

Service	Instrument Tag No.	Safety Train	Range
SW to Auxiliary Feedwater Pump 1A-SA Supply Valve 3 SW-B75SA	2261.2	SA	-
SW to Auxiliary Feedwater Pump 1B-SB Supply Valve 3 SW-B76SB	2264.2	SB	-
SW to Auxiliary Feedwater Pump 1B-SB Supply Valve 3 SW-B77SB	2263.2	SB	-
A Hdr SW to Turb. Driven Auxiliary Feedwater Pump 1X-SAB Supply Valve 3 SW-B70SA	2257.2	SA	-
A Hdr SW to Turb. Driven Auxiliary Feedwater Pump 1X-SAB Supply Valve 3 SW-B71SA	2258.2	SA	-
B Hdr SW to Turbine Driven Auxiliary Feedwater Pump 1X-SAB Supply Valve 3 SW-B72SB	2260.2	SB	
B Hdr SW to Auxiliary Feedwater Pump 1X-SAB Supply Valve 3 SW-B73SB	2259.2	SB	-
CONTROL SWITCHES:			
ELECTRICAL SYSTEM			
Emergency Diesel Generator 1A-SA, Stop	1988.3	SA	-
Emergency Diesel Generator 1B-SB, Stop	2008.3	SB	-
Emergency Bus 1A-SA, Voltmeter Phase Selector	1729.2	SA	-
Emergency Bus 1B-SB, Voltmeter Phase Selector	1730.2	SB	-
Service Transformer 1A1 BKR 1A1A-SA	1741.2	SA	-
Service Transformer 1B1 BKR 1B1A-SB	1745.2	SB	-
HVAC SYSTEMS			-
Control Room Recirculation System Damper CZ D69SA-1	2960.2	SA	-
Control Room Air Exhaust Valve 3CZ-B3SA-1	2958.2	SA	-
Containment Fan Cooler AH-2 (1A-SA)	2673.2	SA	-
Containment Fan Cooler AH-2 (1A-SA) Trip	2673.4	SA	-
Control Room Recirculation System Damper CZ D70SB-1	2961.2	SB	-
Control Room Air Exhaust Valve 3CZ-B4SB-1	2957.2	SB	-
SW from WC-2 (1A-SA) 3 SW-B300SA	2612.2	SA	-
Chiller WC-2 (1A-SA)	2601.2	SA	-
SW from WC-2 (1B-SB) 3 SW-B303SB	2642.2	SB	-
Chiller WC-2 (1B-SB)	2631.2	SB	-
Containment Fan Cooler AH-1 (1A-SB)	2669.2	SB	-
Containment Fan Cooler AH-1 Trip (1A-SB)	2669.4	SB	-
Control Room Purge Make Up Valve 3CZ-B17SA-1	2964.2	SA	-
Control Room Supply Fan AH-15 (1A-SA)	2946.2	SA	-
Containment Fan Cooler AH-2 (1B-SA)	2675.2	SA	-
Containment Fan Cooler AH-2 Trip (1B-SA)	2675.4	SA	-
Control Room Purge Make-Up Valve 3CZ-B18SB-1	2965.2	SB	-
Control Room Supply Fan AH-15 (1B-SB)	2947.2	SB	-
Containment Fan Cooler AH-1 (1B-SB)	2671.2	SB	-
Containment Fan Cooler AH-1 Trip (1B-SB)	2671.4	SB	-
Control Room Purge Exhaust Valve 3CZ-B13SA-1	2967.2	SA	-
Control Room Air Inlet Valve 3CZ-B1SA-1	2942.2	SA	-
Containment Fan Cooler AH-3 (1A-SA)	2741.2	SA	-
Containment Fan Cooler AH-3 (1A-SA) Trip	2741.4	SA	-
Control Room Purge Exhaust Valve 3CZ-B14SB-1	2968.2	SB	-
Control Room Air Inlet Valve 3CZ-B2SB-1	2943.2	SB	-
Containment Fan Cooler AH-4 (1A-SB)	2745.2	SB	-

TABLE 7.4.1-2 INSTRUMENTATION AND CONTROL AUXILIARY CONTROL PANEL (ACP)

Service	Instrument Tag No.	Safety Train	Range
Containment Fan Cooler AH-4 (1A-SB) Trip	2745.4	SB	-
Containment Fan Cooler AH-3 (1B-SA)	2743.2	SA	-
Containment Fan Cooler AH-3 (1B-SA) Trip	2743.4	SA	-
Containment Fan Cooler AH-4 (1B-SB)	2747.2	SB	-
Containment Fan Cooler AH-4 (1B-SB) Trip	2747.4	SB	-
Chilled Water Pump P4 (1A-SA)	2604.2	SA	-
Chilled Water Pump P4 (1B-SB)	2634.2	SB	-
CRDM Cooling Fan E-80 (1A-NNS)	472.2	Non-Safety	-
CRDM Cooling Fan E-80 (1B-NNS)	473.2	Non-Safety	-
CRDM Cooling Fan E-81 (1A-NNS)	474.2	Non-Safety	-
CRDM Cooling Fan E-81 (1B-NNS)	475.5	Non-Safety	-
Control Room Exhaust Fan E-9 (1A-NNS)	2955.2	Non-Safety	-
Control Room Purge Exhaust Fan ES-1 (1A-NNS)	2969.2	Non-Safety	-
Control Room Exhaust Fan E-9 (1B-NNS)	2956.2	Non-Safety	-
Control Room Purge Exhaust Fan ES-1 (1B-NNS)	2970.2	Non-Safety	-
AUXILIARY INDICATION			
Transfer Status - SA	1081	SA	-
Transfer Status - NNS A	1083	Non-Safety	-
Transfer Status - SB	1084	SB	-
Transfer Status - NNS B	1086	Non-Safety	-
AUXILIARY SWITCHES			
SIR A2 Safety Injection Reset	455.2	SA	-
SIR B2 Safety Injection Reset	455.4	SB	-
Annunciator Switch	-	Non-Safety	-
Pressurizer Pressure SI Block/Reset	141.2	SA	-
Pressurizer Pressure SI Block/Reset	141.4	SB	-
Main Steam Pressure SI Block/Reset	1008.2	SA	-
Main Steam Pressure SI Block/Reset	1008.4	SB	-

TABLE 7.5.1-1

CONTROL ROOM INDICATORS AND/OR RECORDS AVAILABLE TO THE OPERATOR
TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS

CONTAINMENT SPRAY AND CONTAINMENT COOLING SYSTEM

				Instrument		Required for					
Monitored Parameter	Function	Inst Tag. No.	Train	Range	ESF	ESF Support	PPDI	PAMI	Location	CWD	Note
CS Additive Tank Level	Indication	LI-7150	SA	0-100%	X		X	X	MCB	1043	
CS Additive Tank Level	Indication	LI-7166	SB	0-100%	X		X	X	MCB	1043	
CS Pump A Disch Press.	Indication	PI-7131A	SA	0-400 psig	X			X	MCB	1041	
CS Pump B Disch. Press.	Indication	PI-7131B	SB	0-400 psig	X			X	MCB	1042	
Cont Sump A Level	Indication	LI-7160A	SA	0-100%	X		X	X	MCB	1041	
Cont Sump B Level	Indication	LI-7160B	SB	0-100%	X		X	X	MCB	1042	
Cont Temp	Indication	TI-7541	SB	0-400°F	X		X		MCB	3062	
	Recording	TR-1AV-0005 (PT-22)	NNS	0-400°F					AEP-2		
Cont Temp	Indication	TI-7542	SA	0-400°F	X		X		MCB	3061	
	Recording	TR-1AV-0005 (PT-23)	NNS	0-400°F					AEP-2		
Cont WR Sump Level	Indication	LI-7162A	SA	0-222 inch	X		X	X	MCB	1046	
	Indication	LI-7162B	SB	0-222inch	X		X	X	MCB	1046	
Cont Sump Temp	Indication	TI-7133A	SA	50-250°F	X			X	MCB	1041	
	Indication	TI-7133B	SB	50-250°F	X			X	MCB	1042	
Cont Outside Diff Press.	Indication	PDI-7680A	SA	±5 in. wg.	X		X		MCB	2688	
Cont Outside Diff Press.	Indication	PDI-7680B	SB	±5 in. wg.	X		X		MCB	2689	
Cont fan CLR-AH1	Recording	TR-1AV-0005 (PT-15)	NNS	0-400F	X		X		AEP-2		
Cooling Coil Outlet Temp											
- AH2	Recording	TR-IAV-0005 (PT-16)	NNS	0-400F	X		X		AEP-2		
- AH3	Recording	TR-IAV-0005 (PT-17)	NNS	0-400F	X		X		AEP-2		
- AH4	Recording	TR-IAV-0005 (PT-18)	NNS	0-400F	X		X		AEP-2		
- AH37	Recording	TR-IAV-0005 (PT-19)	NNS	0-400F	X		X		AEP-2		
- AH38	Recording	TR-IAV-0005 (PT-20)	NNS	0-400F	X		X		AEP-2		
- AH39	Recording	TR-IAV-0005 (PT-21)	NNS	0-400F	X		X		AEP-2		

TABLE 7.5.1-2

CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR
TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS

AUXILIARY FEEDWATER SYSTEM

				Instrument		Required for					
Monitored Parameter	Function	Inst Tag. No.	Train	Range	ESF	ESF Support	PPDI	PAMI	Location	CWD	Note
AFW Flow to SG-A	Indication	FI-2050A1	SA	0-266 KPPH	X			X	MCB	1957	
	Recorded	FR-AF-2050 PEN-1 (Red)	NNS	0-266 KPPH						1559	
AFW Flow to SG-B	Indication	FI-2050B1	SB	0-266 KPPH	X			X	MCB	1957	
	Recorded	FR-AF-2050 PEN-2 (Green)	NNS	0-266 KPPH						1559	
AFW Flow to SG-C	Indication	FI-2050C1	SA	0-266 KPPH	X			X	MCB	1957	
	Recorded	FR-AF-2050 PEN-3 (Blue)	NNS	0-266 KPPH						1559	
AFW Pump A Disch Press.	Indication	PI-2150A1	SA	0-2000 psig	X			X	MCB	1957	
AFW Pump B Disch Press.	Indication	PI-2150B1	SB	0-2000 psig	X			X	MCB	1957	
AFW Turb Pump Disch Press.	Indication	PI-2170.1	SB	0-2000 psig	X			X	MCB	1959	
AFW Pump A Suction Press.	Indication	PI-2250A1	SA	0-200 psig	X				MCB	1957	
AFW Pump B Suction Press.	Indication	PI-2250B1	SB	0-200 psig	X				MCB	1957	
AFW Turb Pump Suction Press.	Indication	PI-2270.1	SB	0-200 psig	X				MCB	1958	
STM/AFW Turb Pump Diff Press.	Indication	PDI-2180.1	SB	0-100 psid	X				MCB	1960	
AFW Turb Pump Speed	Indication	SI-2180.1	SB	0-6000 RPM	X				MCB	1978	
Condensate Storage Tank Level	Indication	LI-9010A1	SA	0-100 %	X		X	X	MCB	2092	
	Indication	LI-9010B1	SB	0-100 %	X		X	X	MCB	2092	
STM/AFW Turb Pump STM Press.	Indication	PI-430.1	SB	0-1500 psig	X				MCB	1960	

TABLE 7.5.1-3 CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS

EMERGENCY POWER SYSTEM

Monitored Parameter	Function	Inst Tag. No.	Train	Instrument Range	ESF	Required for ESF Support	PPDI	PAMI	Location	CWD	Note
Emergency Bus 1A Voltage	Indication	EI-6956A1	SA	0-9000 V		X			MCB	1729	
Diesel Generator A Voltage	Indication	EI-6955A	SA	0-9000 V		X		X	MCB	1993	
Diesel Generator A Field Voltage	Indication	EI-6954A	SA	0-150 V		X		X	MCB	1994	
Diesel Generator A Synchronizing Diff Voltage	Indication	EI-6953A	SA	±30 V		X			MCB	1791	
Emergency Bus 1A Frequency	Indication	EI-6960A	SA	55-65 Hz		X			MCB	1729	
Diesel Generator A Frequency	Indication	EI-6959A	SA	55-65 Hz		X			MCB	1993	
Diesel Generator A Synchroscope	Indication	EI-6926A	SA	slow/fast		X			MCB	1791	
Diesel Generator A Field Current	Indication	EI-6950A	SA	0-500 A		X			MCB	1994	
Diesel Generator A Current	Indication	EI-6951A	SA	0-800 A		X		X	MCB	1994	
Diesel Generator A Power	Indication	EI-6957A1	SA	0-9.6 MW		X			MCB	1994	
Diesel Generator A Reactive Power	Indication	EI-6958A	SA	0-9.6 MVAR		X			MCB	1994	
Battery A Voltage	Indication	EI-6961A	SA	0-150 V		X	X	X	MCB	1798	
Diesel Generator A Day Tank Level	Indication	LI-2461A	SA	0-100%		X	X		MCB	2546	
Emergency Bus 1B Voltage	Indication	EI-6956B1	SB	0-9000 V		X			MCB	1730	
Diesel Generator B Voltage	Indication	EI-6955B	SB	0-9000 V		X		X	MCB	2013	
Diesel Generator B Field Voltage	Indication	EI-6954B	SB	0-150 V		X		X	MCB	2014	
Diesel Generator B Synchronizing Diff Voltage	Indication	EI-6953B	SB	±30 V		X			MCB	1793	
Emergency Bus 1B Frequency	Indication	EI-6960B	SB	55-65 Hz		X			MCB	1730	
Diesel Generator B Frequency	Indication	EI-6959B	SB	55-65 Hz		X			MCB	2013	
Diesel Generator B Synchroscope	Indication	EI-6962B	SB	Slow/Fast		X			MCB	1793	
Diesel Generator B Field Current	Indication	EI-6950B	SA	0-500 A		X			MCB	2014	
Diesel Generator B Current	Indication	EI-6951B	SA	0-800 A		X		X	MCB	2014	
Diesel Generator B Power	Indication	EI-6957B1	SA	0-9.6 MW		X			MCB	2014	
Diesel Generator B Reactive Power	Indication	EI-6958B	SB	0-9.6 MVAR		X			MCB	2014	
Battery B Voltage	Indication	EI-6961B1	SB	0-150 V		X	X	X	MCB	1799	

TABLE 7.5.1-3 CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS

EMERGENCY POWER SYSTEM

				Instrument		Required for					
Monitored Parameter	Function	Inst Tag. No.	Train	Range	ESF	ESF Support	PPDI	PAMI	Location	CWD	Note
Diesel Generator B Day Tank Level	Indication	LI-2461B	SB	0-100%		X	X		MCB	2547	
Battery A Amp	Indication	EI-6963A1	SA	±600 A		X	X		MCB	1798	
Battery B Amp	Indication	EI-6963B1	SB	±600 A		X	X		MCB	1799	

TABLE 7.5.1-4

CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR
TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III, AND IV EVENTS

SERVICE WATER SYSTEM

				Instrument		Required for					
Monitored Parameter	Function	Inst Tag. No.	Train	Range	ESF	ESF Support	PPDI	PAMI	Location	CWD	Note
SW Supply HDR A Disch Press.	Indication	PI-9101A1	SA	0-200 psig		X		X	MCB	2213	
SW Supply HDR B Disch Press.	Indication	PI-9101B1	SB	0-200 psig		X		X	MCB	2213	
Service Water Header "A" Flow	Indication	FI-9101A1	SA	0-25 kgpm		X	X	X	MCB	2213	
Service Water Header "B" Flow	Indication	FI-9101B1	SB	0-25 kgpm		X	X	X	MCB	2213	
Service Water Booster Pump A Disch Flow	Indication	FI-9112A	SA	0-4000 gpm		X		X	MCB	2235	
Service Water Booster Pump B Disch Flow	Indication	FI-9112B	SB	0-4000 gpm		X		X	MCB	2235	
Service Water Booster Pump A Disch Press.	Indication	PI-9112A	SA	0-350 psig		X		X	MCB	2235	
Service Water Booster Pump B Disch Press.	Indication	PI-9112B	SB	0-350 psig		X		X	MCB	2235	

TABLE 7.5.1-5 CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III, AND IV EVENTS

CONTROL ROOM EMERGENCY FILTRATION SYSTEM

Monitored Parameter	Function	Inst Tag. No.	Train	Instrument Range	ESF	Required for ESF Support	PPDI	PAMI	Location	CWD	Note
Control Room Em Filter SYS A Overall Diff Pressure	Indication	PDI-7827A	SA	0-15” H_2O		X			MCB	2993	
Control Room Em Filter SYS B Overall Diff Pressure	Indication	PDI-7827B	SB	0-15” H_2O		X			MCB	2994	
Control Room Em Filter CHAR Filter in Temp	Indication Recording	TI-7824A TR-1AV-0005 (PT-10)	SA NNS	0-250 F 0-250 F		X			MCB AEP-2	2993	
Control Room Em Filter HEPA Filter Diff Press.	Indication Recording	TI-7824B TR-1AV-0005 (PT-12)	SB NNS	0-250 F 0-250 F		X			MCB AEP-2	2994	
Control Room Em Filter HEPA Filter Diff Press.	Indication	PDI-7823A	SA	0-5” H_2O		X			MCB	2993	
Control Room Em Filter HEPA Filter Diff Press.	Indication	PDI-7823A	SB	0-5” H_2O		X			MCB	2994	
Control Room Emerg. Filter A Outside Air Flow	Indication	FI-7817A	SA	0-500 cfm		X			MCB AEP-2	2993	
Control Room Emerg. Filter B Outside Air Flow	Indication	FI-7817B	SB	0-500 cfm		X			MCB	2994	
Control Room Fan AH-15 (1A-SA) EHC Outlet Temp	Indication	TI-7835A1	SA	0-100 F		X	X		MCB	2991	
Control Room Fan AH-15 (1B-SB) EHC Outlet Temp	Indication	TI-7835B1	SB	0-100 F		X	X		MCB	2991	
Control Room Temp	Indication	TI-7837A1	SA	0-100 F		X	X		MCB	2991	
Control Room Temp	Indication	TI-7837B1	SB	0-100 F		X	X		MCB	2991	
Control Room to Outside Differential Press.	Indication	PDI-7838A1	SA	0-1 in. w.c.		X	X		MCB	2992	
Control Room to Outside Differential Press.	Indication	PDI-7838B1	SB	0-1 in. w.c.		X	X		MCB	2992	
Control Room Em Filter A EHC-72 Air Inlet Temp	Indication Recording	TI-7821A1 TR-1AV-0005 (PT-9)	SA NNS	0-250 F 0-250 F		X			MCB AEP-2	2993	
Control Room Em Filter B EHC-72 Air Inlet Temp	Indication Recording	TI-7821B1 TR-1AV-0005 (PT-11)	SB NNS	0-250 F 0-250 F		X			MCB AEP-2	2994	
Control Room Em Filter Fan R2(A) Air Flow	Indication	FI-7819A	SA	0-5000 cfm		X			MCB	2993	
Control Room Em Filter Fan R2 (B) Air Flow	Indication	FI-7819B	SB	0-5000 cfm		X			MCB	2994	
Control Room Em Filter Fan R2(A) Out Temp	Indication	TI-7819A	SA	50-350°F		X			MCB	2991	
Control Room Em Filter Fan R2(B) Out Temp	Indication	TI-7819B	SB	50-350°F		X			MCB	2991	

TABLE 7.5.1-6

CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR
TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III, AND IV EVENTS

REACTOR AUXILIARY BUILDING EMERGENCY EXHAUST SYSTEM

				Instrument		Required for					
Monitored Parameter	Function	Inst Tag. No.	Train	Range	ESF	ESF Support	PPDI	PAMI	Location	CWD	Note
RAB Emergency Filter A Air Inlet Temp	Indication Recording	TI-4836A TR-1AV-005 (PT-1)	SA NNS	0-250 F 0-250 F		X			AEP-1 AEP-2	3090	
RAB Emergency Filter B Air Inlet Temp	Indication Recording	TI-4836B TR-1AV-005 (PT-3)	SA NNS	0-250 F 0-250 F		X			AEP-1 AEP-2	3091	
RAB Emergency Exhaust A HEPA Diff Press.	Indication	PDI-4838A	SA	0-5” H_2O		X			AEP-1	3090	
RAB Emergency Exhaust B HEPA Diff Press.	Indication	PDI-4838B	SB	0-5” H_2O		X			AEP-1	3091	
RAB Emergency Filter A Outlet Temp	Indication Recording	TI-4839A TR-1AV-0005 (PT-2)	SA NNS	0-250 F 0-250 F		X			AEP-1 AEP-2	3090	
RAB Emergency Filter B Outlet Temp	Indication Recording	TI-4839B TR-1AV-0005 (PT-4)	SA NNS	0-250 F 0-250 F		X			AEP-1 AEP-2	3091	
RAB Emergency Exhaust Filter A Overall Diff Press.	Indication	TI-4843A	SA	0-15” H_2O		X			AEP-1	3090	
RAB Emergency Exhaust Filter B Overall Diff Press.	Indication	PDI-4843B	SB	0-15” H_2O		X			AEP-1	3091	
RAB Emergency Exhaust Fan A Discharge Flow	Indication	FI-4842A	SA	0-7500 cfm		X			AEP-1	3095	
RAB Emergency Exhaust Fan B Discharge Flow	Indication	FI-4842B	SB	0-7500 cfm		X			AEP-1	3095	
RAB Em Exhaust	Indication	TI-4842A	SA	50-350°F		X			AEP-1	3095	
FAN EG Outlet Temp	Indication	TI-4842B	SB	50-350°F		X			AEP-1	3095	

TABLE 7.5.1-7 CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS

FUEL HANDLING BUILDING EMERGENCY EXHAUST SYSTEM

Monitored Parameter	Function	Inst Tag. No.	Train	Range	ESF	ESF Support	PPDI	PAMI	Location	CWD	Note
FHB Emergency Filter A Air in Temp	Indication Recording	TI-5021A TR-1AV-0005 (PT-5)	SA NNS	0-250 F 0-250 F		X			AEP-1 AEP-2	2931	
FHB Emergency Filter B Air in Temp	Indication Recording	TI-5021B TR-1AV-0005 (PT-7)	SB NNS	0-250 F 0-250 F		X			AEP-1 AEP-2	2933	
FHB Emergency Diff Press. Across HEPA Filter A	Indication	PDI-5023A1	SA	0-5" H2O		X			AEP-1	2931	
FHB Emergency Diff Press. Across HEPA Filter B	Indication	PDI-5023B1	SB	0-5" H_2O		X			AEP-1	2933	
FHB Emergency Filter A Outlet Air Temp	Indication Recording	TI-5023 TR-1AV-0005 (PT-6)	SA NNS	0-250 F 0-250 F		X			AEP-1 AEP-2	2931	
FHB Emergency Filter B Outlet Air Temp	Indication Recording	TI-5023 TR-1AV-0005 (PT-8)	SB NNS	0-250 F 0-250 F		X			AEP-1 AEP-2	2933	
FHB Emergency Filter Sys A Diff Press.	Indication	PDI-5026A	SA	0-15" H_2O		X			AEP-1	2931	
FHB Emergency Filter Sys B Diff Press.	Indication	PDI-5026B	SB	0-15" H_2O		X			AEP-1	2933	
FHB Emergency Exh Fan A Flow	Indication	FI-5027A1	SA	0-7500 cfm		X			AEP-1	2931	
FHB Emergency Exh Fan B Flow	Indication	FI-5027B1	SB	0-7500 cfm		X			AEP-1	2933	
FHB Em Exh Fan A Out Temp	Indication	TI-3027A	SA	50-350°F		X			AEP-1	2931	
FHB Em Exh Fan B Out Temp	Indication	TI-5027B	SB	50-350°F		X			AEP-1	2933	

TABLE 7.5.1-8

CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR
TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS

FUEL HANDLING SPENT FUEL PUMP ROOM VENTILATION SYSTEM

Monitored Parameter	Function	Inst Tag. No.	Train	Range	ESF	ESF Support	PPDI	PAMI	Location	CWD	Note
FHB Pump Area South Temp	Indication	TI-6537A	SA	50-150 F		X	X		AEP-1	2851	
FHB Pump Area North Temp	Indication	TI-6537A1	SA	50-150 F		X	X		AEP-1	2851	
FHB Pump Area South Temp	Indication	TI-6537B	SB	50-150 F		X	X		AEP-1	2851	
FHB Pump Area North Temp	Indication	TI-6537B1	SB	50-150 F		X	X		AEP-1	2851	

TABLE 7.5.1-9 CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS

REACTOR COOLANT SYSTEM

Monitored Parameter	Function	Inst Tag. No.	Train	Range	ESF	ESF Support	PPDI	PAMI	Location	CWD	Note
COLD LEG TEMPERATURE	INDICATION										
	LOOP-A	TI-410.1	SB	0-700 F			X	X	MCB	184[1]	
	LOOP-B	TI-420.1	SB	"			X	X	MCB	184[2]	
	LOOP-C	TI-430	SB	"			X	X	MCB	184	
	RECORDING	PEN-1	NNS	0-700 F			X		RCDR PNL	184[3]	
	LOOP-A	PEN-2									
	LOOP-B	PEN-3									
	LOOP-C	TI-410.1									
HOT LEG TEMPERATURE	INDICATION	TI-413.1	SA	0-700 F			X	X	MCB	183	
	LOOP-A	TI-423.1	SA	"			X	X	MCB	183	
	LOOP-B	TI-433	SA	"			X	X	MCB	183	
	LOOP-C	TR-413	NNS	0-700 F			X		RCDR PNL	183	
	RECORDING	PEN-1									
	LOOP-A	PEN-2									
	LOOP-B	PEN-3									
	LOOP-C										
HOT/COLD LEG OVER-POWER ΔT SETPOINT	INDICATION										
	LOOP-1	TI-412B	NNS	0-150%			X		MCB	191	
	LOOP-2	TI-422B	NNS	"			X		MCB	191	
	LOOP-3	TI-432B	NNS	"			X		MCB	192	
HOT/COLD LEG OVER TEMPERATURE ΔT SETPOINT	INDICATION										
	LOOP-1	TI-412C	NNS	0-150%			X		MCB	191	
	LOOP-2	TI-422C	NNS	"			X		MCB	191	
	LOOP-3	TI-432C	NNS	"			X		MCB	192	
	RECORDING OVERPOWER	TR-412 PEN-1	NNS	"			X		RCDR PNL	193[4]	

TABLE 7.5.1-9 CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS

REACTOR COOLANT SYSTEM

Monitored Parameter	Function	Inst Tag. No.	Train	Range	ESF	ESF Support	PPDI	PAMI	Location	CWD	Note
	OVER TEMP	PEN-2									
PRESSURIZER PRESSURE	INDICATION	PI-455.1	NNS	1700-2500 PSIG			X		MCB	148	
		PI-456	NNS	"			X		MCB	148	
		PI-457	NNS	"			X		MCB	149	
		PI-444	NNS	"			X		MCB	149	
		PI-445.1	NNS	"			X		MCB	149	
PRESSURIZER LEVEL	INDICATION	LI-459A1	SA	0-100%			X	X	MCB	145(5)	
		LI-460	SB	"			X	X	MCB	145(6)	
		LI-461.1	SA	"			X	X	MCB	145	
	RECORDING	LR-459	NNS	0-100%			X		RCDR PNL	146	
	LEVEL	PEN-1									
	LEVEL SP	PEN-2									
PRIMARY COOLANT FLOW	INDICATION	FI-414	NNS	0-120%			X		MCB	195	
	LOOP-A	FI-415	NNS	"			X		MCB	195	
		FI-416	NNS	"			X		MCB	196	
	LOOP-B	FI-424	NNS	"			X		MCB	195	
		FI-425	NNS	"			X		MCB	195	
		FI-426	NNS	"			X		MCB	196	
	LOOP-C	FI-434	NNS	"			X		MCB	195	
		FI-435	NNS	"			X		MCB	195	
		FI-436	NNS	"			X		MCB	196	
SYSTEM WIDE RANGE PRESSURE	INDICATION	PI-402.1	SA	0-3000 PSIG			X	X	MCB	197(7)	
		PI-403.1	SB	"			X	X	MCB	197	
	RECORDING	PR-402	NNS	"			X		RCDR PNL	197	
	SET I	PEN-1									
	SET IV	PEN-2									
REACTOR COOLANT PUMP CURRENT	INDICATION		NNS								
	LOOP-A	RCP-1	EI-0160	0-800 Amps			X		MCB	101	

TABLE 7.5.1-9 CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS

REACTOR COOLANT SYSTEM

Monitored Parameter	Function	Inst Tag. No.	Train	Range	ESF	ESF Support	PPDI	PAMI	Location	CWD	Note
	LOOP-B	RCP-2	EI-0161	0-800 Amps			X		MCB	103	
	LOOP-C	RCP-3	EI-0162	0-800 Amps			X		MCB	105	
RMW STORAGE TANK LEVEL	INDICATION	LI-8901A	SA	0-100%	X		X		MCB	2383	
RMW STORAGE TANK LEVEL	INDICATION	LI-8901B	SB	0-100%	X		X		MCB	2383	
Boric Acid Tank Level	INDICATION	LI-106	SA	0-100%				X	MCB	208	
		LI-161.1	SB	0-100%				X	MCB	208	
Neutron Flux Monitoring System	INDICATION	NI-60B1	SA	10 to 200% power				X	MCB	71	
		NI-60A1		10^{-1} to 10^{6} cps							
		NI-61B	SB	10^{-3} to 200% power				X	MCB	72	
		NI-61A		10^{-1} to 10^{6} cps							

NOTES:
(1) Maintain the plant in a safe shutdown condition.
(2) Ensure proper cooldown rate.
(3) Ensure proper relationship between system pressure and temperature.
(4) Each channel is selected through TS-412Z.
(5) Maintain proper reactor coolant inventory.
(6) Determine return of water level to pressurizer following steam break and steam generator tube ruptures.
(7) Ensure proper relationship between system pressure and temperature.

TABLE 7.5.1-10

CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS

CONTAINMENT SYSTEM

Monitored Parameter	Function	Inst Tag. No.	Train	Range	ESF	ESF Support	PPDI	PAMI	Location	CWD	Note
CONTAINMENT PRESSURE	INDICATION										
	SET-I	PI-950	SA	0 TO 55 PSIG			X	X	MCB	185[1]	
	SET-II	PI-951	SB	"			X	X	MCB	185	
	SET-III	PI-952	SA	"			X	X	MCB	185	
	SET-IV	PI-953	SB	"			X	X	MCB	185	
	RECORDING	PR-950	NNS	“			X		RCDR PNL	185	
	SET-I	PEN-1									
	SET-II	PEN-2									
CONTAINMENT WIDE RANGE PRESSURE	INDICATION	PI-7160A	SA	-5 TO 135 PSIG			X	X	MCB	188	
		PI-7160B	SB	-5 TO 135 PSIG			X	X	MCB	188	

NOTES:

(1) Monitor containment conditions following primary or secondary system break inside Containment.

TABLE 7.5.1-11

CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR

TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS

MAIN STEAM SUPPLY SYSTEM

Monitored Parameter	Function	Inst Tag. No.	Train	Range	ESF	ESF Support	PPDI	PAMI	Location	CWD	Note
STEAM GEN-1 LEVEL (NARROW RANGE)	INDICATION										
	SET-I	LI-474	SA	0-100%			X	X	MCB	993[1]	
	SET-II	LI-475	SB	"			X	X	MCB	993[2]	
	SET-III	LI-476	SA	"			X	X	MCB	994[3]	
	SET-IV	LI-473	SB	"			X	X	MCB	994	
	RECORDING	UR-478	NNS	0-100%			X		MCB	994	
STEAM GEN-2 LEVEL (NARROW RANGE)	INDICATION										
	SET-I	LI-484	SA	0-100%			X	X	MCB	993	
	SET-II	LI-485	SB	"			X	X	MCB	993	
	SET-III	LI-486	SA	"			X	X	MCB	994	
	SET-IV	LI-483	SB	"			X	X	MCB	994	
	RECORDING	UR-488	NNS	0-100%			X		MCB	994	
STEAM GEN-3 LEVEL (NARROW RANGE)	INDICATION										
	SET-I	LI-494	SA	0-100%			X	X	MCB	993	
	SET-II	LI-495	SB	"			X	X	MCB	993	
	SET-III	LI-496	SA	"			X	X	MCB	994	
	SET-IV	LI-493	SB	"			X	X	MCB	994	
	RECORDING	UR-498	NNS	0-100%			X		MCB	994	
STEAM GEN-1 LEVEL (WIDE RANGE)	INDICATION										
	SET-I	LI-477.1	SA	0-100%			X	X	MCB	995	
STEAM GEN-2 LEVEL (WIDE RANGE)	INDICATION	LI-487.1	SB	0-100%			X	X	MCB	995	
	SET-II										
STEAM GEN-3 LEVEL (WIDE RANGE)	INDICATION	LI-497.1	SA	“			X	X	MCB	995	
	SET III										
	RECORDING	LR-477	NNS	“			X		MCB	995	
	SET-1	CH-1							MCB	995	

TABLE 7.5.1-11

CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR

TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS

MAIN STEAM SUPPLY SYSTEM

Monitored Parameter	Function	Inst Tag. No.	Train	Range	ESF	ESF Support	PPDI	PAMI	Location	CWD	Note
	SET-II	CH-2							MCB	995	
	SET-III	CH-3							MCB	995	
STEAM GEN-1 FW FLOW	INDICATION	FI-476	NNS	0-5 MPPH			X		MCB	991	
		FI-477	NNS	"			X		MCB	990	
	RECORDING	UR-478	NNS	0-5 MPPH					MCB	807	
STEAM GEN-2 FW FLOW	INDICATION	FI-486	NNS	0-5 MPPH			X		MCB	991	
		FI-487	NNS	"			X		MCB	990	
	RECORDING	UR-488	NNS	0-5MPPH					MCB	808	
STEAM GEN-3 FW FLOW	INDICATION	FI-496	NNS	"			X		MCB	991	
		FI-497	NNS	"			X		MCB	990	
	RECORDING	UR-498	NNS	0-5MPPH					MCB	608	
STEAM GEN-A FW PRESS	INDICATION	PI-2001A	SA	0-1500 PSIG			X		MCB	1834	
STEAM GEN-B FW PRESS	INDICATION	PI-2001B	SB	0-1500 PSIG			X		MCB	1834	
STEAM GEN-C FW PRESS	INDICATION	PI-2001C	SA	0-1500 PSIG			X		MCB	1834	
STEAM GEN-1 STEAM FLOW	INDICATION	FI-474	NNS	0-5 MPPH			X		MCB	990	
		FI-475		"			X		MCB	991	
	RECORDING	UR-478		Pen 1 & 2; 0-5 MPPH Pen 3; 0-100%			X		MCB	807	
STEAM GEN-2 STEAM FLOW	INDICATION	FI-484	NNS	0-5 MPPH			X		MCB	990	
		FI-485		"			X		MCB	991	
	RECORDING	UR-488		Pen 1 & 2; 0-5 MPPH Pen 3; 0-100%			X		MCB	808	
STEAM GEN-3 STEAM FLOW	INDICATION	FI-494	NNS	0-5 MPPH			X		MCB	990	
		FI-495		"			X		MCB	991	
	RECORDING	UR-498		Pen 1 & 2; 0-5 MPPH Pen 3; 0-100%			X		MCB	809	
STEAM LINE PRESSURE	INDICATION										
	SET-III										
	LOOP-1	PI-474.1	SB	0-1300 PSGI			X	X	MCB	989[4]	
	LOOP-2	PI-484.1	SB	"			X	X	MCB	989	

TABLE 7.5.1-11

CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR

TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS

MAIN STEAM SUPPLY SYSTEM

Monitored Parameter	Function	Inst Tag. No.	Train	Range	ESF	ESF Support	PPDI	PAMI	Location	CWD	Note
	LOOP-3	PI-494	SB	"			X	X	MCB	989	
	SET-III										
	LOOP-1	PI-475	SA	"			X	X	MCB	988(6)	
	LOOP-2	PI-485	SA	"			X	X	MCB	988	
	LOOP-3	PI-495	SA	"			X	X	MCB	988	
STEAM LINE PRESSURE	SET IV										
	LOOP-1	PI-476	SB	0-1300 PSIG			X	X	MCB	988	
	LOOP-2	PI-486	SB	"			X	X	MCB	988	
	LOOP-3	PI-496.1	SB	"			X	X	MCB	988	
	RECORDING	PR-475	NNS	"			X		RCDR PNL	989	
	SET-III										
	LOOP-1	PEN-1		0-1300 PSIG							
	LOOP-2	PEN-2		0-1300 PSIG							
	LOOP-3	PEN-3		0-1300 PSIG							
STEAM DUMP DEMAND	INDICATION	TI-408	NNS	0-100%			X		MCB	875(6)	
FIRST STAGE TURBINE PRESSURE	INDICATION										
	SET-III	PI-446	NNS	0-1200 PSIG			X		MCB	992	
	SET-IV	PI-447	NNS	"			X		MCB	992	

NOTES:
(1) Maintain adequate heat sink following an accident.
(2) Needed in recovery procedure following steam generator tube rupture.
(3) Ensure that steam generator tubes are covered following a LOCA.
(4) Needed to determine type of accident that has occurred and the proper recovery procedure to use.
(5) Determine that plant is in a safe shutdown condition.
(6) Open/close status indication for all the steam dump valves.

TABLE 7.5.1-12

CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR
TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS

REFUELING WATER STORAGE TANK

Monitored Parameter	Function	Inst Tag. No.	Train	Range	ESF	ESF Support	PPDI	PAMI	Location	CWD	Note
RWST LEVEL	INDICATION										
	SET-I	LI-990	SA	0-100%			X	X	MCB[1]	1045	
	SET-II	LI-991	SB				X	X	MCB	1045	
		LI-992	NNS				X		MCB	1045	
		LI-993	NNS				X		MCB	1045	
	RECORDING	LR-990	NNS	“			X		RCDR PNL	1045	
	SET-I	PEN-1									
	SET-II	PEN-2									

NOTES:

(1) Determine when to perform the necessary manual action following switchover from the injection phase to the recirculation phase of safety injection after a LOCA.

TABLE 7.5.1-13

CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR
TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION AND CONDITION II, III AND IV EVENTS

COMPONENT COOLING WATER SYSTEM

Monitored Parameter	Function	Inst Tag. No.	Train	Range	ESF	ESF Support	PPDI	PAMI	Location	CWD
CCW SURGE TK LEVEL	INDICATION									
	SET-I	LI-670A1	SA	0-100%			X	X	MCB	967
	SET-II	LI-676A1	SB	“			X	X	MCB	967
	RECORDING	LR-670	NNS	“			X		RCDR PNL	967
	SET-I	PEN-1								
	SET-II	PEN-2								
CCW HX DISCH PRESS	INDICATION									
	SET-I	PI-649	SA	0-200 PSIG			X	X	MCB	969
	SET-II	PI-650	SB	“			X	X	MCB	969
	RECORDING	PR-649	NNS	“			X		RCDR PNL	969
	SET-I	PEN-1								
	SET-II	PEN-2								
CCW HX DISCH TEMP	INDICATION									
	SET-I	TI-674.1	SA	0-200 F			X	X	MCB	968
	SET-II	TI-675.1	SB	“			X	X	MCB	968
	RECORDING	TR-674	NNS	“			X		RCDR PNL	968
	SET-I	PEN-1								
	SET-II	PEN-2								

TABLE 7.5.1-14 CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION

NUCLEAR INSTRUMENTATION

Parameter	No. of Channels Available	Tag Number	Range	Indicated Accuracy	Indicator/Recorder	Location	Notes
1. Source Range							
a. Count rate	2	NI-31B NI-32B	10^0 to 10^6 counts/sec	±7% of the linear full scale analog voltage	Both channels indicated. Either may be selected for recording.	MCB	One two-pen recorder is used to record any of 8 nuclear channels (2 source range; 2 intermediate range and 4 power range)
b. Startup rate	2	NI-31D NI-32D	-0.5 to 5.0 decades/min	±7% of the linear full scale analog voltage	Both channels indicated.	MCB	-
2. Intermediate Range							
a. Flux level	2	NI-35B NI-35B	10^{-11} to 10^{-3} 8 decades of neutron flux (corresponds to 0 to full scale analog voltage) overlapping the source range by 2 decades	±7% of the linear full scale analog voltage and ±3% of the linear full scale voltage in the range of 10^{-4} to 10^{-3} amps.	Both channels indicated. Either may be selected for recording using the recorder in item 1 above.	MCB	-
b. Startup rate	2	NI-35D NI-36D	-0.5 to 5.0 decades/ min	±7% of the linear full scale analog voltage	Both channels indicated.	MCB	-
3. Power Range							
a. Uncalibrated ion chamber current (top and bottom uncompensated ion chambers)	4		0 to 120% of full power current	±1% of full power current	All 8 current signals indicated.	NIS racks in control room	-
b.							
c. Upper and lower ion chamber current difference	4		-60 to +60%	±3% of full power	Diagonally opposed channels may be selected for recording at the same time using recorder in item 1.	NIS RACKS	-

TABLE 7.5.1-14 CONTROL ROOM INDICATORS AND/OR RECORDERS AVAILABLE TO THE OPERATOR TO MONITOR SIGNIFICANT PLANT PARAMETERS DURING NORMAL OPERATION

NUCLEAR INSTRUMENTATION

Parameter	No. of Channels Available	Tag Number	Range	Indicated Accuracy	Indicator/Recorder	Location	Notes
d. Average flux of the top and bottom ion chambers	4	NI-41B NI-42B NI-43B NI-44B	0 to 120% of full power	±3% of full power for indication; ±2% for recording	All 4 channels indicated. Any 2 of the 4 channels may be recorded using recorder in item 1 above.	MCB	-
e. Average flux of the top and bottom ion chambers	4		0 to 200% of full power	±2% of full power to 200%	All 4 channels recorded.	ERFIS	-
f. Flux difference of the top and bottom ion chambers	4	NI-41C NI-42C NI-43C NI-44C	-30 to +30%	±4%	All 4 channels indicated.	MCB	-

TABLE 7.5.1-15

REACTOR CONTROL SYSTEM

Parameter	No. of Channels Available	Tag Number	Range	Indicated Accuracy	Indicator/Recorder	Location	Notes
1. Demanded Rod Speed	1	SI-408	0 to 76 steps/minute	±2%	The one channel is indicated	MCB	-
2. Median T_{avg}	1	TR-408	530 to 630 F	±4 F	The one channel is recorded.	MCB	-
3. Treference	1	TR-408	530 to 630 F	±4 F	The one channel is recorded.	MCB	-
4. Control Rod Position							If system not available, borate sample accordingly
a. Number of steps of demanded rod withdrawal	1/group		0 to 233 step	±1 step	Each group is indicated during rod motion.	SCB (SAF)	These signals are used in conjunction with the measured position signals (item 4.b) to detect deviation of any individual rod from the demanded position. A deviation will actuate an alarm and annunciator.
b. Full length rod measured position	1 for each rod		0 to 228 steps	±4 steps	Each rod position is indicated	SCB (SAF)	-

TABLE 7.5.1-16

ANNUNCIATOR LIGHT BOXES

Equipment No.	Systems	Location
ALB-1	Containment Spray & Accumulator System	MCB
ALB-2	Emergency Service Normal Service Water System	MCB
ALB-3	Misc. Systems	MCB
ALB-4	RHR/RWST System	MCB
ALB-5	Component Cooling Water System	MCB
ALB-6	Chemical Volume Control System	MCB
ALB-7	Chemical Volume Control System	MCB
ALB-8	RCP System	MCB
ALB-9	Pressurizer System	MCB
ALB-10	Reactor Coolant System	MCB
ALB-11	Reactor First Out System	MCB
ALB-12	Reactor First Out System	MCB
ALB-13	Nuclear Instrumentation System and Rod Control System	MCB
ALB-14	Steam Generator System	MCB
ALB-15	Various Protective Panels Trouble Alarm	MCB
ALB-16	Feedwater System	MCB
ALB-17	Auxiliary Feedwater System	MCB
ALB-18	Turbine First Out System	MCB
ALB-19	Heater Drain Pump & Condensate System	MCB
ALB-20	MSR & Turbine System	MCB
ALB-21	LP/HP Heaters & Circulating Water System	MCB
ALB-22	Generator Exciter, Startup & Unit Transformer	MCB
ALB-23	RAB/FHB HVAC System	AEP-1
ALB-24	Diesel Generator - A System	MCB
ALB-25	Diesel Generator - B System	MCB
ALB-26	Control Panels Trouble Alarm System	MCB
ALB-27	HVAC System (DG & Containment)	MCB
ALB-28	HVAC System (Containment)	MCB
ALB-29	HVAC System (Containment)	MCB
ALB-30	HVAC System (Control Room)	MCB

TABLE 7.7.1-1

PLANT CONTROL SYSTEM INTERLOCKS

Designation	Derivation	Function
C-1	1/2 neutron flux (intermediate range) above setpoint	Blocks automatic and control rod manual withdrawal
C-2	1/4 neutron flux (power range) above setpoint	Blocks automatic and control rod manual withdrawal
C-3	2/3 Overtemperature ΔT above setpoint	Blocks automatic and manual control rod withdrawal
		Actuates turbine runback via load reference
		Defeats remote load dispatching (if remote load dispatching is used)
C-4	2/3 Overpower ΔT above setpoint	Blocks automatic and manual control rod withdrawal
		Actuates turbine runback via load reference
		Defeats remote load dispatching (if remote load dispatching is used)
C-5	1/1 turbine First Stage pressure below setpoint	Defeats remote load dispatching (if remote load dispatching is used)
		Blocks automatic control rod withdrawal
C-7	1/1 time derivative (absolute value) of turbine First Stage pressure (decrease only) above setpoint	Makes steam dump values available for either tripping or modulation
C-8	Turbine trip, 2/3 turbine auto stop oil pressure below setpoint	
	or	
	4/4 turbine valves closed	Makes steam dump valves available for either tripping or modulation
	No turbine trip, 2/3 turbine auto stop oil pressure above setpoint and 1/4 turbine-inlet line stop valves not closed	Blocks steam dump control via load rejection Tavg controller
C-9	Any condenser pressure above setpoint, or all circulation water pump breakers open	Blocks steam dump to condenser
C-11	1/1 bank D control rod position above setpoint	Blocks automatic rod withdrawal
C-16	Reduce limit in coolant temperature above normal setpoint	Stops automatic turbine loading until condition clears

FIGURE	TITLE
7.1.1-1	PROTECTION SYSTEM BLOCK DIAGRAM
7.2.1-1	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.2.1-2	SETPOINT REDUCTION FUNCTION FOR OVERTEMPERATURE ΔT TRIP
7.2.1-3	REACTOR TRIP/ESF ACTUATION MECHANICAL LINKAGE
7.3.1-1	SOLID STATE PROTECTION SYSTEM FUNCTIONAL DIAGRAMS
7.3.1-2	REACTOR TRIP/ESF ACTUATION MECHANICAL LINKAGE (2 SHEETS)
7.3.1-3	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-4	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-5	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-6	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-7	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-8	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-9	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-9A	DELETED BY AMENDMENT NO. 48
7.3.1-9B	DELETED BY AMENDMENT NO. 48
7.3.1-10	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-11	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-12	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-13	FHB EMERGENCY EXHAUST SYSTEMS, LOGIC & SCHEMATIC DIAGRAMS
7.3.1-14	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-15	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-15A	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-16	ESSENTIAL SERVICE CHILLED WATER SYSTEM - LOGIC & SCHEMATIC DIAGRAMS
7.3.1-17	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-18	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-19	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-20	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE

FIGURE	TITLE
7.3.1-21	RAB SWITCHGEAR ROOMS - LOGIC & SCHEMATIC DIAGRAMS
7.3.1-22	FHB SPENT FUEL POOL PUMP ROOM VENTILATION SYSTEM - LOGIC & SCHEMATIC DIAGRAMS
7.3.1-23	CONTAINMENT VACUUM RELIEF SYSTEM - LOGIC & SCHEMATIC
7.3.1-24	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-25	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-26	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-27	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.3.1-28	DELETED BY AMENDMENT NO. 48
7.3.2-1	TYPICAL ENGINEERED SAFETY FEATURES TEST CIRCUITS
7.3.2-2	ENGINEERED SAFETY FEATURES TEST CABINET - INDEX, NOTES AND LEGEND
7.4.1-1	LOGIC DIAGRAM FOR BORIC ACID TRANSFER PUMPS
7.4.1-2	LOGIC DIAGRAM FOR CENTRIFUGAL CHARGING PUMPS
7.4.1-3	LOGIC DIAGRAM FOR LETDOWN ORIFICE ISOLATION VALVES
7.4.1-4	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.4.1-5	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.4.1-6	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.4.1-7	LOGIC DIAGRAM FOR RESIDUAL HEAT REMOVAL PUMPS
7.4.1-8	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.5.1-1	PRESSURE, FLOW AND TEMPERATURE TYPICAL PROCESS LOOP DIAGRAM
7.5.1-2	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.5.1-3	ESF BYPASS PANEL TYPICAL WIRING DIAGRAM
7.5.1-4	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.5.1-5	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.5.1-6	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.5.1-7	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.5.1-8	STATUS LIGHT BOX TYPICAL WIRING DIAGRAM
7.5.1-9	SERVICE WATER LEAK DETECTION WINDOW LAYOUT DIAGRAM

FIGURE	TITLE
7.5.1-10	SERVICE WATER LEAK DETECTION WINDOW LAYOUT DIAGRAM
7.5.1-11	SERVICE WATER LEAK DETECTION WINDOW LAYOUT DIAGRAM
7.5.1-12	SERVICE WATER LEAK DETECTION WINDOW LAYOUT DIAGRAM
7.5.1-13	SERVICE WATER LEAK DETECTION TYPICAL WIRING DIAGRAM
7.5.1-14	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.5.1-15	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.6.1-1	RHR SYSTEM ISOLATION VALVES LOGIC DIAGRAM
7.6.1-2	RHR SYSTEM ISOLATION VALVES LOGIC DIAGRAM
7.6.1-3	ACCUMULATOR DISCHARGE VALVES CONTROL CIRCUIT LOGIC DIAGRAM
7.6.1-4	INSTRUMENTATION AND CONTROL POWER SUPPLY SYSTEM
7.6.1-5	RHR RECIRCULATION SYSTEM LOGIC DIAGRAM
7.6.1-6	RHR RECIRCULATION SYSTEM LOGIC DIAGRAM
7.6.1-7	RCS PRESSURE CONTROL LOGIC DIAGRAM
7.6.1-8	FHB FUEL POOLS A & B - LOGIC AND SCHEMATIC DIAGRAMS
7.6.1-9	FHB FUEL POOLS A & B - LOGIC AND SCHEMATIC DIAGRAMS
7.6.1-10	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.6.1-11	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.6.1-12	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.6.1-13	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.6.1-14	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.6.1-15	REFER TO FSAR TABLE 1.6-3 FOR DESIGN DOCUMENT INCORPORATED BY REFERENCE
7.7.1-1	SIMPLIFIED BLOCK DIAGRAM OF REACTOR CONTROL ROD SYSTEM
7.7.1-2	CONTROL BANK ROD INSERTION MONITOR
7.7.1-3	ROD DEVIATION COMPARATOR
7.7.1-4	BLOCK DIAGRAM OF PRESSURIZER PRESSURE CONTROL SYSTEM
7.7.1-5	BLOCK DIAGRAM OF PRESSURIZER LEVEL CONTROL SYSTEM
7.7.1-6	BLOCK DIAGRAM OF STEAM GENERATOR WATER LEVEL CONTROL SYSTEM

FIGURE	TITLE
7.7.1-7	DELETED BY AMENDMENT NO. 27
7.7.1-8	BLOCK DIAGRAM OF STEAM DUMP CONTROL SYSTEM
7.7.1-9	BASIC FLUX-MAPPING SYSTEM
7.7.2-1	SIMPLIFIED BLOCK DIAGRAM OF ROD CONTROL SYSTEM
7.7.2-2	CONTROL BANK D PARTIAL SIMPLIFIED SCHEMATIC DIAGRAM OF POWER CABINETS 1BD AND 2BD

FIGURE 7.1.1-1

PROTECTION SYSTEM BLOCK DIAGRAM

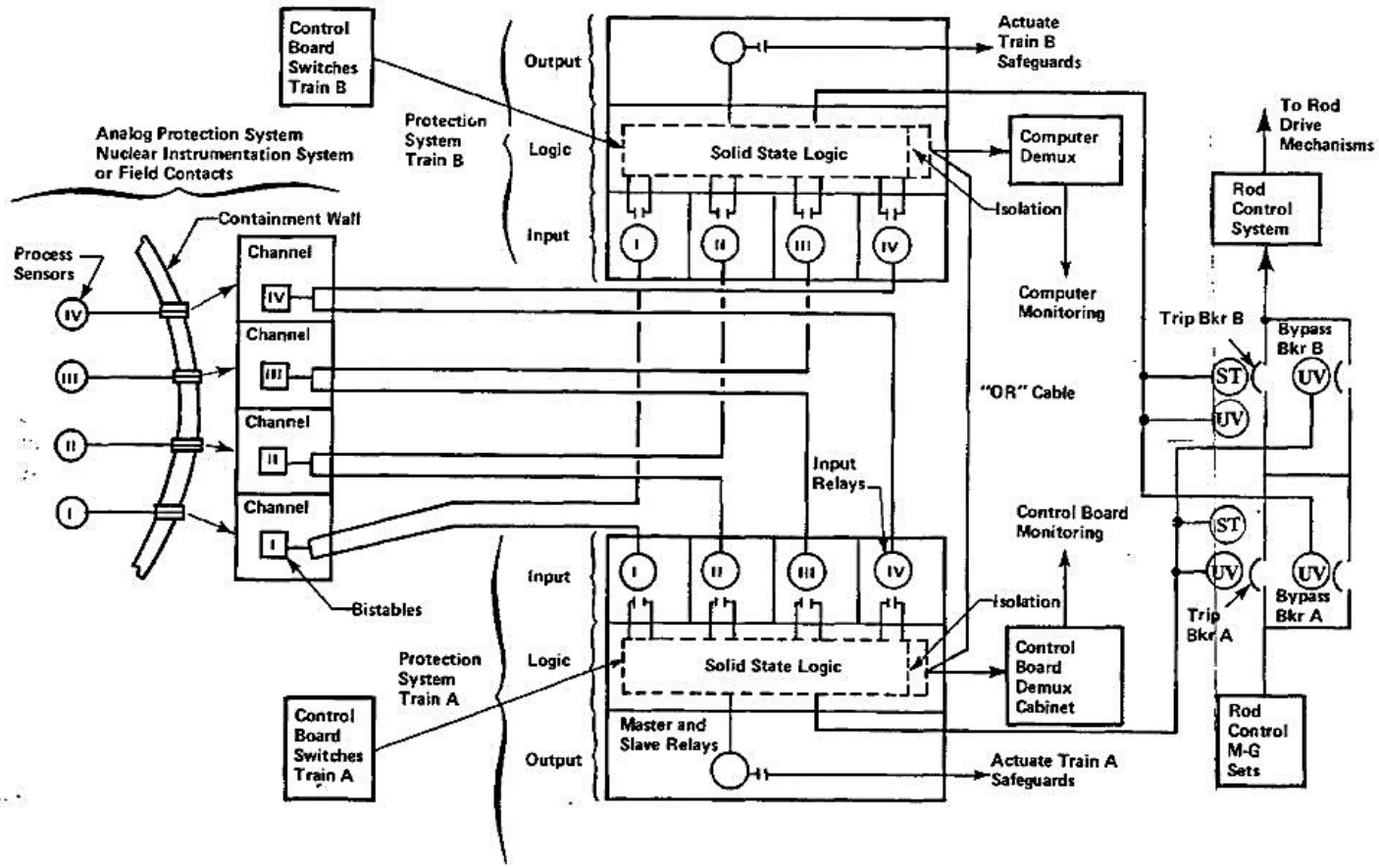
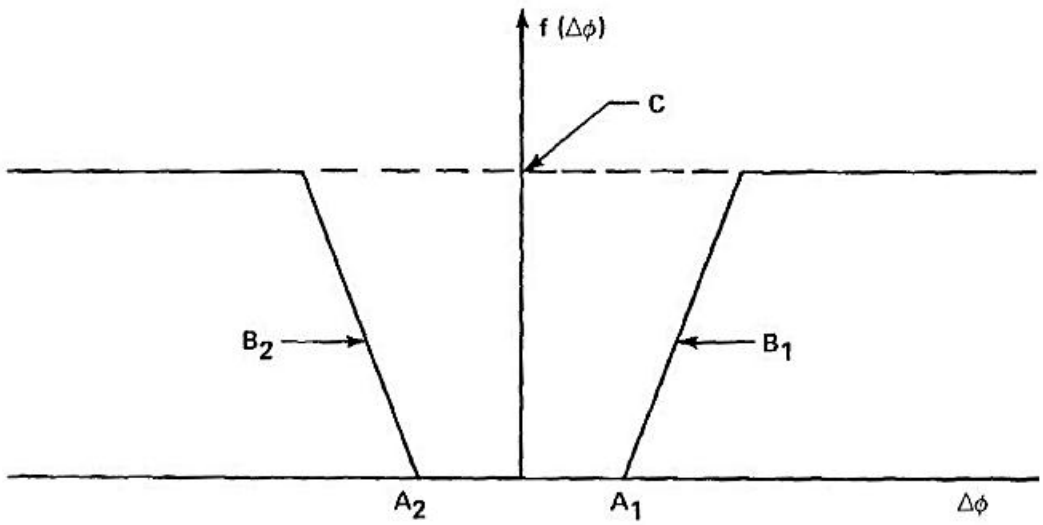


FIGURE 7.2.1-2

SETPOINT REDUCTION FUNCTION FOR OVERTEMPERATURE ΔT TRIP



$\Delta\phi$ - Neutron flux difference between upper and lower long ion chambers

A_1, A_2 - Limit of F ($\Delta\phi$) 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

FIGURE 7.2.1-3

REACTOR TRIP/ESF ACTUATION MECHANICAL LINKAGE

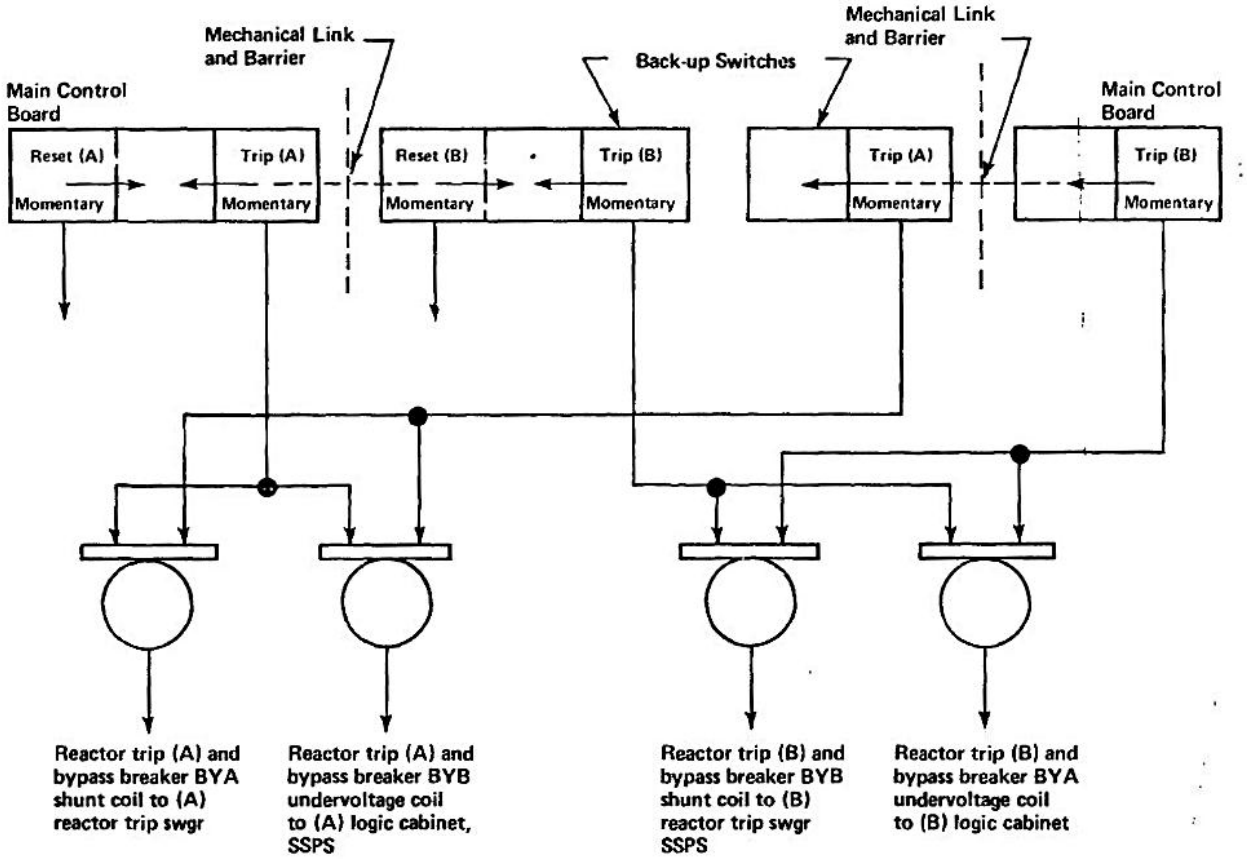
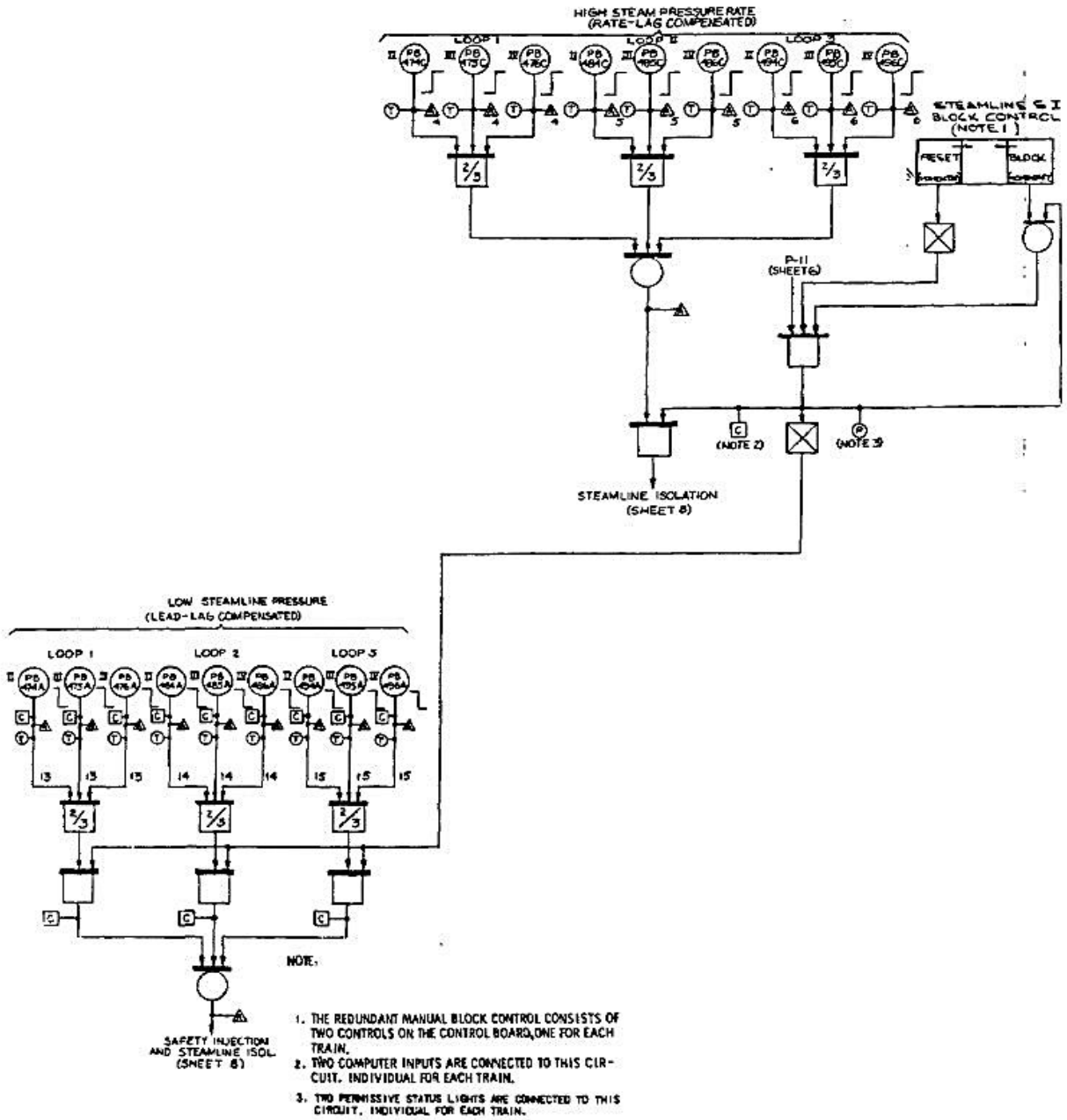


FIGURE 7.3.1-1

SOLID STATE PROTECTION SYSTEM FUNCTIONAL DIAGRAMS

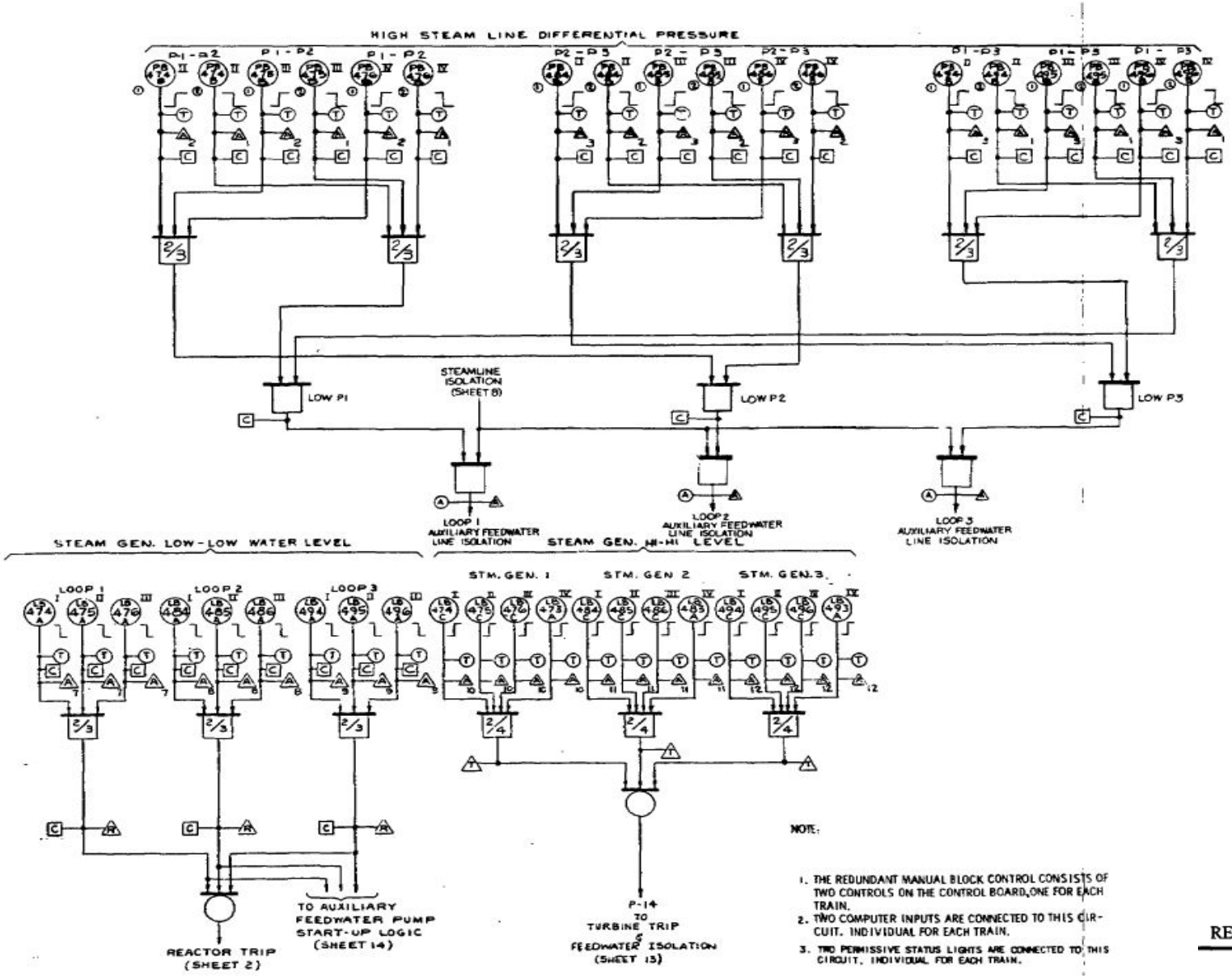


A

REF DWG: 1364-000870 (REV 6)

FIGURE 7.3.1-1

SOLID STATE PROTECTION SYSTEM FUNCTIONAL DIAGRAMS (Continued)



REF DWG: 1364-000870 (REV 6)

FIGURE 7.3.1-2

REACTOR TRIP/ESF ACTUATION MECHANICAL LINKAGE

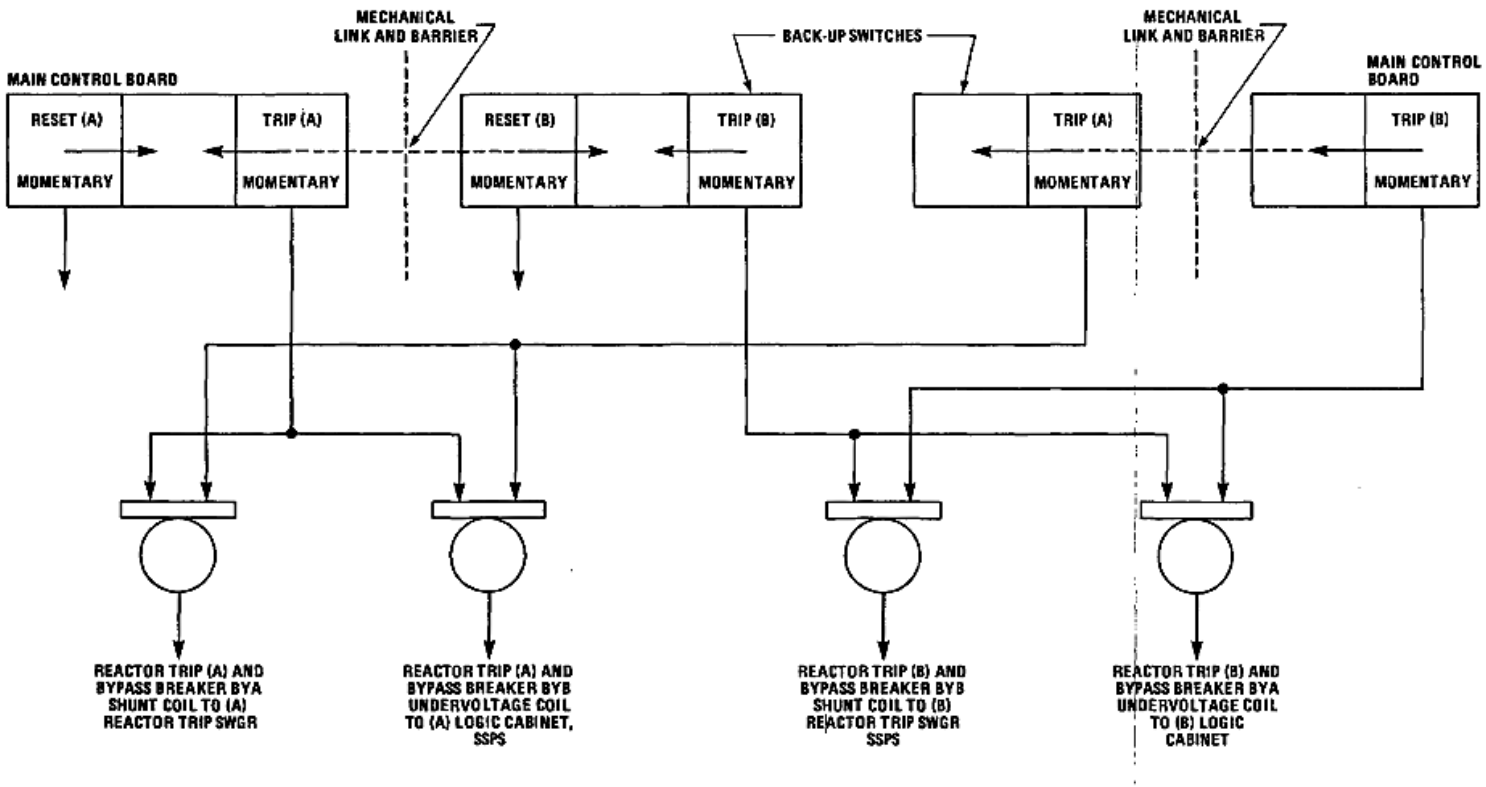


FIGURE 7.3.1-2

REACTOR TRIP/ESF ACTUATION MECHANICAL LINKAGE (Continued)

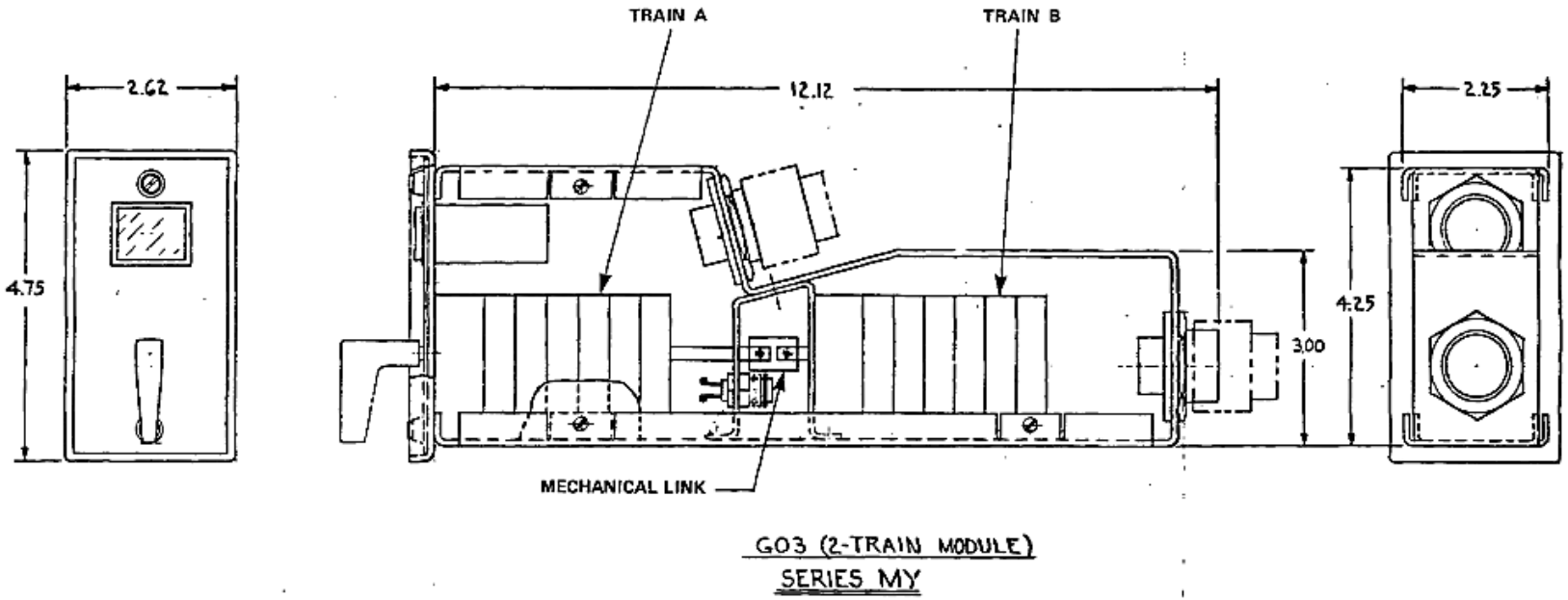


FIGURE 7.3.1-13

FHB EMERGENCY EXHAUST SYSTEMS, LOGIC & SCHEMATIC DIAGRAMS

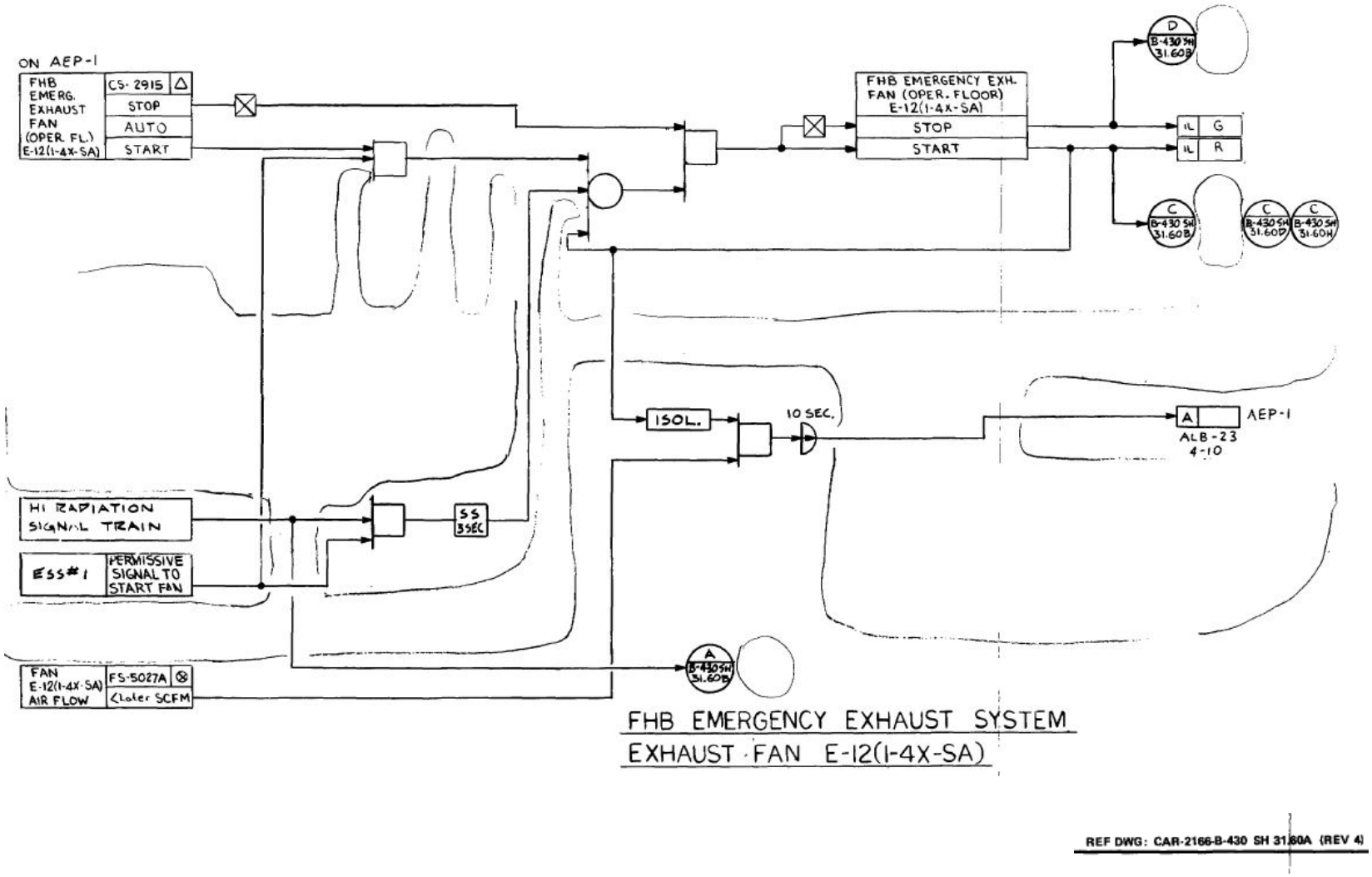


FIGURE 7.3.1-13

FHB EMERGENCY EXHAUST SYSTEMS, LOGIC & SCHEMATIC DIAGRAMS (Continued)

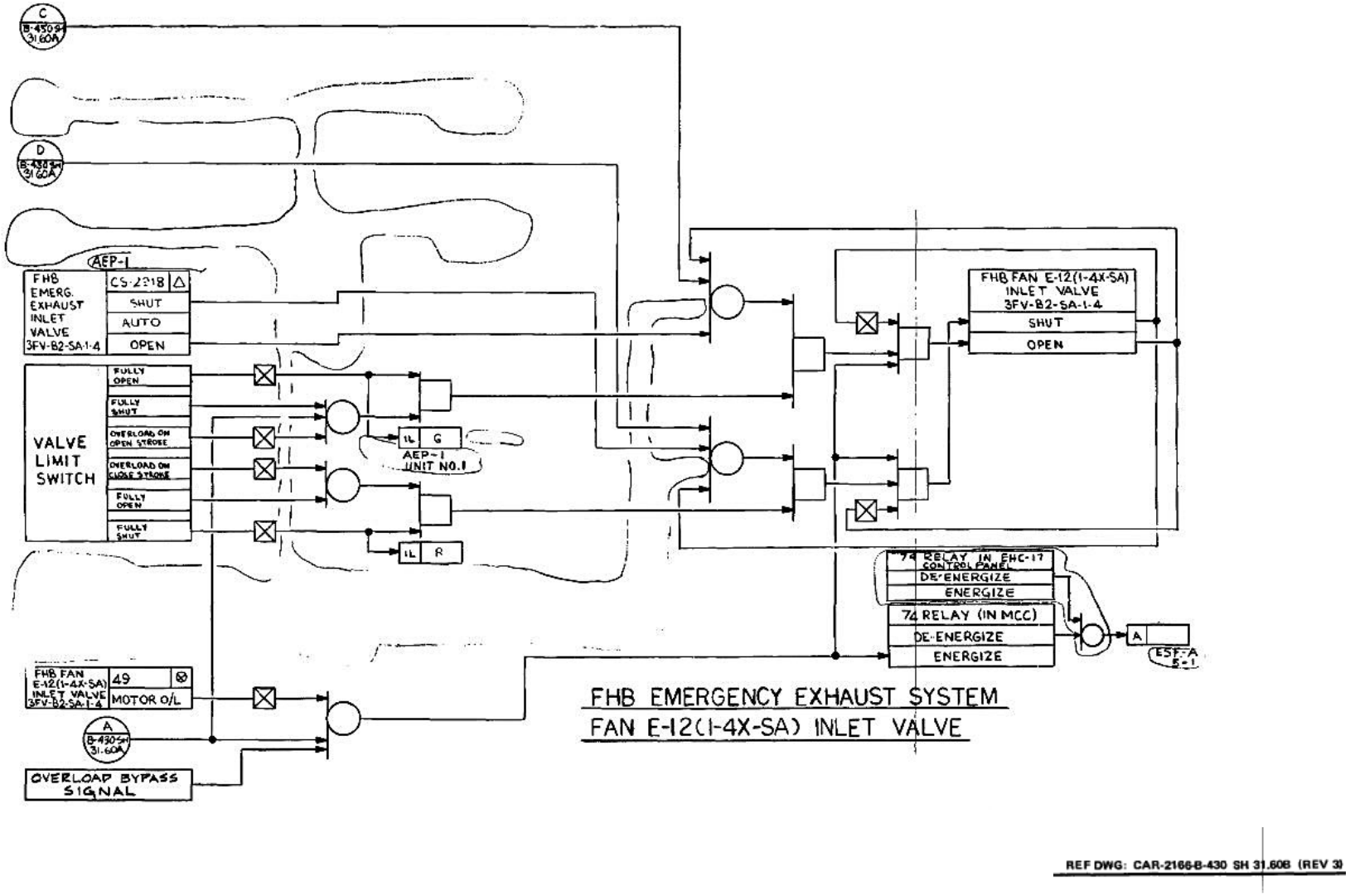
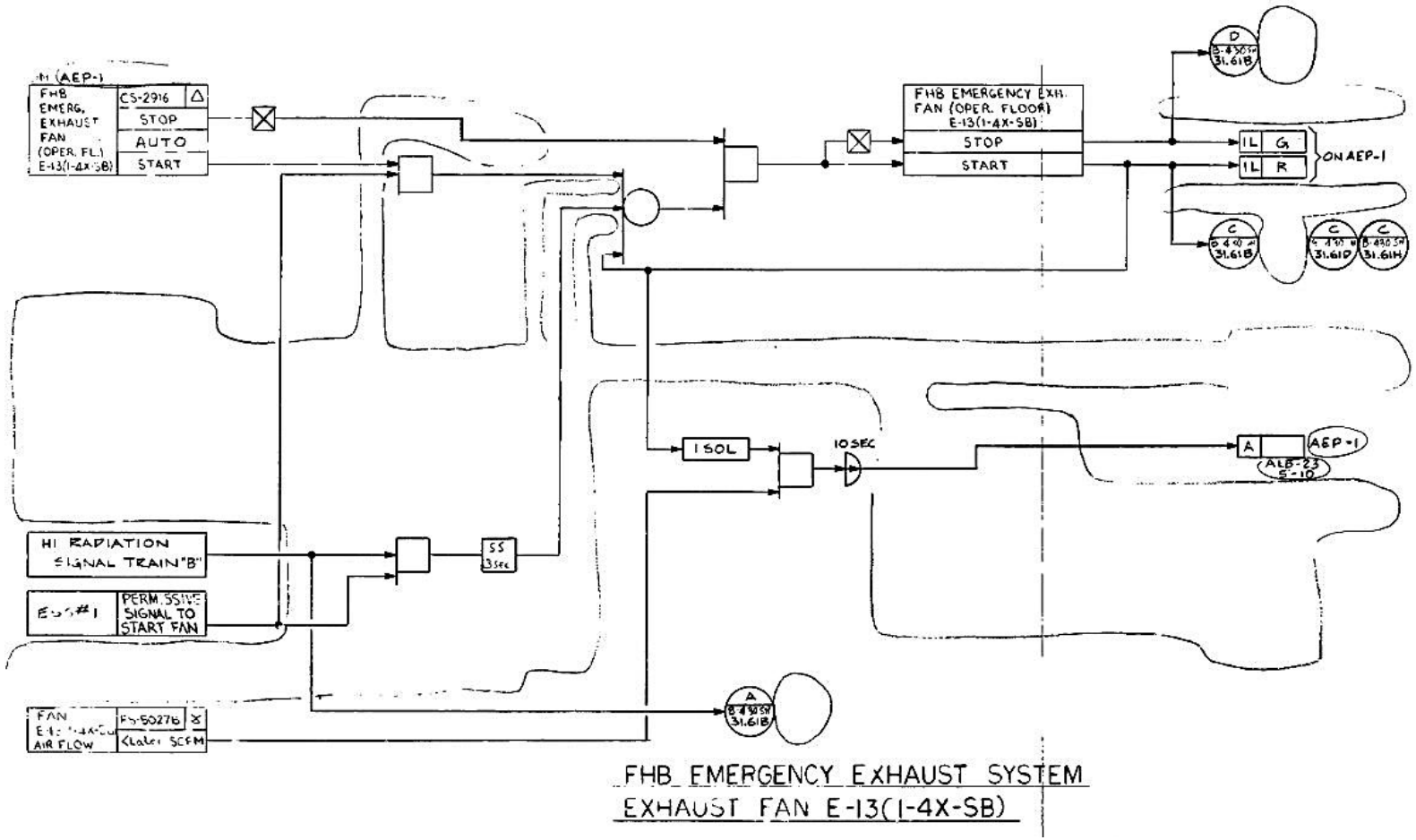


FIGURE 7.3.1-13

FHB EMERGENCY EXHAUST SYSTEMS, LOGIC & SCHEMATIC DIAGRAMS (Continued)



REF DWG: CAR-2166-B-430 SH 31.61A (REV 4)

FIGURE 7.3.1-13

FHB EMERGENCY EXHAUST SYSTEMS, LOGIC & SCHEMATIC DIAGRAMS (Continued)

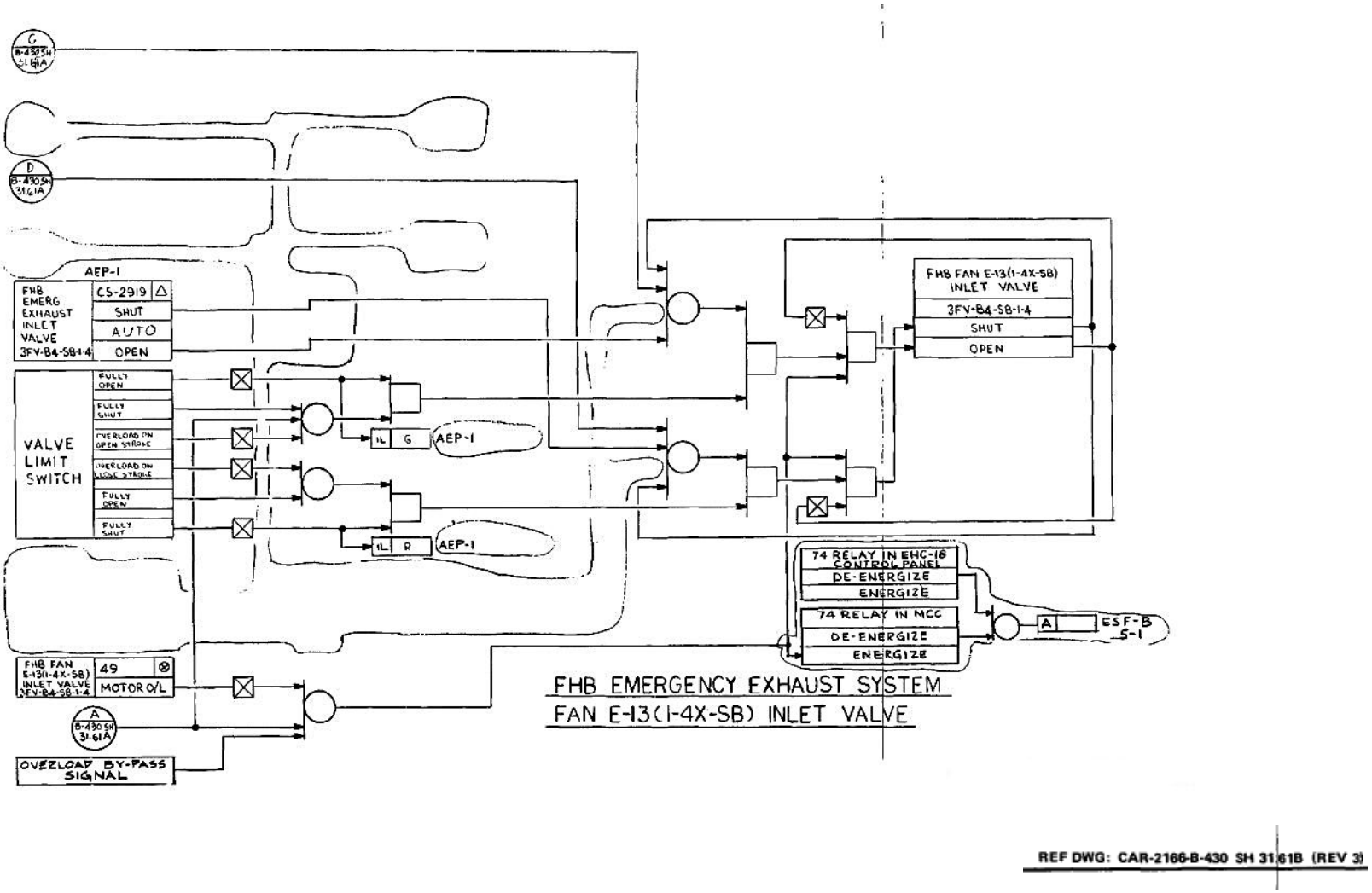


FIGURE 7.3.1-16

ESSENTIAL SERVICE CHILLED WATER SYSTEM LOGIC & SCHEMATIC DIAGRAMS

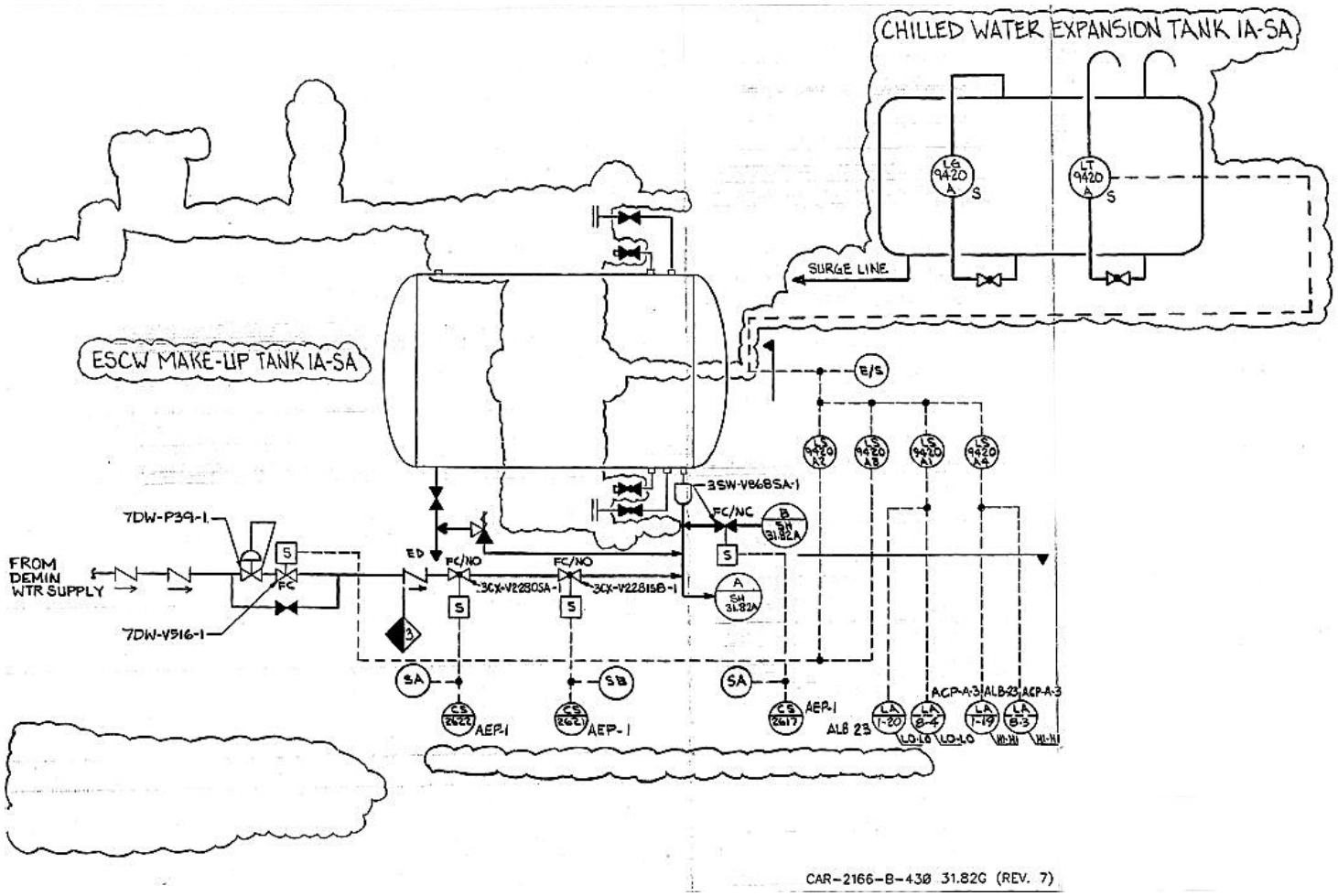


FIGURE 7.3.1-16

ESSENTIAL SERVICE CHILLED WATER SYSTEM LOGIC & SCHEMATIC DIAGRAMS (Continued)

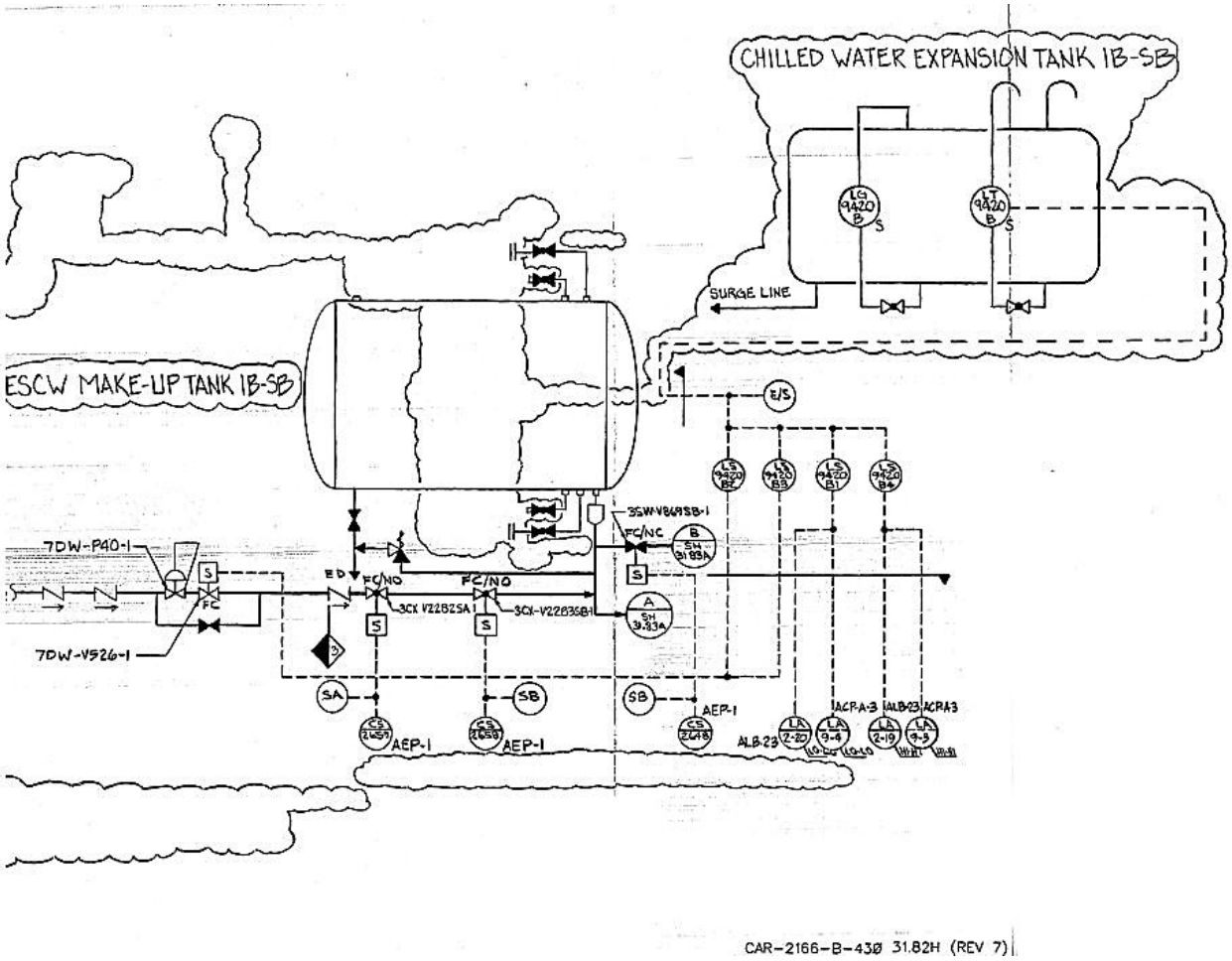


FIGURE 7.3.1-21

RAB SWITCHGEAR ROOMS LOGIC AND SCHEMATIC DIAGRAMS

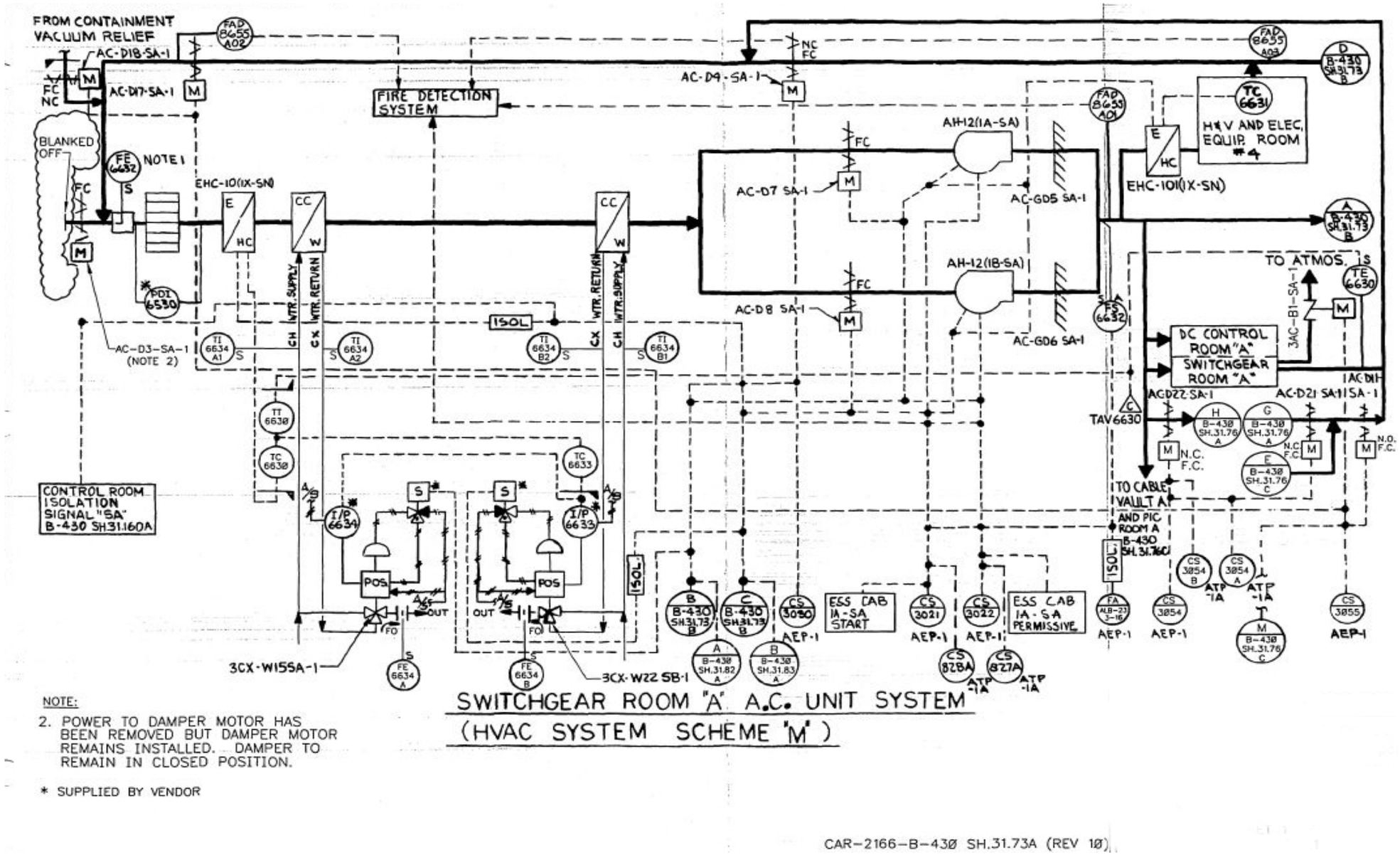


FIGURE 7.3.1-22

FHB SPENT FUEL POOL PUMP ROOM VENTILATION SYSTEM – LOGIC & SCHEMATIC DIAGRAMS

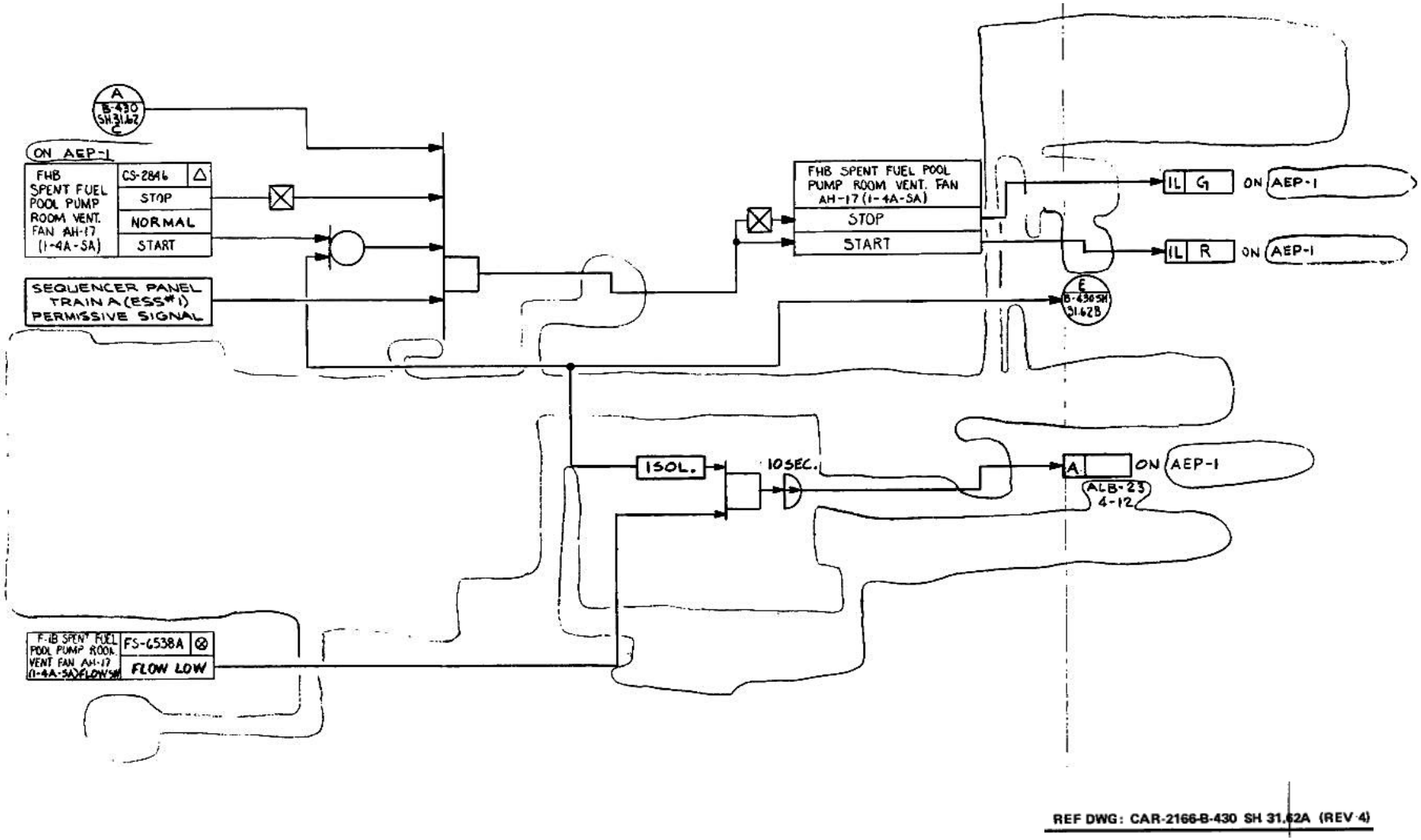


FIGURE 7.3.1-22

FHB SPENT FUEL POOL PUMP ROOM VENTILATION SYSTEM – LOGIC & SCHEMATIC DIAGRAMS (Continued)

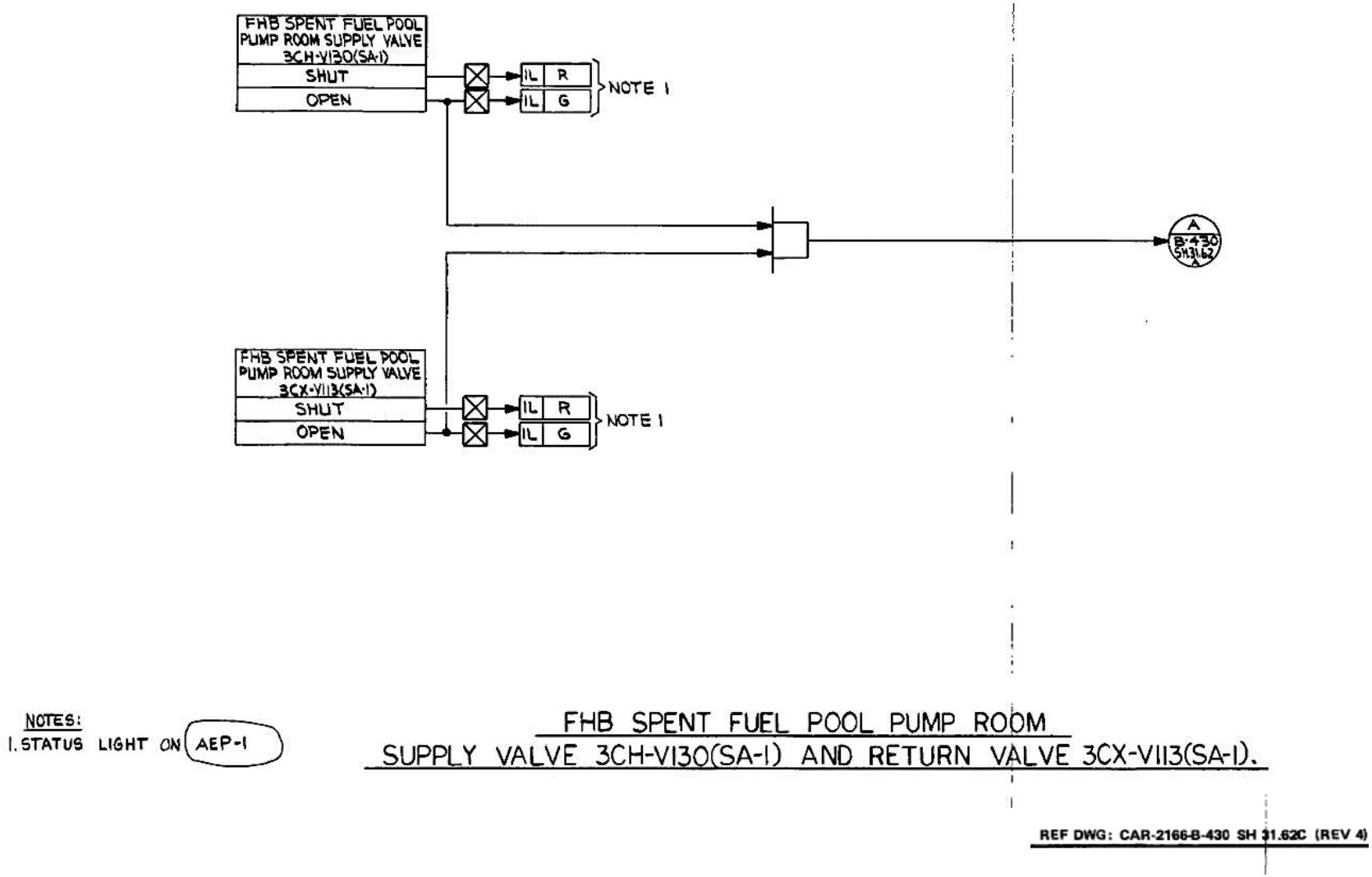


FIGURE 7.3.1-22

FHB SPENT FUEL POOL PUMP ROOM VENTILATION SYSTEM – LOGIC & SCHEMATIC DIAGRAMS (Continued)

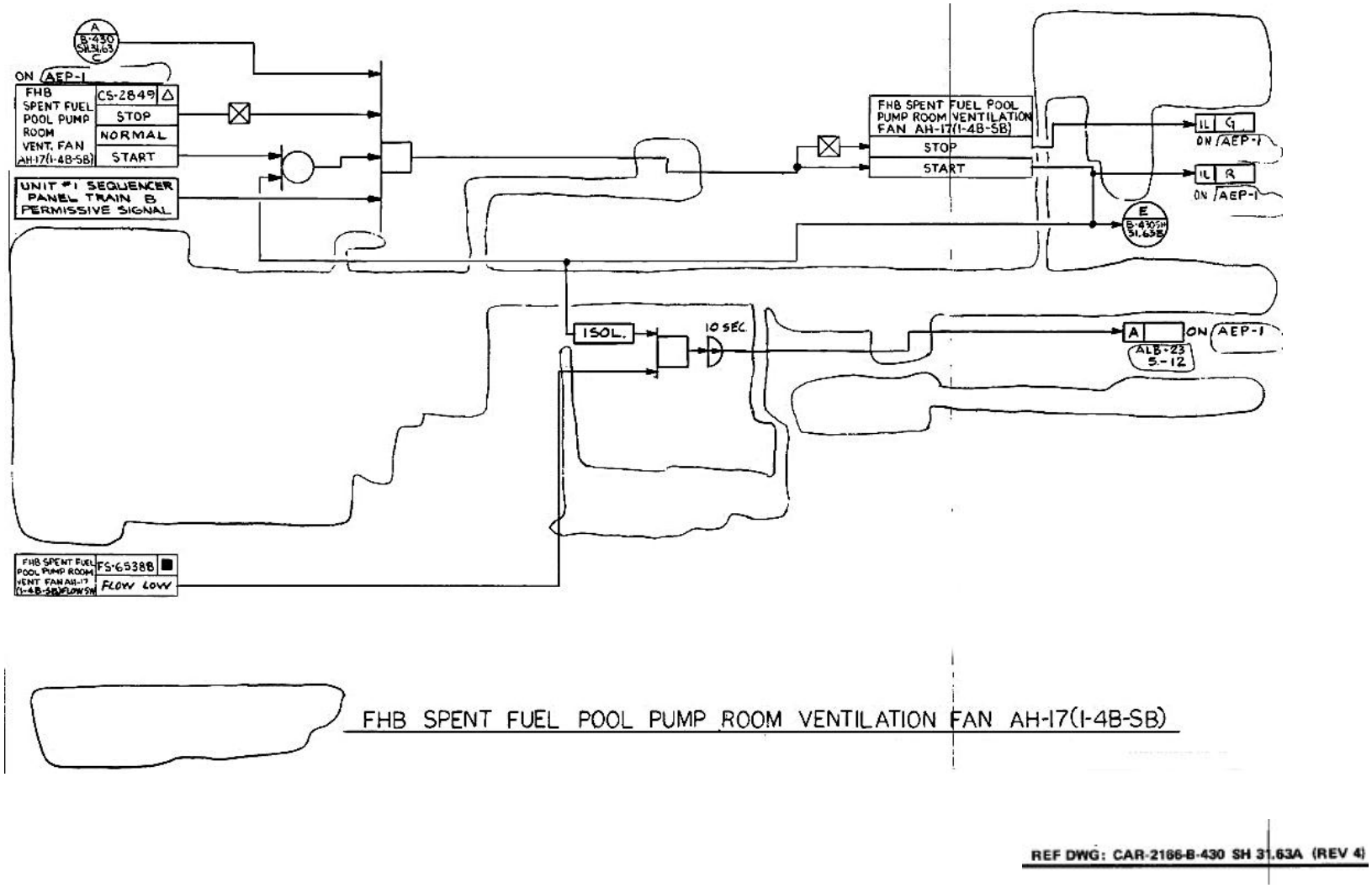


FIGURE 7.3.1-23

CONTAINMENT VACUUM RELIEF SYSTEM – LOGIC & SCHEMATIC DIAGRAMS

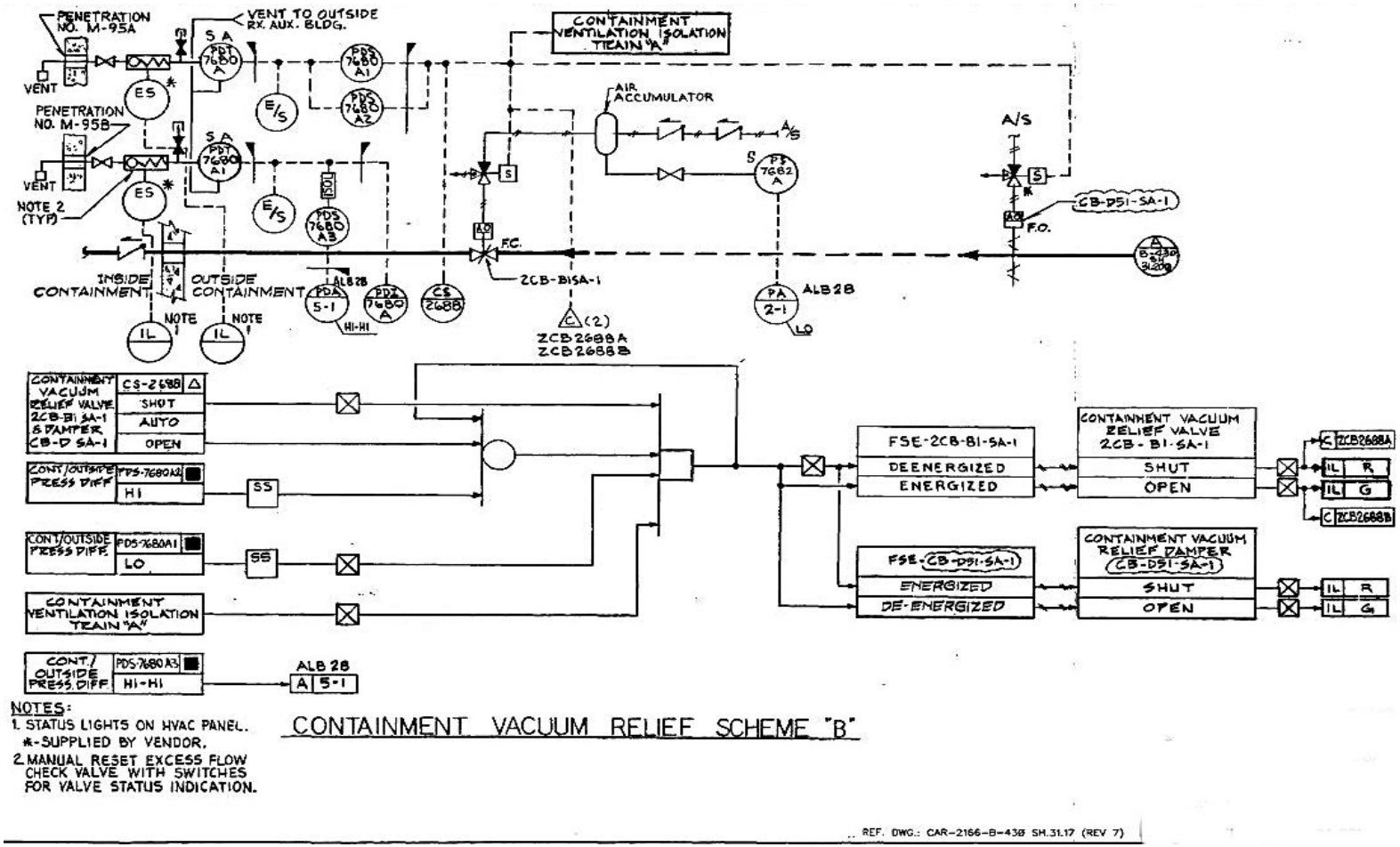


FIGURE 7.3.1-23

CONTAINMENT VACUUM RELIEF SYSTEM – LOGIC & SCHEMATIC DIAGRAMS (Continued)

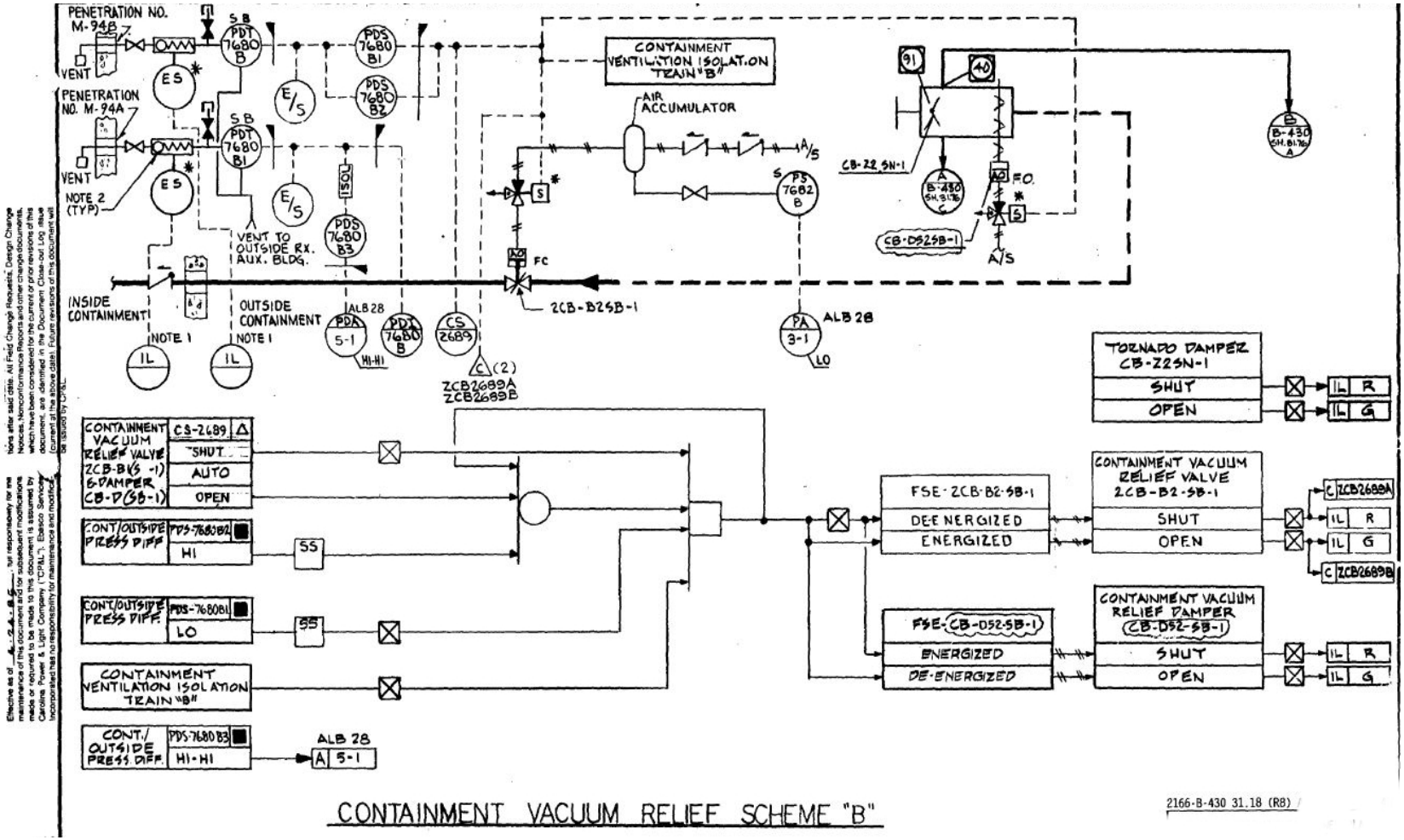


FIGURE 7.3.2-1

TYPICAL ENGINEERED SAFETY FEATURES TEST CIRCUITS

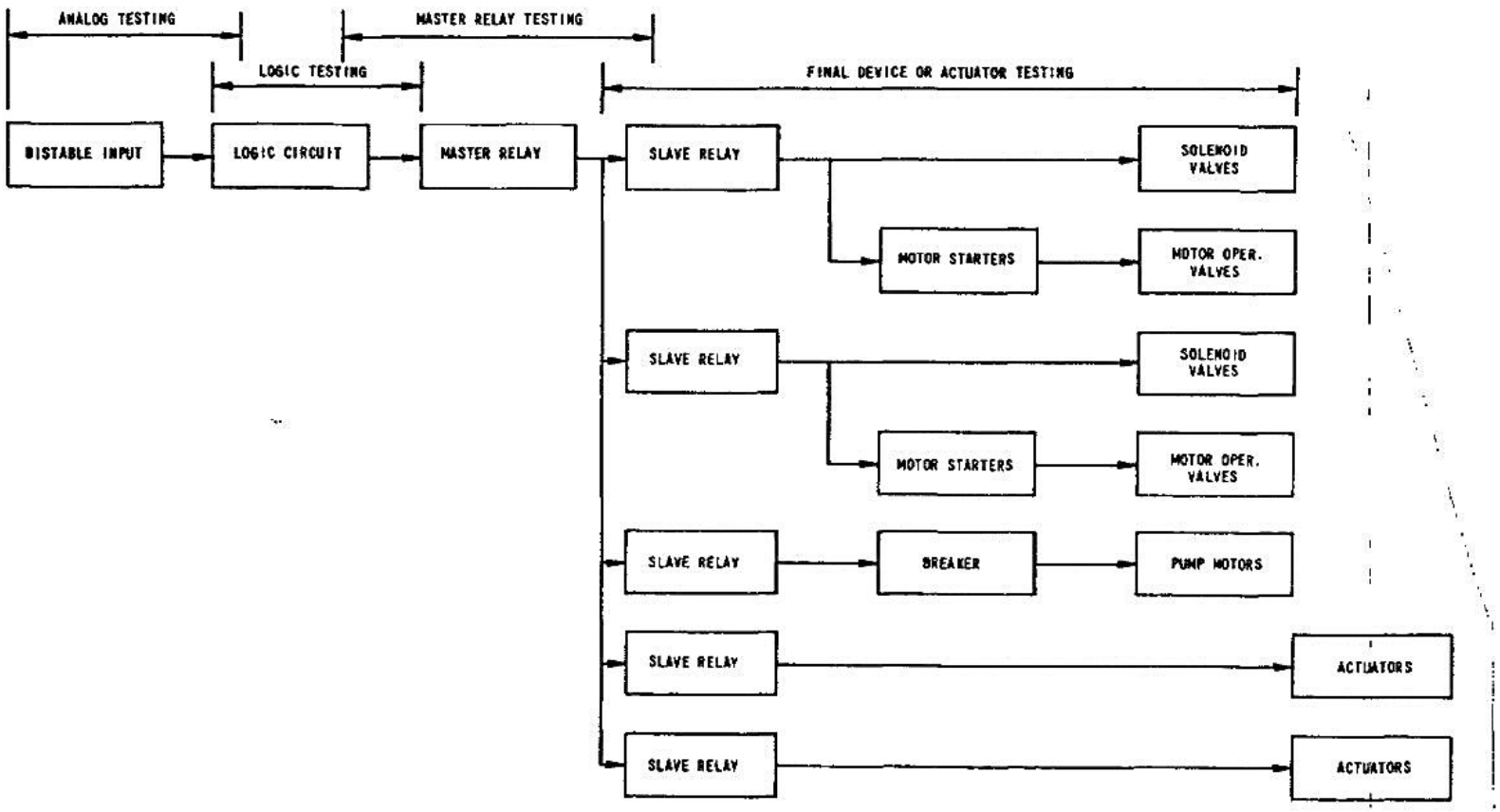


FIGURE 7.3.2-2

ENGINEERED SAFETY FEATURES TEST CABINET – INDEX, NOTES & LEGEND

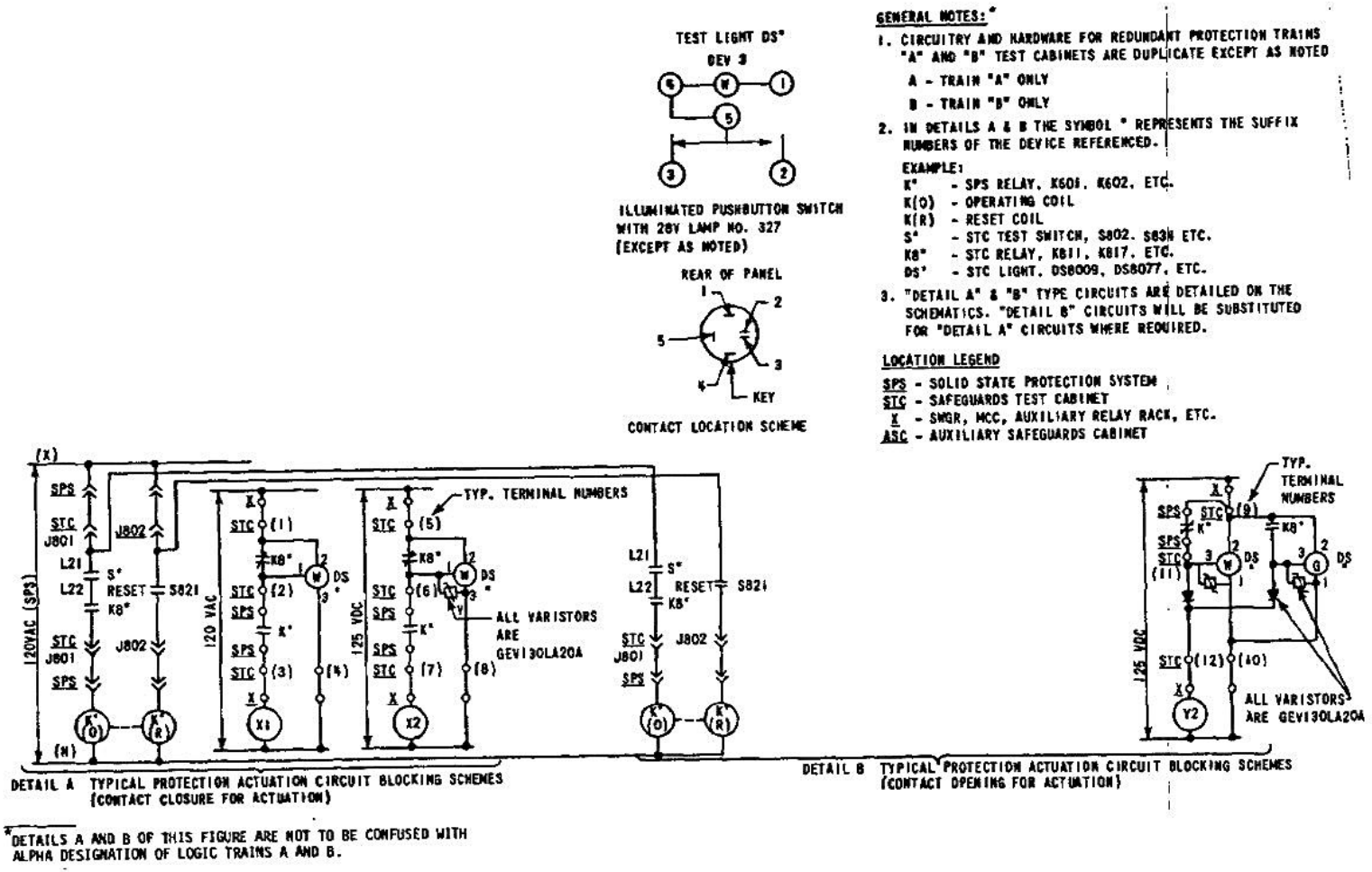


FIGURE 7.4.1-1

LOGIC DIAGRAM FOR BORIC ACID TRANSFER PUMPS

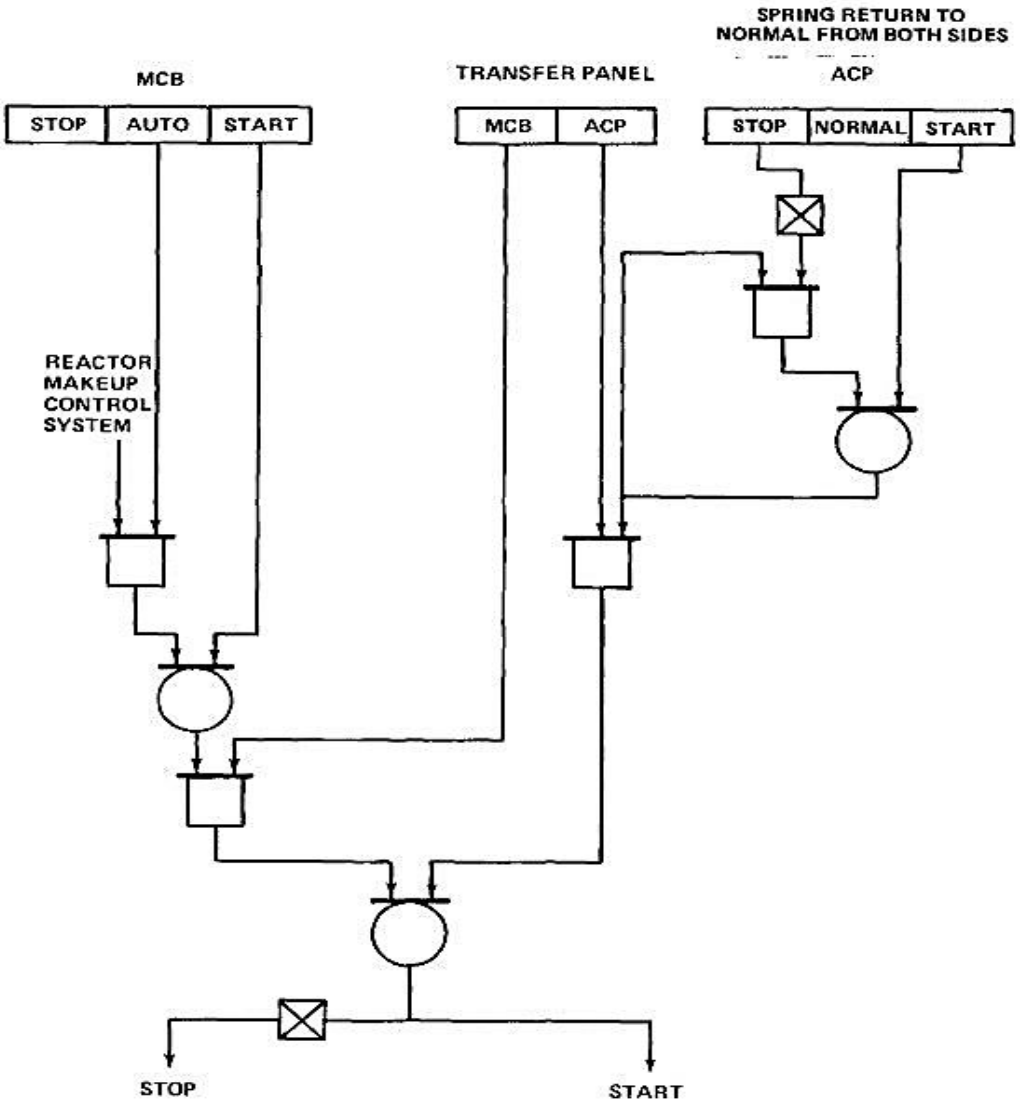


FIGURE 7.4.1-2

LOGIC DIAGRAM FOR CENTRIFUGAL CHARGING PUMPS

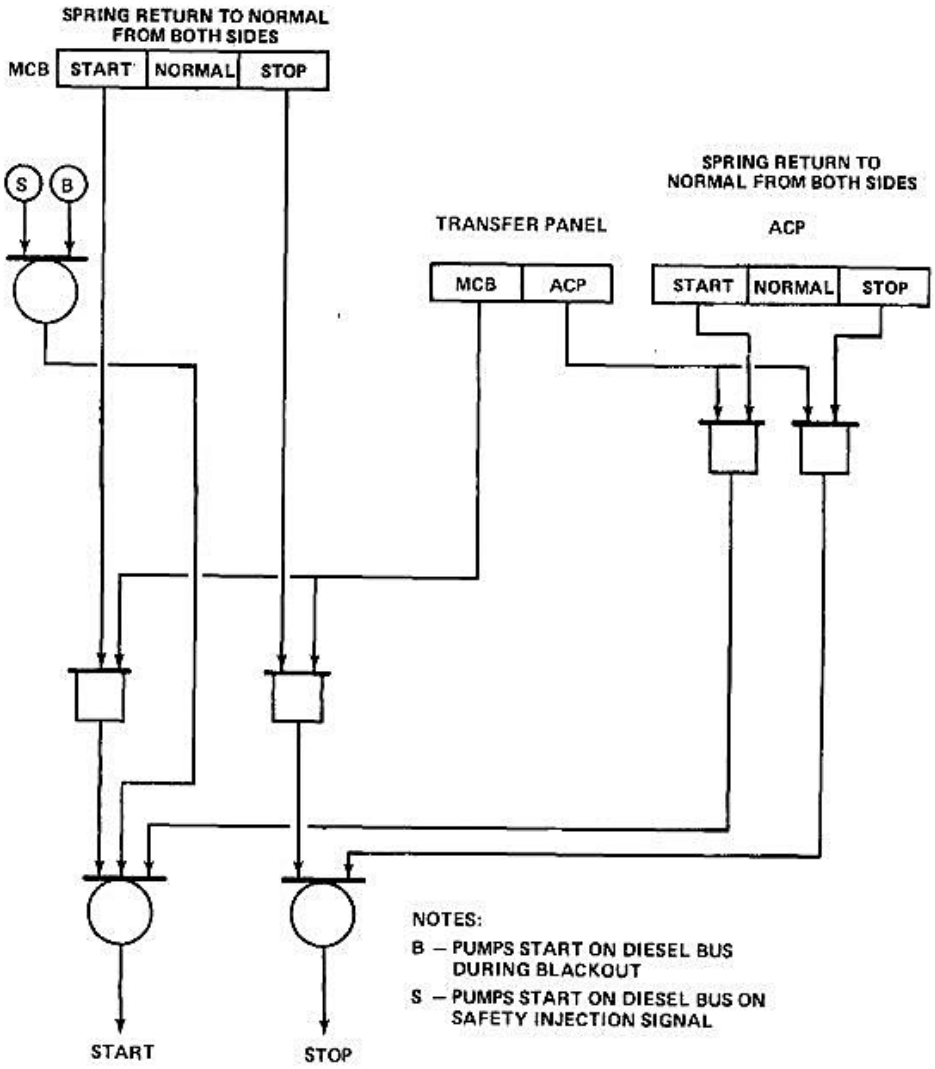


FIGURE 7.4.1-3

LOGIC DIAGRAM FOR LETDOWN ORIFICE ISOLATION VALVES

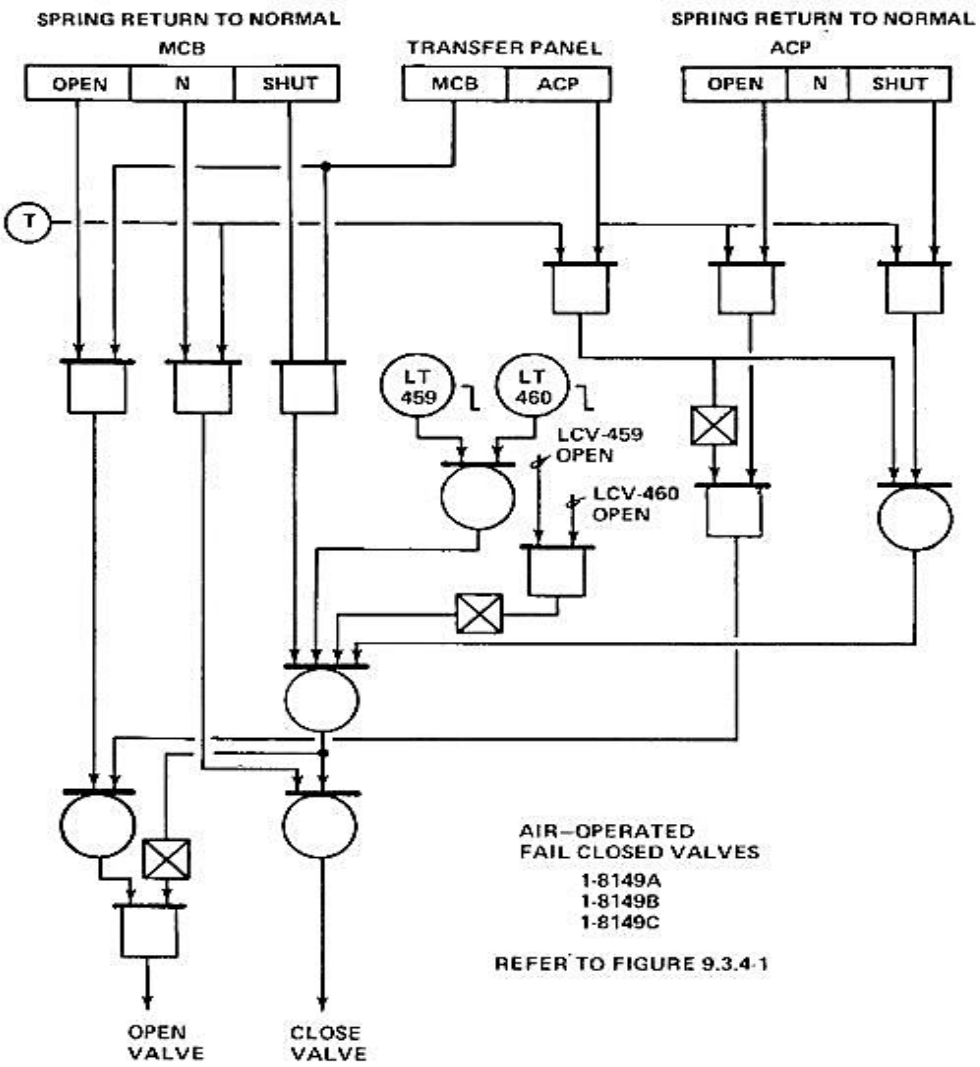


FIGURE 7.4.1-7

LOGIC DIAGRAM FOR RESIDUAL HEAT REMOVAL PUMPS

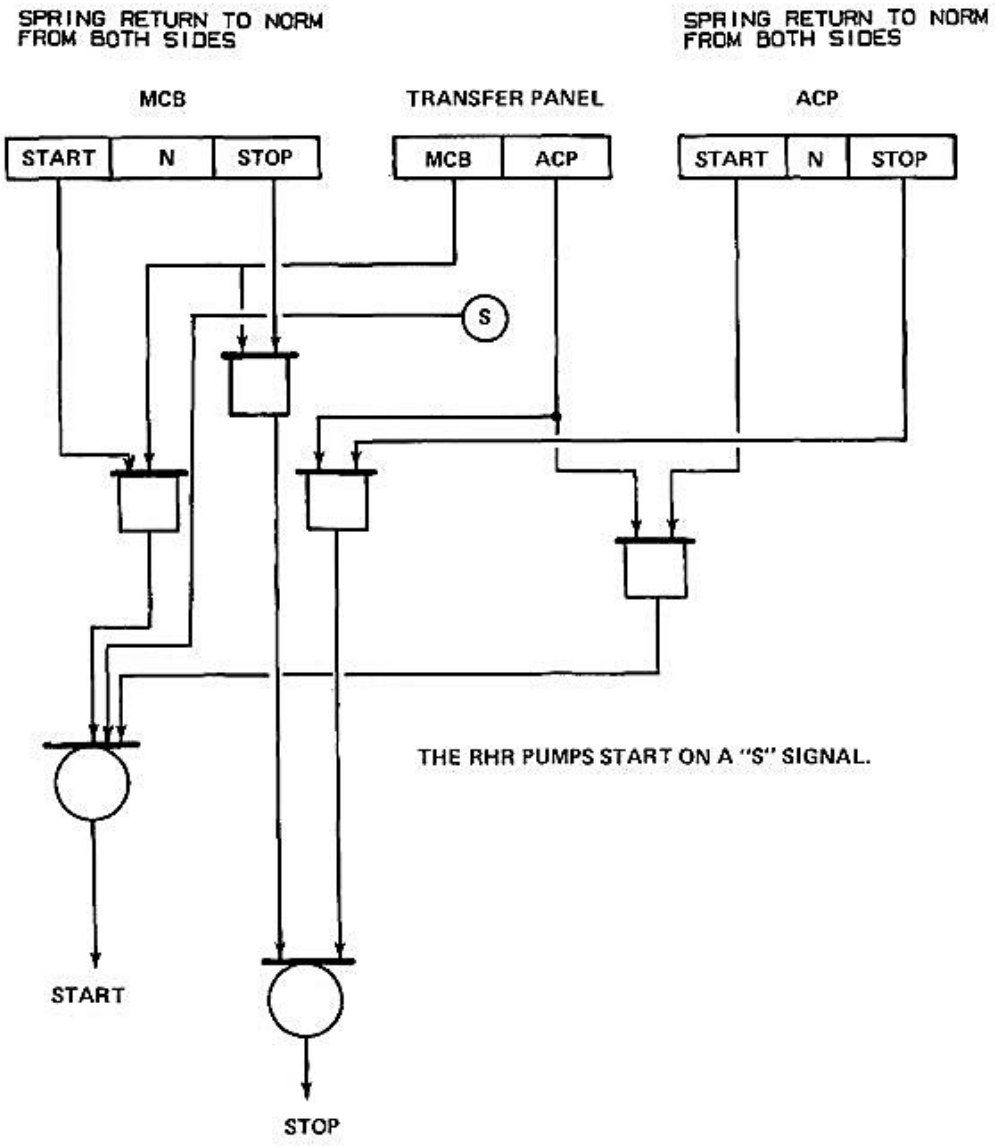


FIGURE 7.5.1-1

PRESSURE, FLOW AND TEMPERATURE TYPICAL PROCESS LOOP DIAGRAM

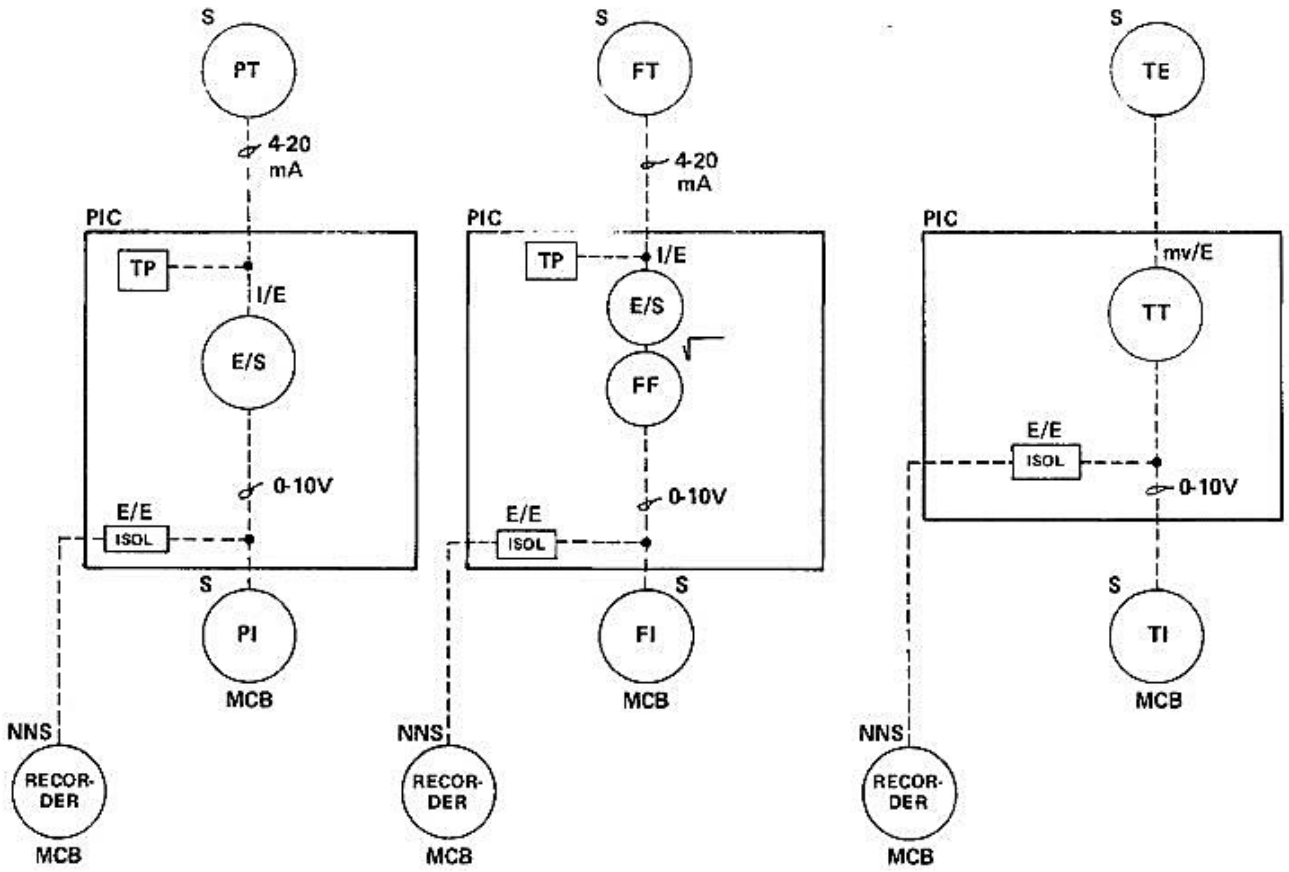


FIGURE 7.5.1-3

ESF BYPASS PANEL TYPICAL WIRING DIAGRAM

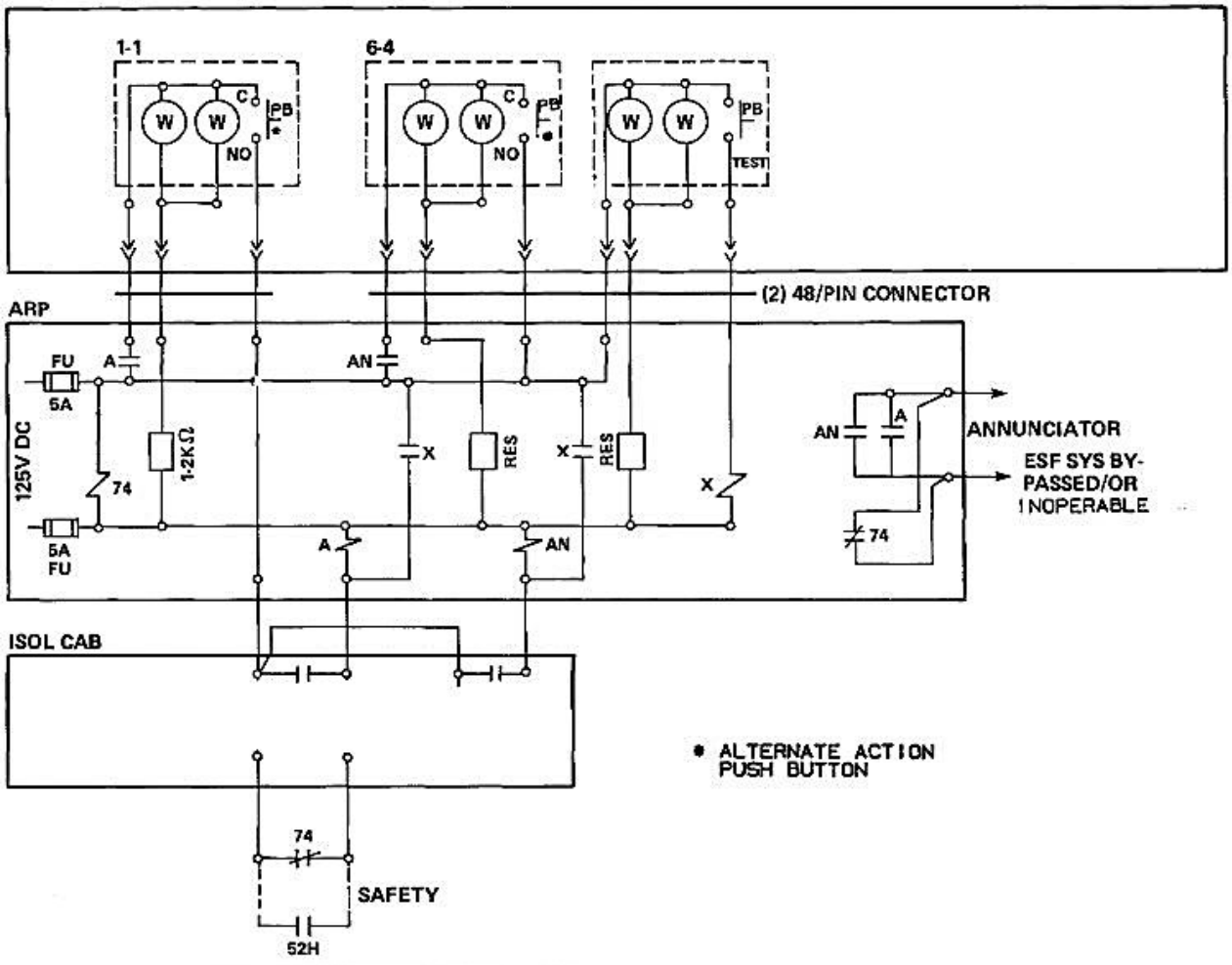


FIGURE 7.5.1-8

STATUS LIGHT BOX TYPICAL WIRING DIAGRAM

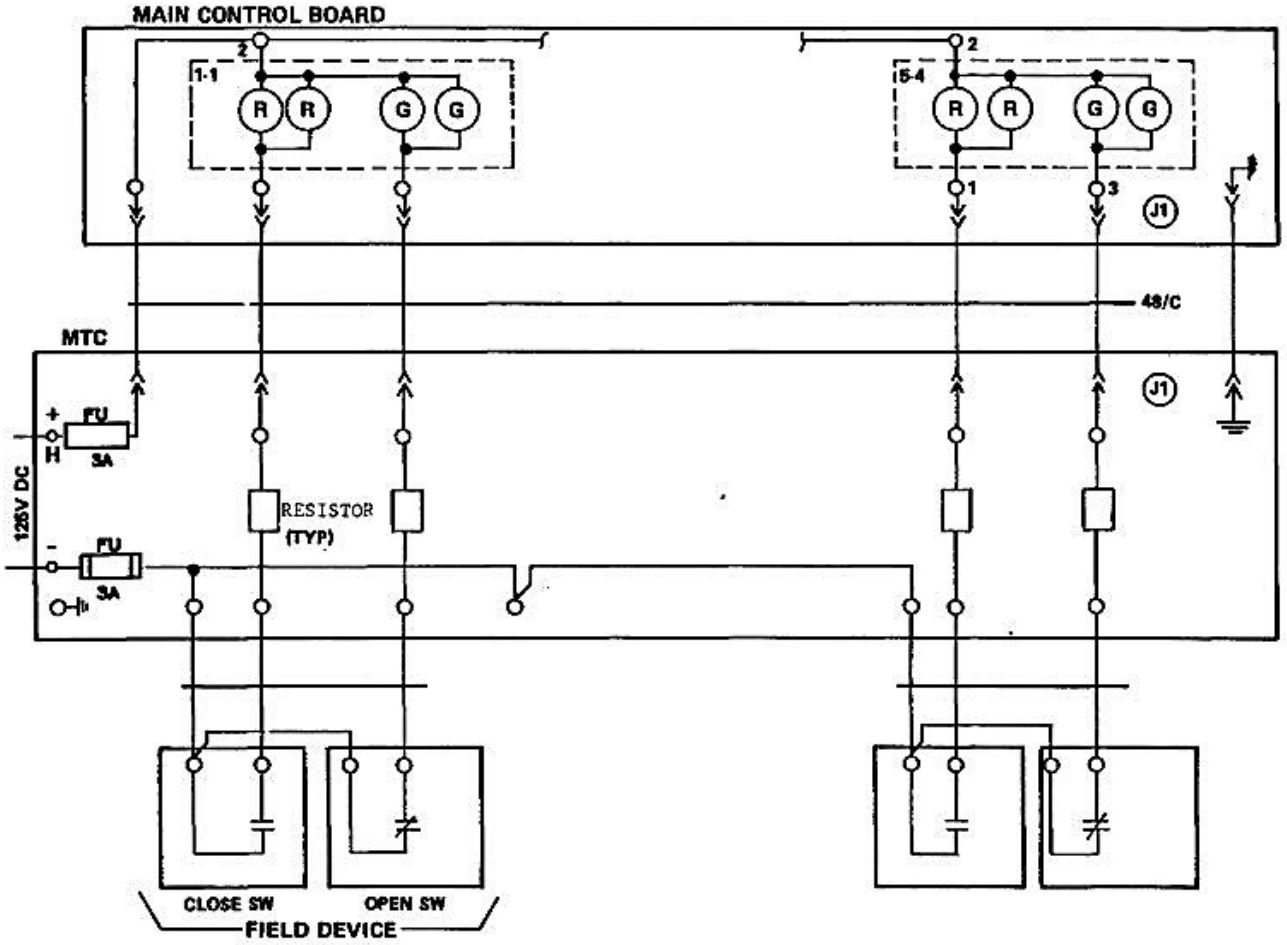


FIGURE 7.5.1-9

SERVICE WATER LEAK DETECTION WINDOW LAYOUT DIAGRAM

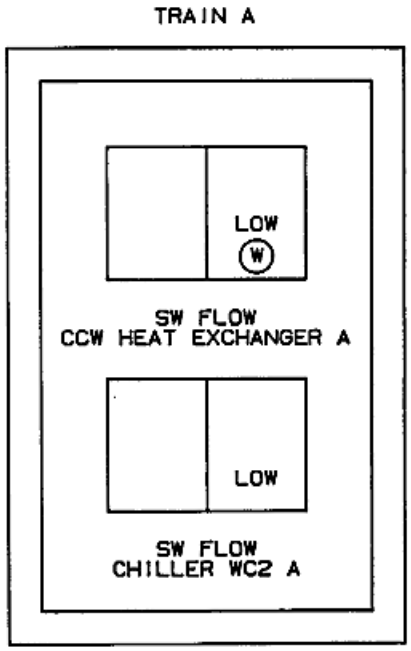


FIGURE 7.5.1-10

SERVICE WATER LEAK DETECTION WINDOW LAYOUT DIAGRAM

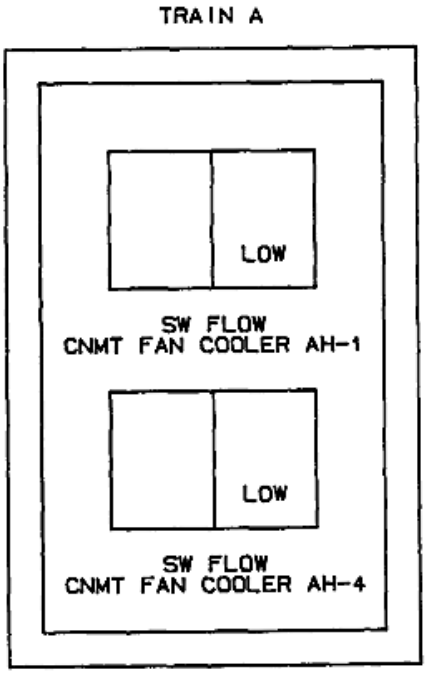


FIGURE 7.5.1-11

SERVICE WATER LEAK DETECTION WINDOW LAYOUT DIAGRAM

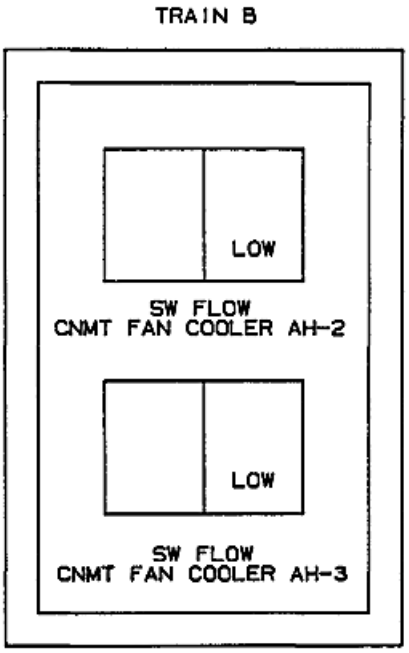


FIGURE 7.5.1-12

SERVICE WATER LEAK DETECTION WINDOW LAYOUT DIAGRAM

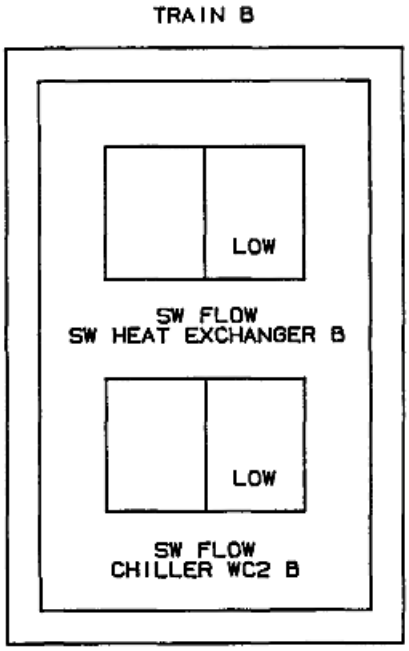


FIGURE 7.5.1-13

SERVICE WATER LEAK DETECTION TYPICAL WIRING DIAGRAM

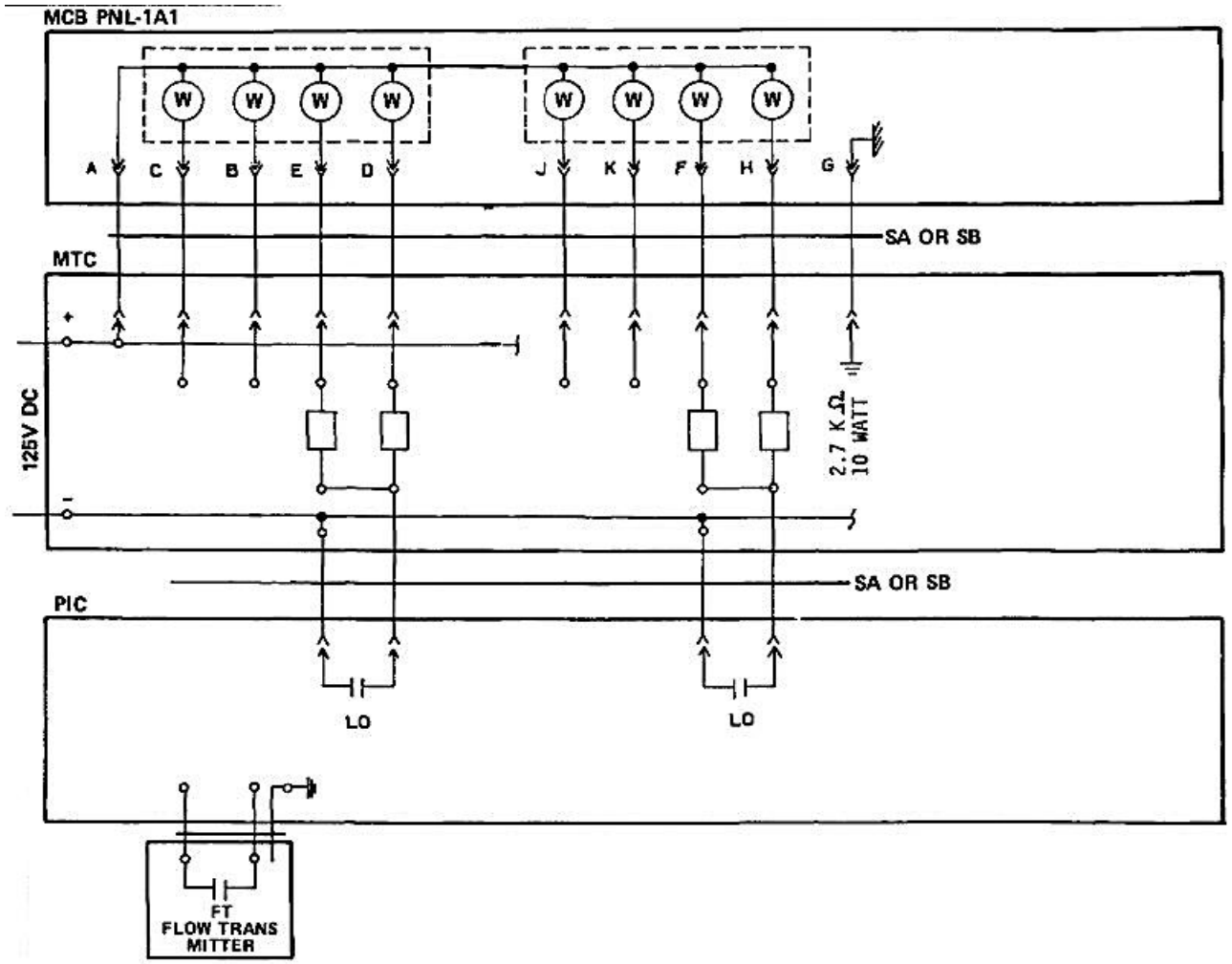
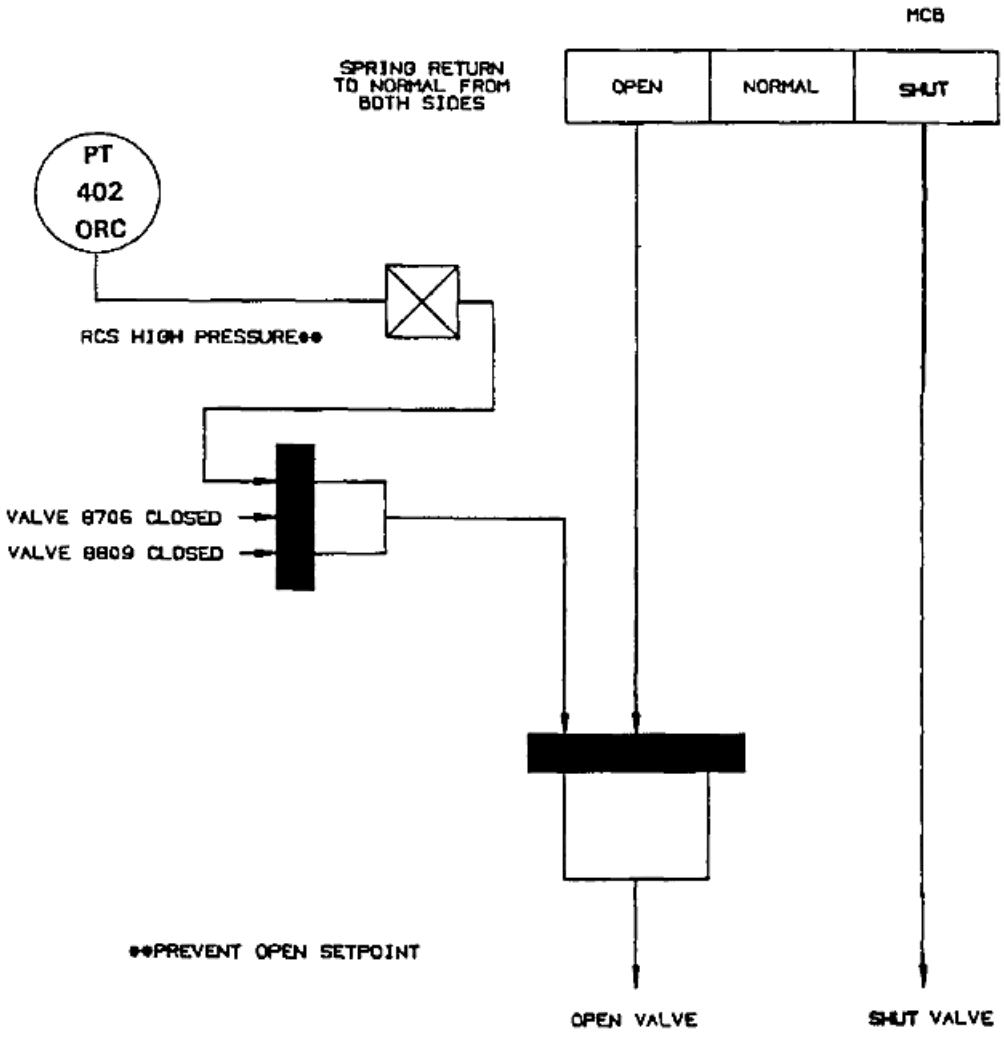


FIGURE 7.6.1-1

RHR SYSTEM ISOLATION VALVES LOGIC DIAGRAM

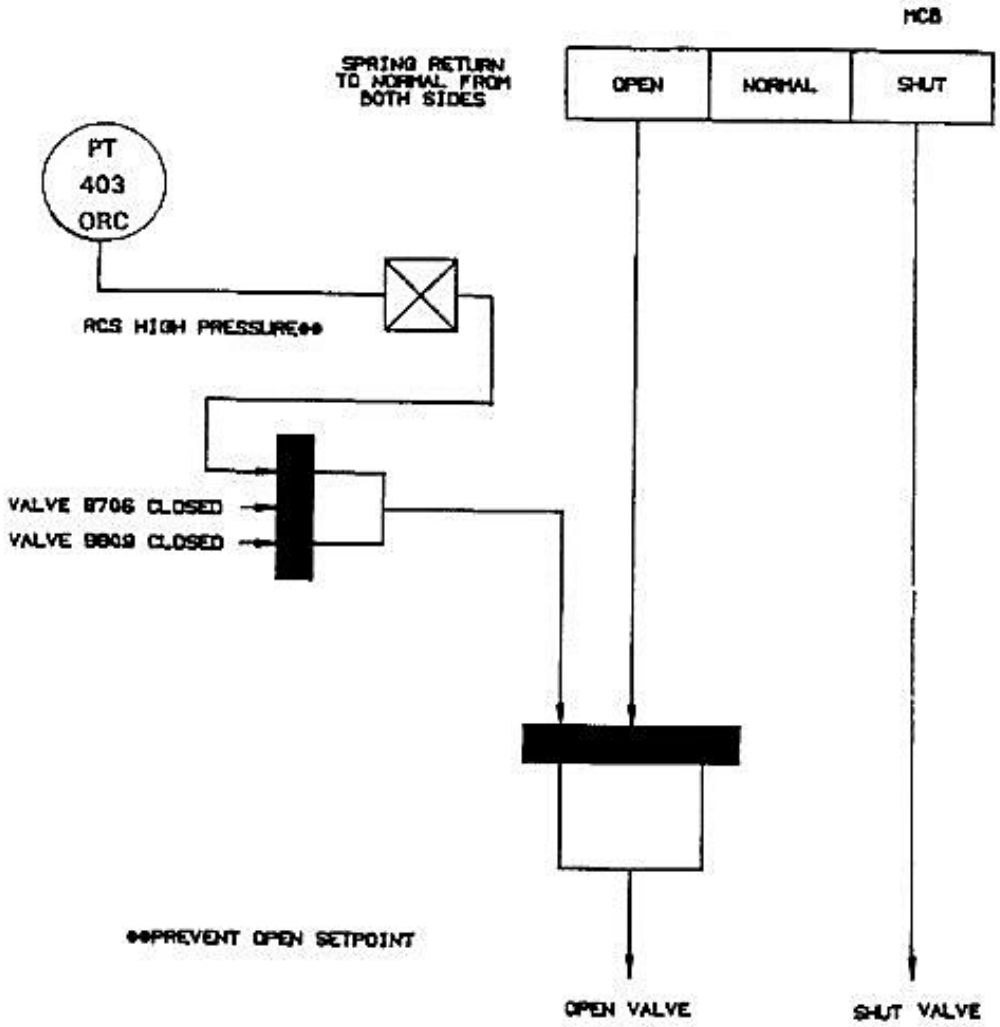


NOTE: LOGIC FOR INNER VALVES 8702A OR 8702B CLOSEST TO RCS IN EACH FLUID SYSTEMS TRAIN IS IDENTICAL

ORC-OUTSIDE REACTOR CONTAINMENT

FIGURE 7.6.1-2

RHR SYSTEM ISOLATION VALVES LOGIC DIAGRAM



NOTE: LOGIC FOR OUTER VALVES 8701A OR 8701B CLOSEST TO RHR IN EACH FLUID SYSTEMS TRAIN IS IDENTICAL
ORC-OUTSIDE REACTOR CONTAINMENT

FIGURE 7.6.1-3

ACCUMULATOR DISCHARGE VALVES CONTROL CIRCUIT LOGIC DIAGRAM

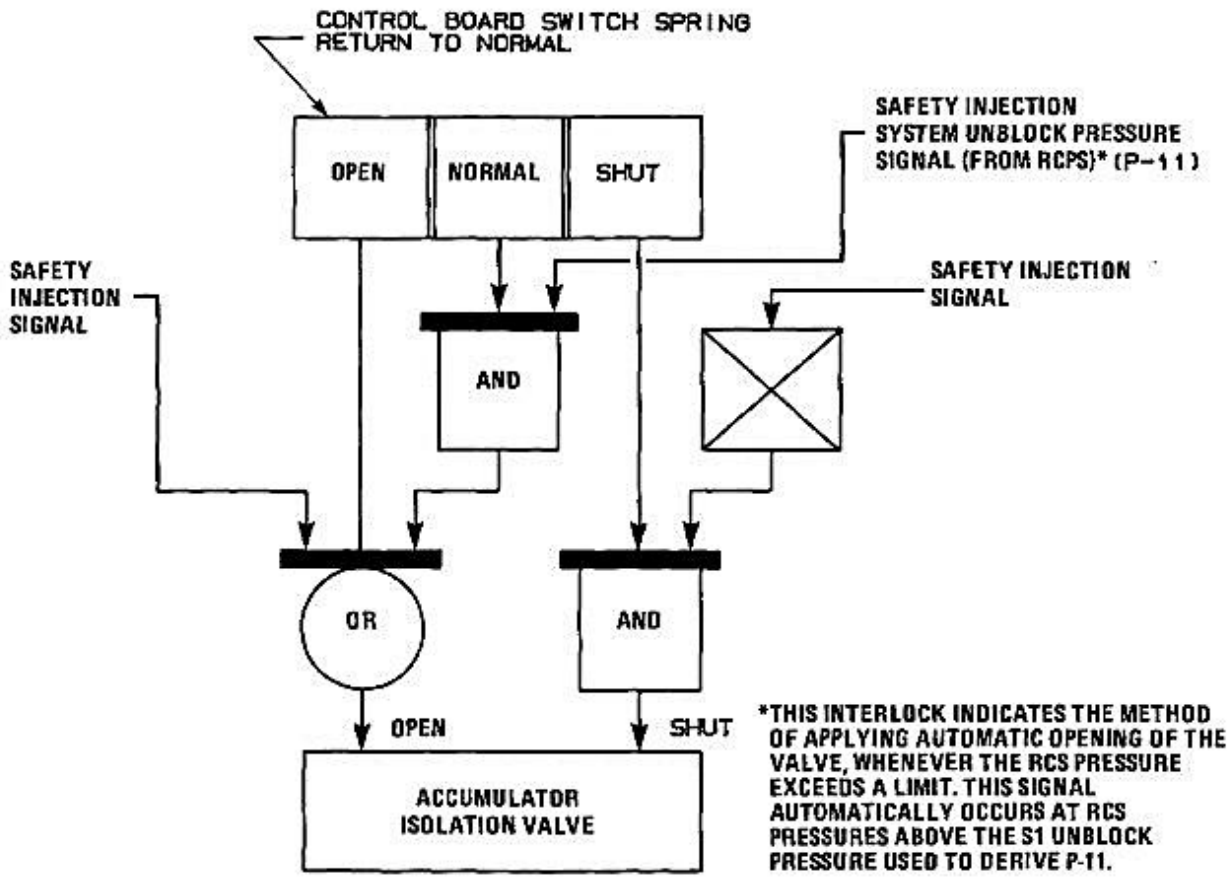


FIGURE 7.6.1-4

INSTRUMENTATION AND CONTROL POWER SUPPLY SYSTEM

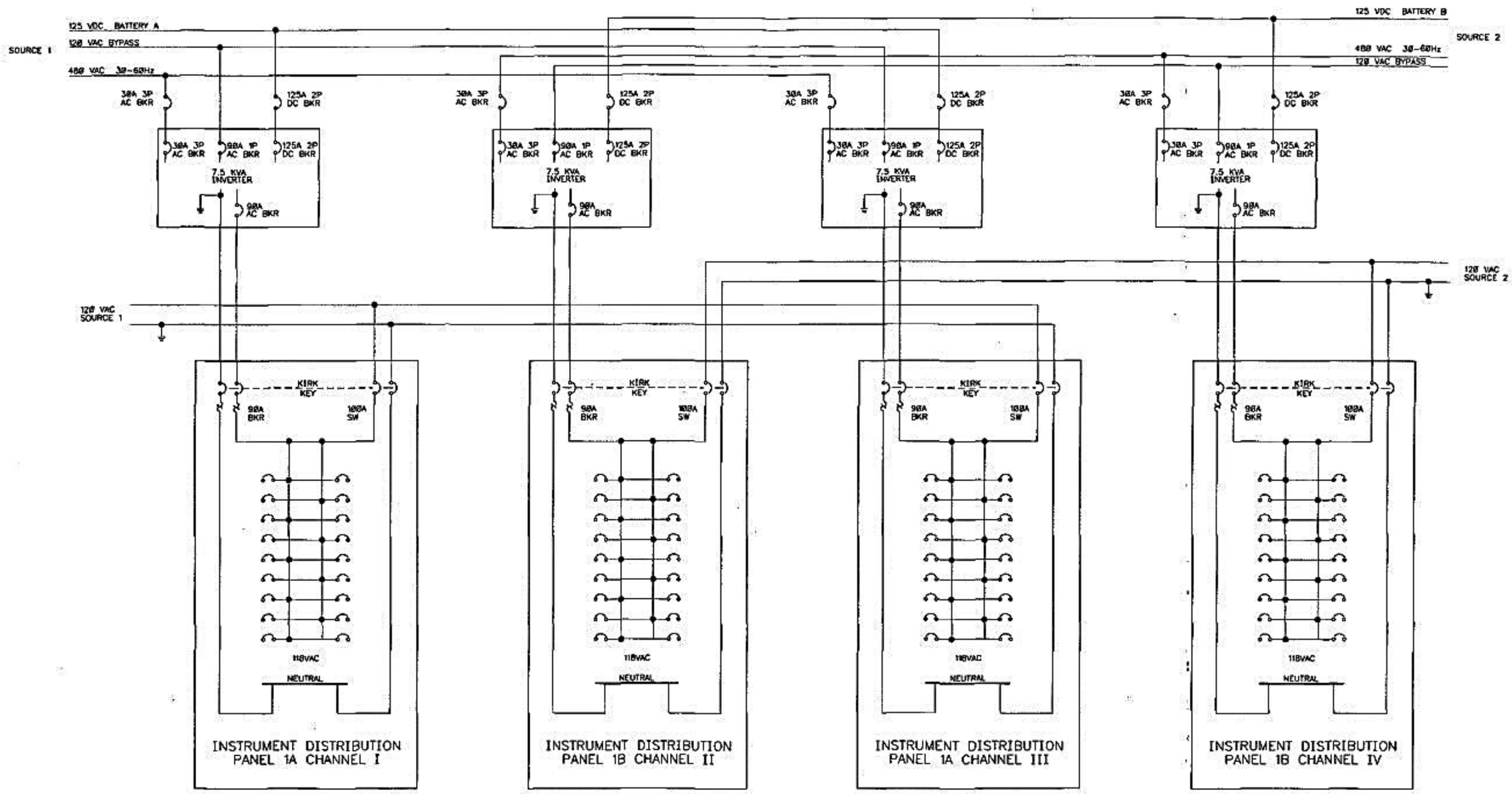
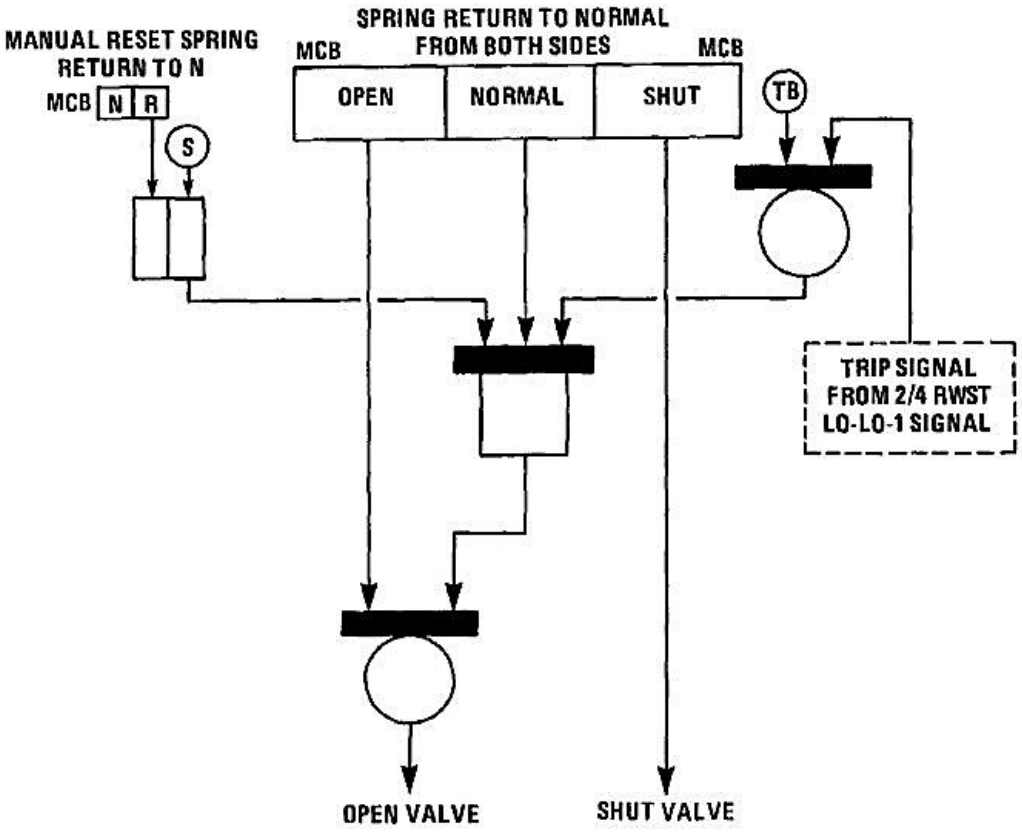


FIGURE 7.6.1-5

RHR RECIRCULATION SYSTEM LOGIC DIAGRAM



APPLICABLE VALVES	
DESCRIPTION	VALVE NO.
SUMP TO NUMBER 1 RHR PUMP	8811A 8812A
SUMP TO NUMBER 2 RHR PUMP	8811B 8812B

FIGURE 7.6.1-6

RHR RECIRCULATION SYSTEM LOGIC DIAGRAM

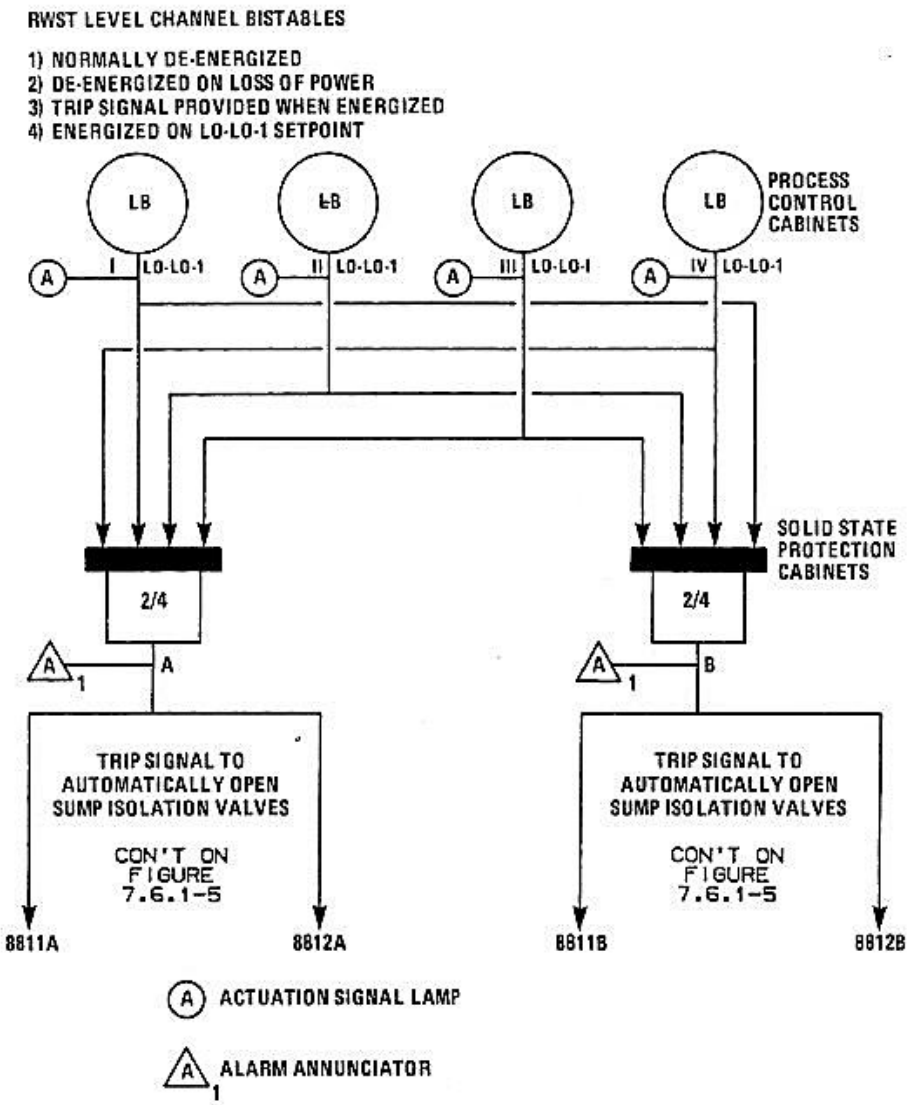


FIGURE 7.6.1-7

RCS PRESSURE CONTROL LOGIC DIAGRAM

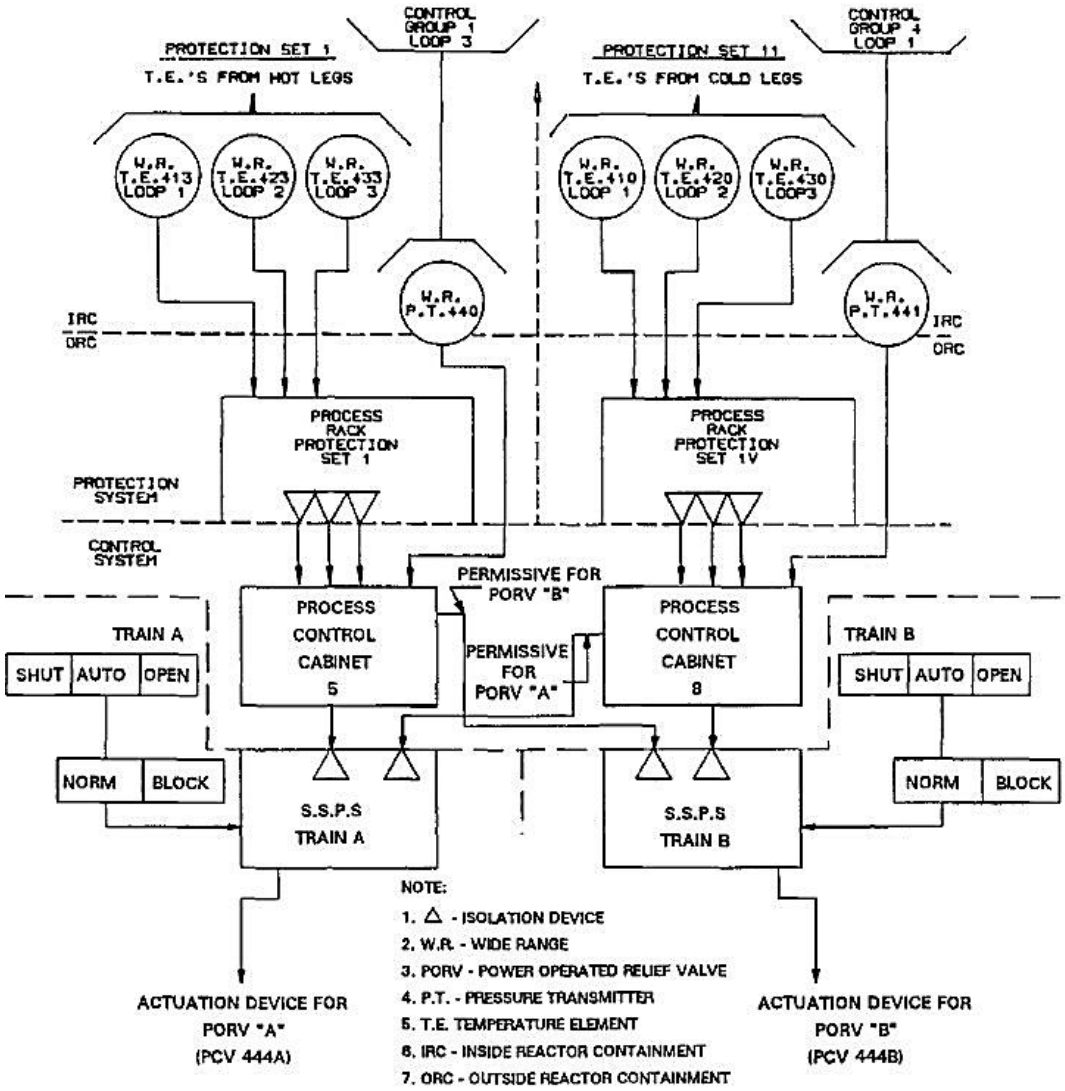


FIGURE 7.6.1-8

FHB FUEL POOLS A & B LOGIC AND SCHEMATIC DIAGRAMS

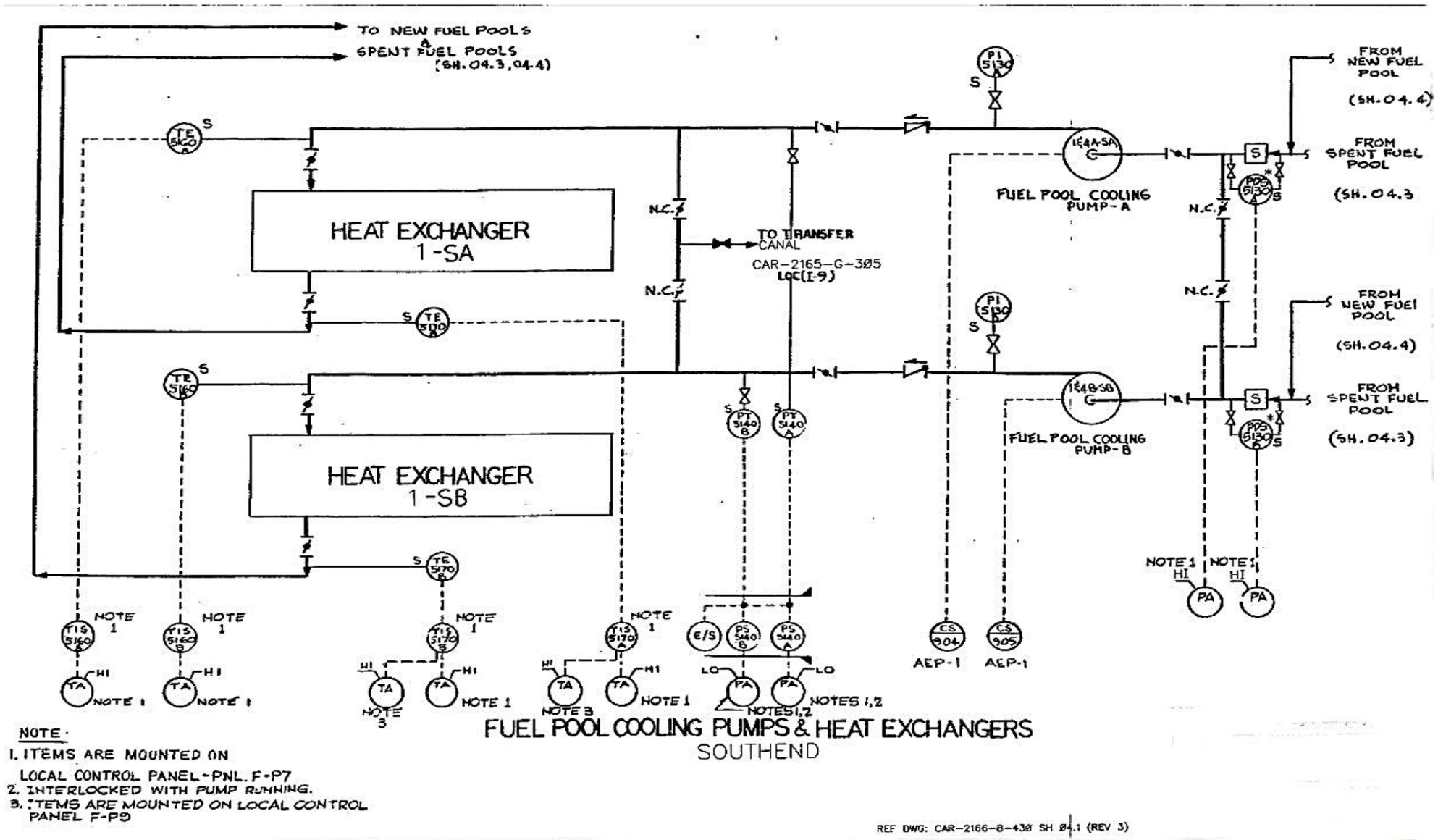
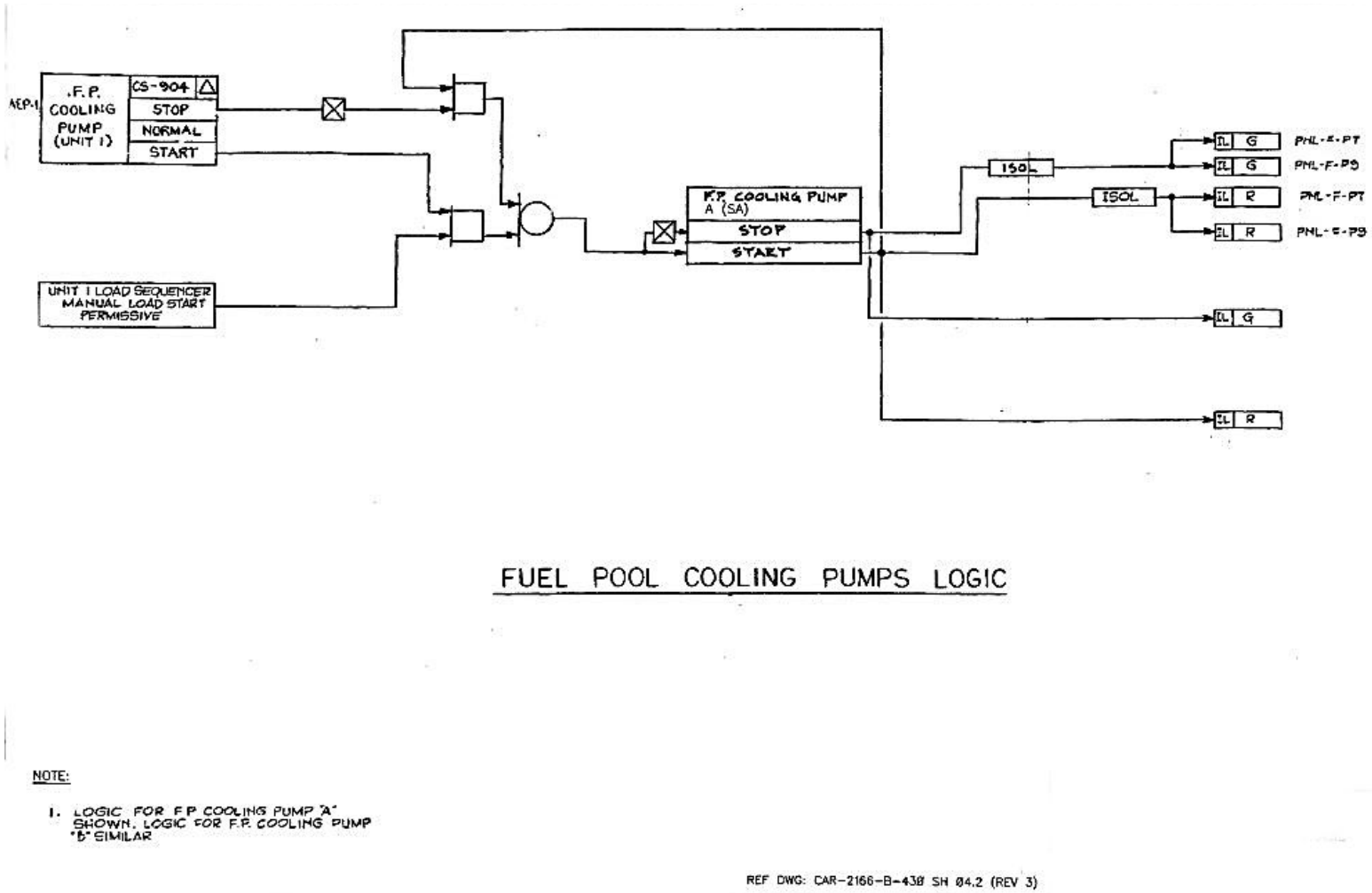

TO NEW FUEL POOLS & SPENT FUEL POOLS (SH. 04.3, 04.4)
HEAT EXCHANGER 1-SA
HEAT EXCHANGER 1-SB
TO TRANSFER CANAL
CAR-2165-G-305
LOC(I-9)
FUEL POOL COOLING PUMP-A
FUEL POOL COOLING PUMP-B
FROM NEW FUEL POOL (SH. 04.4)
FROM SPENT FUEL POOL (SH. 04.3)
FROM NEW FUEL POOL (SH. 04.4)
FROM SPENT FUEL POOL (SH. 04.3)
AEP-1
AEP-1
NOTES 1,2
NOTE 3
NOTE 1
NOTE 1
NOTE 1

FIGURE 7.6.1-9

FHB FUEL POOLS A & B LOGIC AND SCHEMATIC DIAGRAMS



NOTE:

1. LOGIC FOR F.P. COOLING PUMP "A" SHOWN. LOGIC FOR F.P. COOLING PUMP "B" SIMILAR

REF DWG: CAR-2166-B-430 SH 04.2 (REV 3)

FIGURE 7.7.1-1

SIMPLIFIED BLOCK DIAGRAM OF REACTOR CONTROL ROD SYSTEM

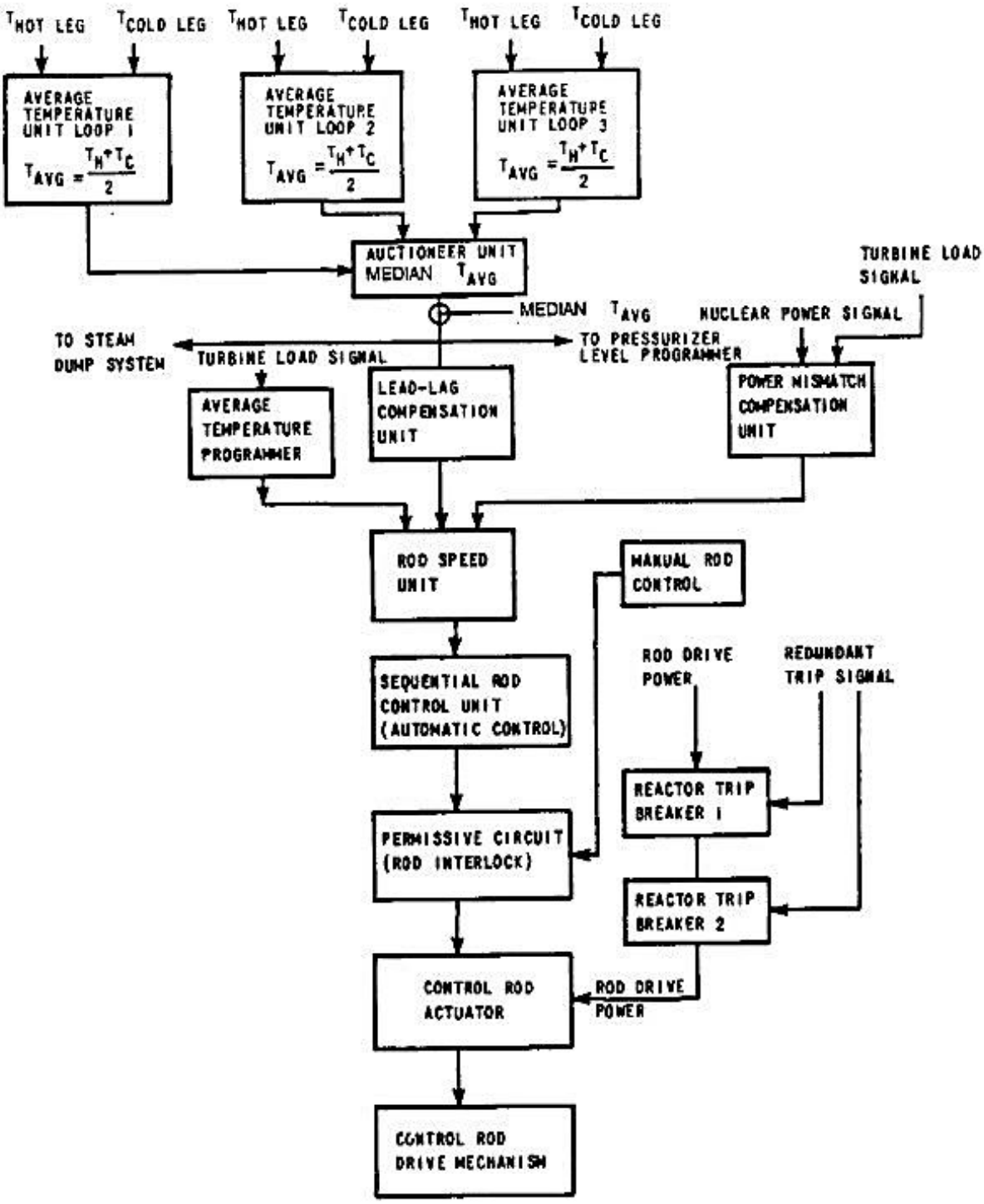
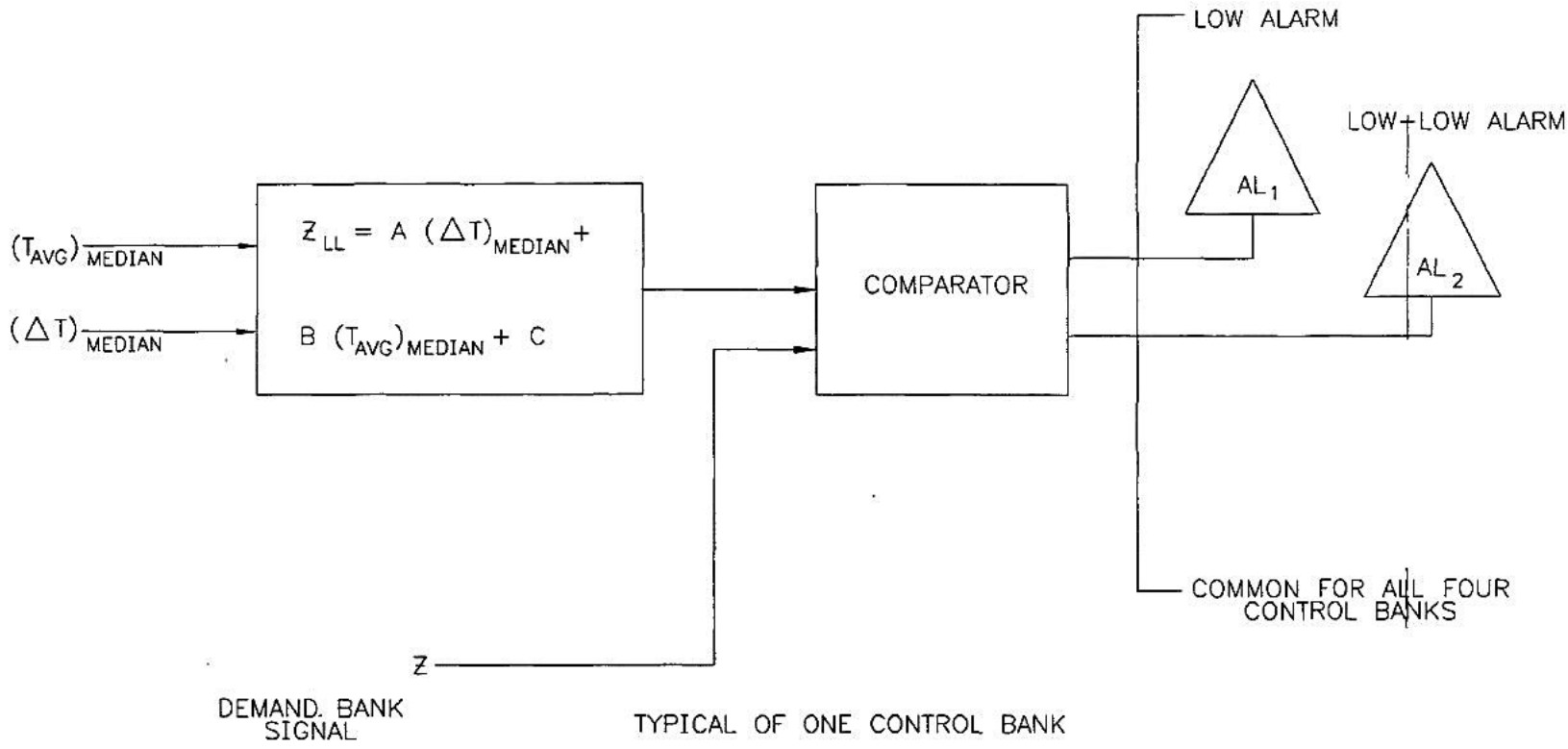


FIGURE 7.7.1-2

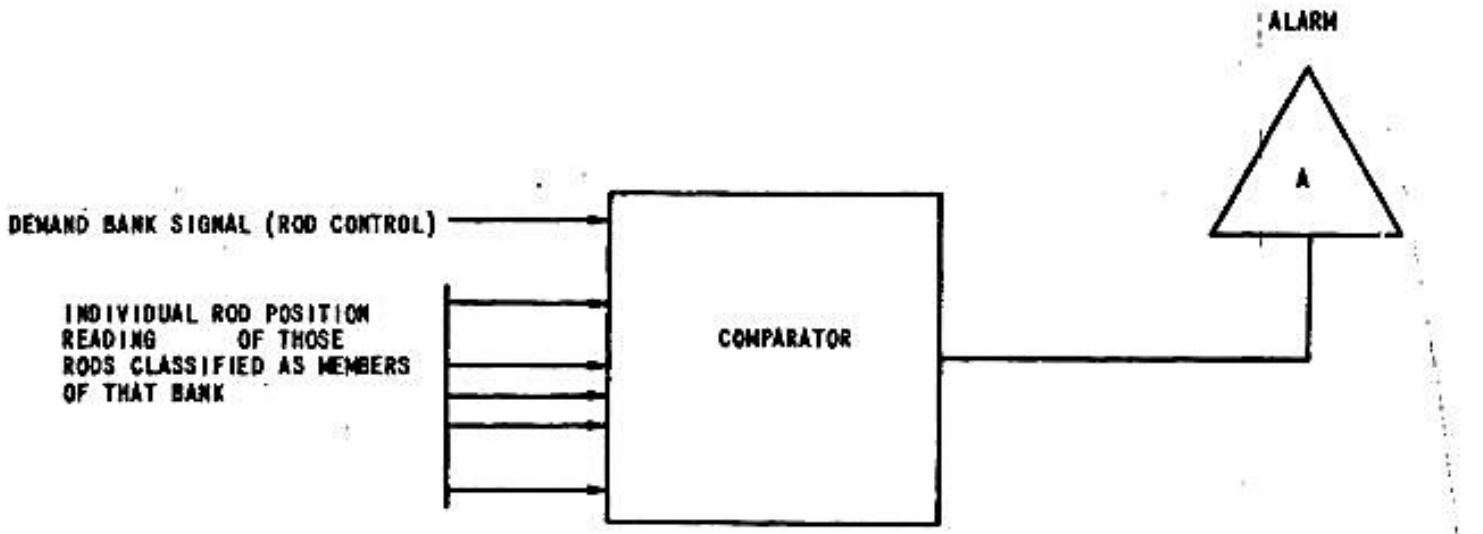
CONTROL BANK ROD INSERTION MONITOR



NOTE: 1. ANALOG CIRCUITRY IS USED FOR THE COMPARATOR NETWORK
2. COMPARISON IS DONE FOR ALL CONTROL BANKS

FIGURE 7.7.1-3

ROD DEVIATION COMPARATOR



NOTE:
1. DIGITAL OR ANALOG SIGNALS MAY BE USED FOR THE COMPARATOR COMPUTER INPUTS.
2. THE COMPARATOR WILL ENERGIZE THE ALARM IF THERE EXISTS A POSITION DIFFERENCE GREATER THAN A PRESET LIMIT BETWEEN ANY INDIVIDUAL ROD AND THE DEMAND BANK SIGNAL.
3. COMPARISON IS INDIVIDUALLY DONE FOR ALL CONTROL BANKS.

FIGURE 7.7.1-4

BLOCK DIAGRAM OF PRESSURIZER PRESSURE CONTROL SYSTEM

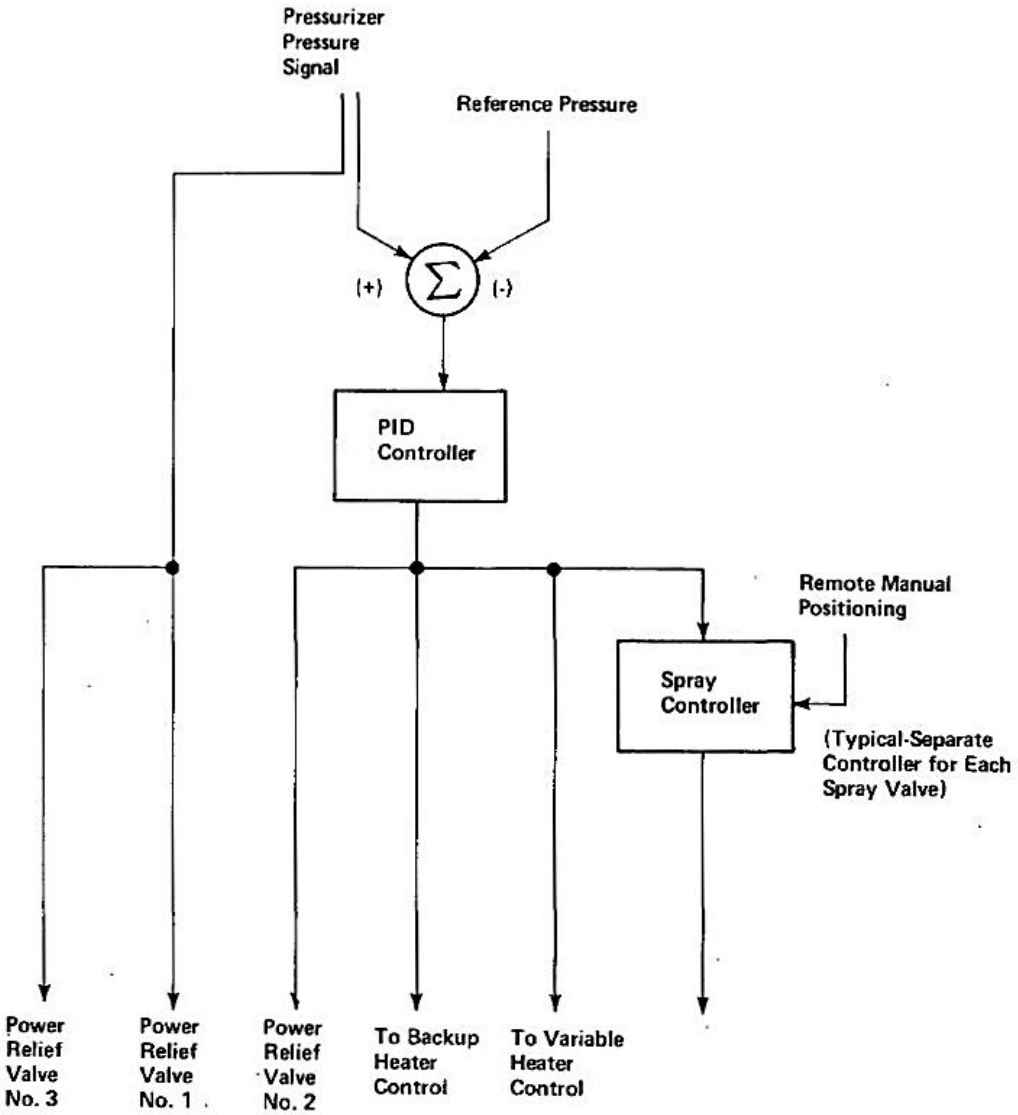


FIGURE 7.7.1-5

BLOCK DIAGRAM OF PRESSURIZER LEVEL CONTROL SYSTEM

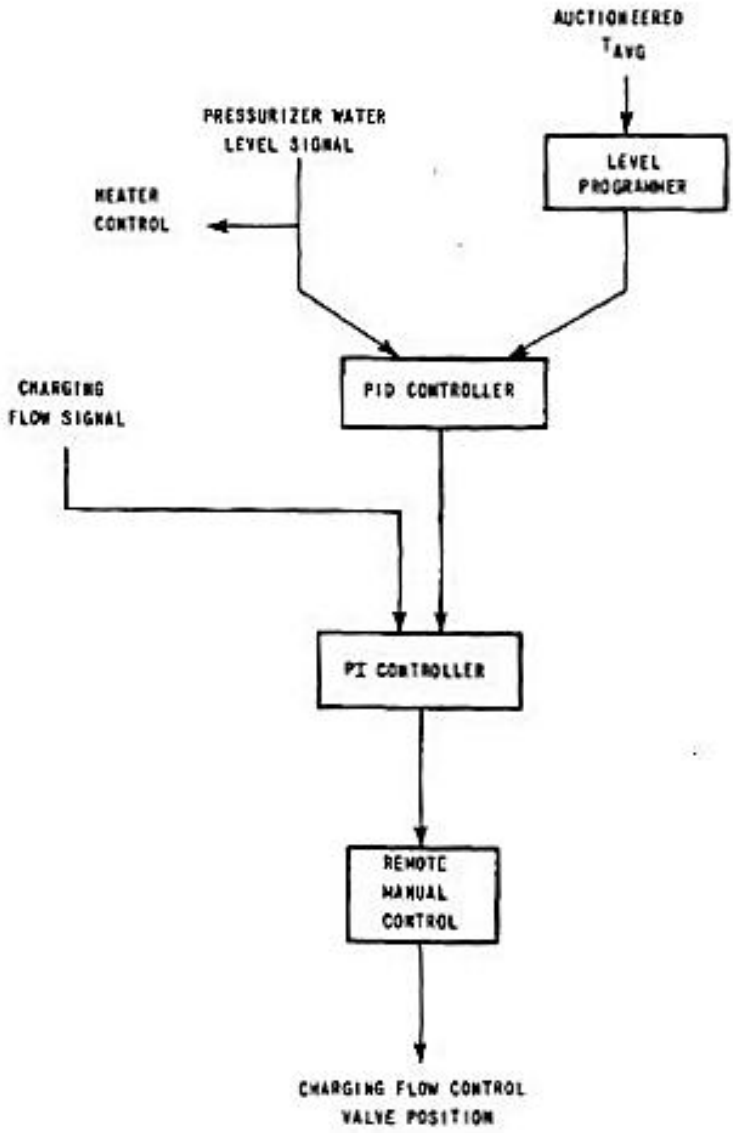
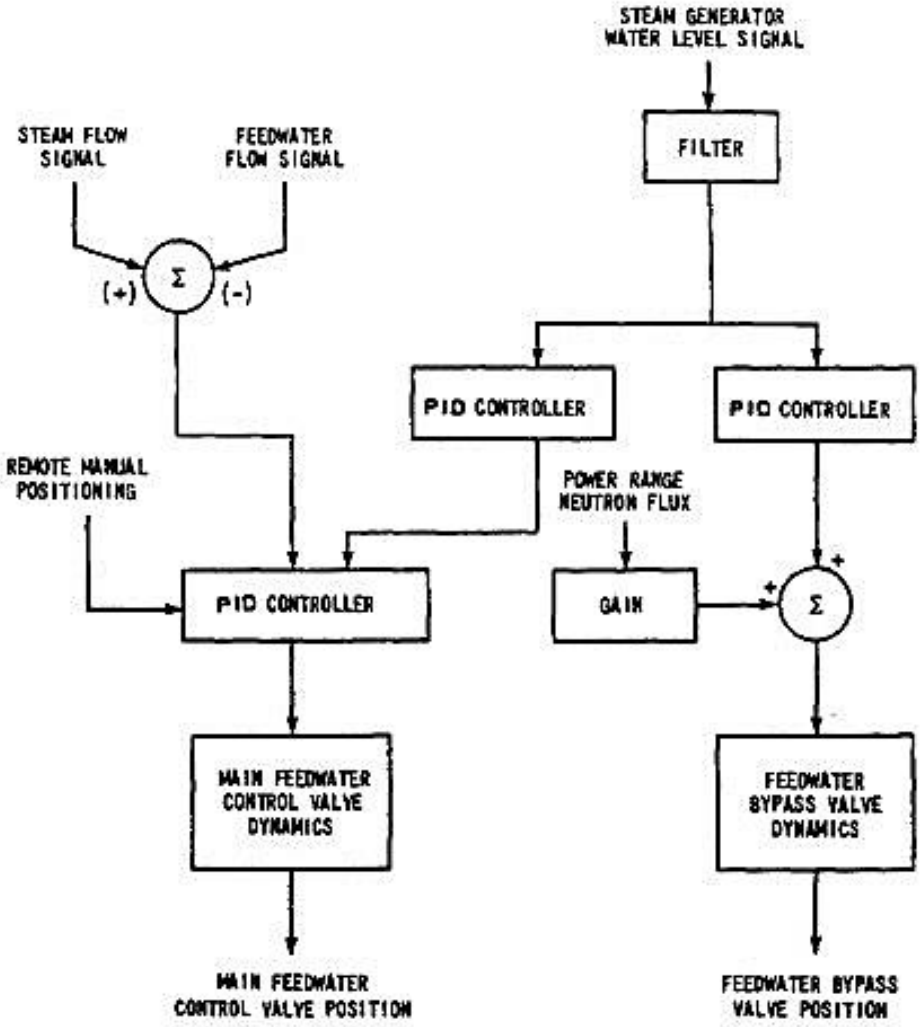


FIGURE 7.7.1-6

BLOCK DIAGRAM OF STEAM GENERATOR WATER LEVEL CONTROL SYSTEM



NOTE: STEAM GENERATOR LEVEL SETPOINT IS CONSTANT AT 57%.

FIGURE 7.7.1-8

BLOCK DIAGRAM OF STEAM DUMP CONTROL SYSTEM

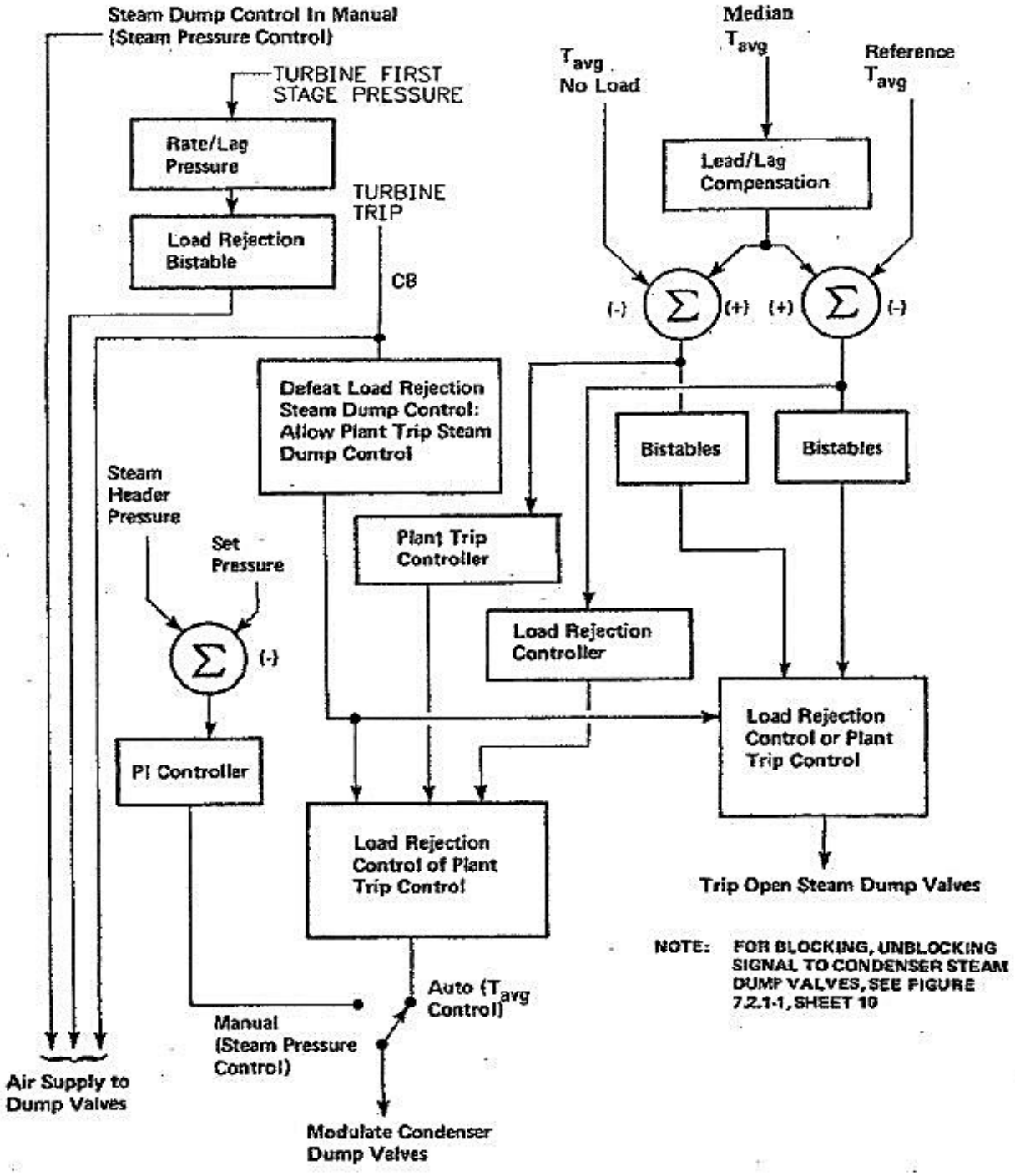


FIGURE 7.7.1-9

BASIC FLUX-MAPPING SYSTEM

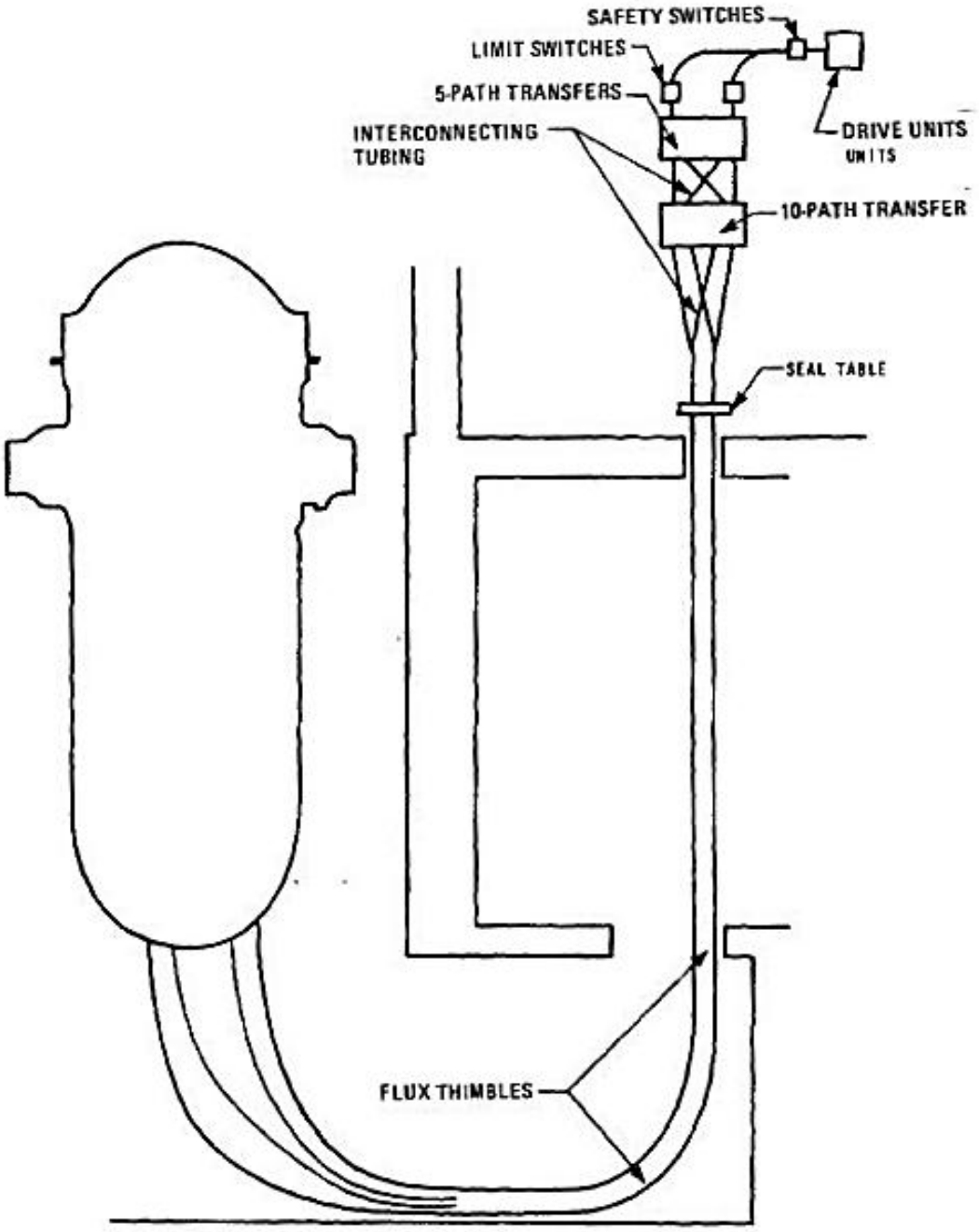


FIGURE 7.7.2-1

SIMPLIFIED BLOCK DIAGRAM OF ROD CONTROL SYSTEM

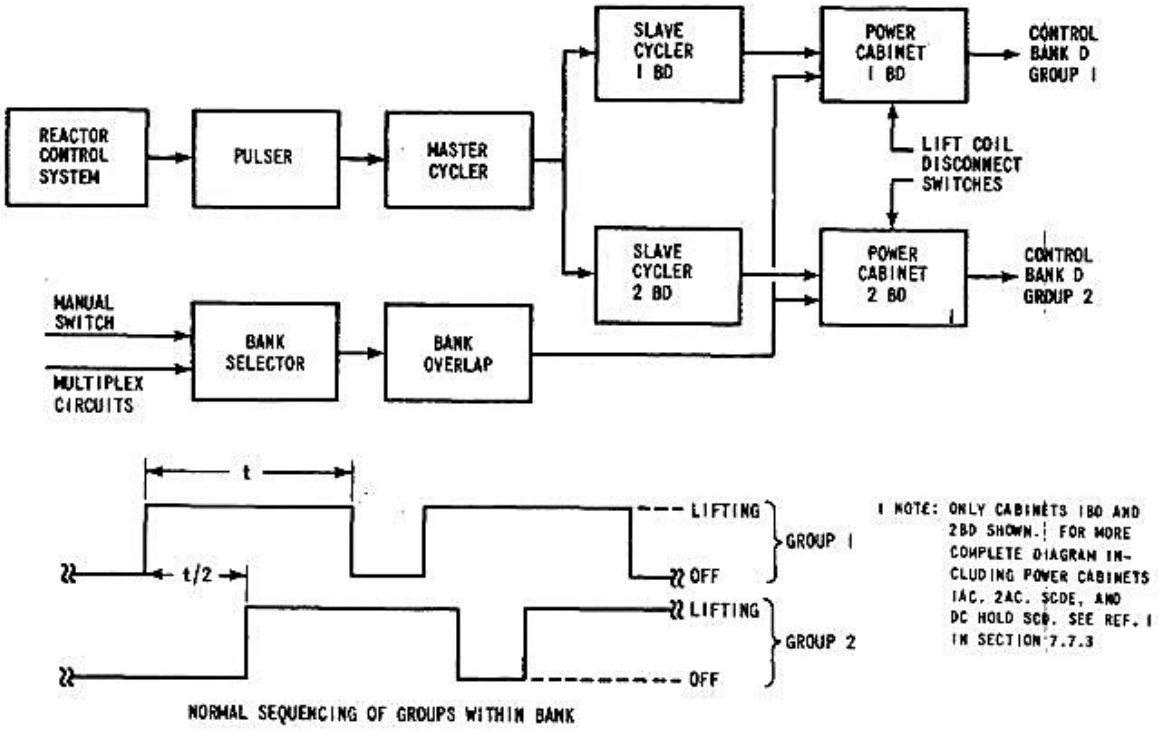
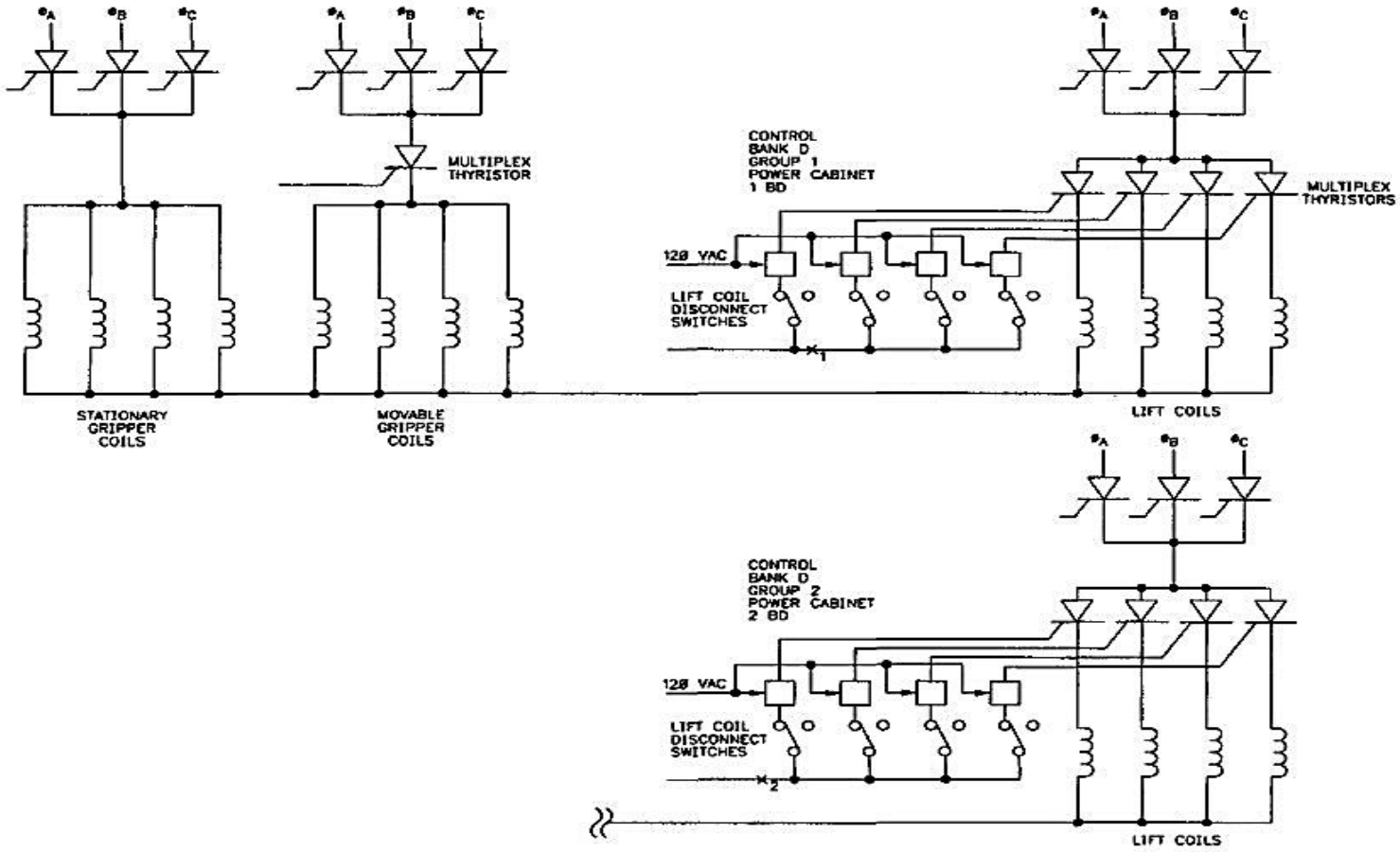


FIGURE 7.7.2-2

CONTROL BANK D PARTIAL SIMPLIFIED SCHEMATIC DIAGRAM OF POWER CABINETS 1BD AND 2BD