Chapter 7: Instrumentation and Control

Table of Contents

Chapter 7: Instrumentation and Control

Table of Contents

Chapter 7: Instrumentation and Control

Table of Contents

Chapter 7: Instrumentation and Control

List of Tables

Chapter 7: Instrumentation and Controls

List of Figures

Intentionally Blank

CHAPTER 7
INSTRUMENTATION AND CONTROL

7.1 SCOPE

This section presents the various plant instrumentation and control systems with discussion focusing on the design bases, system descriptions, and system evaluation. It is shown that the intent of the applicable criteria and codes, such as the AIF GDC (Reference 1) and IEEE-279 (Reference 2), recognized by regulatory agencies (principally the NRC) concerned with the safe generation of nuclear power were reasonably met by the plant instrumentation and control systems and that there is reasonable assurance that these systems do provide for the production of power in a manner that insures no undue risk to the health and safety of the public. WPSC provides Control Room instrumentation that is qualified to monitor accident conditions as suggested in Regulatory Guide (RG) 1.97, Revision 3, with deviations and exceptions as described in the RG 1.97 Plan. In Reference 3, the NRC accepted WPSC's plan for implementation of the RG 1.97 Plan. These instrumentation and control systems have been subdivided for design and presentation purposes along the lines that represent the common division of these systems in existing facilities which adhere to the accepted practice of control and protection separation.

Section 7.2, Protection Systems, presents those features, which act to limit the consequences of faults of moderate frequency, such as loss of feedwater flow by, at most, a shutdown of the reactor and turbine, with the plant capable of returning to operation after corrective action. The Protection System imposes a limiting boundary region to plant operation. This boundary acts as a safety margin so that anticipated abnormal conditions do not cause more severe conditions to develop. The systems were designed to permit periodic on-line testing to demonstrate the operability of the Reactor Protection System. The generation of the tripping functions necessary to actuate the Engineered Safety Features (ESF) are also discussed in Section 7.2, with the discussion of ESF actuation in Section 7.5 serving to cover other aspects of the subject.

Section 7.3, Regulating Systems, describes how the reactor responds to plant power requirements in a stable, reliable, and safe manner, which accommodates occurrences such as startup, shutdown, and power operational load changes without plant parameters exceeding the control limits which would require the functioning of the Protection System or the Engineered Safety Features Instrumentation.

Section 7.4, Nuclear Instrumentation, describes the techniques utilized for reactor protection, for monitoring neutron flux and generating appropriate trip and alarm functions for various phases of reactor operating and shutdown conditions, as well as for control functions.

Section 7.5, Engineered Safety Features Instrumentation, presents those features which act to limit the consequences of potentially severe (infrequent) faults such as reactor coolant leakage from a small rupture which exceeds normal charging system makeup and requires actuation of the Safety Injection (SI) System. ESF instrumentation also acts to mitigate limiting faults that have the potential for significant release of radioactive material and extended outage.

Section 7.6, In-core Instrumentation and Inadequate Core Cooling Monitoring System, presents a system of miniature neutron flux detectors and thermocouples which are designed to yield information on the neutron flux distribution and fuel assembly outlet temperatures at selected core locations. Using the information obtained from the In-core Instrumentation System, it is possible to confirm the reactor core design parameters and calculated hot-channel factors. The system provides means for acquiring data and performs no operational plant-control function.

Section 7.7, Operating Control Stations, discusses the control room containing those controls and instrumentation necessary for safe operation of the plant, including the reactor and the turbine generator, under normal and accident conditions. Process variables, which are required on a continuous basis for the startup, power operation, and shutdown of the plant are indicated, recorded, and/or controlled from a controlled access area.

In summation, the information presented in Chapter 7 is intended to provide assurance that the plant instrumentation and control systems have been designed, constructed, tested, and operated so as to adequately perform their intended functions.

7.1 References

1. AIF, “General Design Criteria for Nuclear Power Plants,” December 22, 1969
2. IEEE No. 279, “Proposed IEEE criteria for Nuclear Power Plant Protection Systems (Effective August 30, 1968)”
3. NRC Safety Evaluation Report, A. G. Hansen (NRC) to C. A. Schrock (WPSC) Letter No. K-92-201, October 15, 1992

7.2 PROTECTION SYSTEMS

The protection system consists of the equipment associated with both the Reactor Protection System and the Engineered Safety Features. The quantity and types of instrumentation provided ensures safe and orderly operation of all systems and processes over the full operating range of the plant (Reference 3).

7.2.1 Design Basis

7.2.1.1 Reactor Protection System

Criterion: Core protection systems, together with associated equipment, shall be designed to prevent or to suppress conditions that could result in exceeding acceptable fuel damage limits (GDC 14).

If the Reactor Protection System receives signals, which are indicative of an approach to unsafe operating conditions, the system actuates alarms, prevents Rod Control Cluster Assemblies (RCCAs) withdrawal, initiates turbine runback, and/or opens the reactor trip breakers.

The basic reactor operating design defines an allowable operating region of power, pressure and coolant temperature conditions. This allowable region is defined by the primary tripping functions: the overpower ΔT trip, the overtemperature ΔT trip and the nuclear overpower trip. The operating region below these trip settings is designed so that no combination of power, temperatures, and pressure could result in a departure from nucleate boiling ratio (DNBR) less than the DNBR correlation limit for any credible operational transient. Tripping functions, in addition to those stated above, are provided to back up the primary tripping functions for specific abnormal conditions. Table 7.2-1 provides a complete list of tripping functions.

Rod withdrawal stops and turbine runbacks based upon intermediate and power range nuclear overpower, overpower ΔT and overtemperature ΔT channels are provided (see Table 7.2-3) to prevent a reactor trip which could result from RCCA withdrawal initiated by a malfunction of the reactor control system or by operator action.

7.2.1.2 Engineered Safety Features Instrumentation

Criterion: Protection systems shall be provided for sensing accident situations and initiating the operation of necessary engineered safety features (GDC 15).

Instrumentation provided for ESF is designed to prevent or limit fission product release from the core and to limit energy release, to signal containment isolation, and to initiate the engineered safety features equipment.

ESF Systems are actuated by redundant logic and coincidence networks similar to those used for reactor protection. Each network actuates a device that operates the associated ESF equipment, motor starters and valve operators. The channels are designed to combine redundant

sensors, independent channel circuitry, and coincident trip logic. Where possible, different but related parameter measurements are utilized. This ensures a safe and reliable system in which a single failure will not defeat the intended function. The action initiating sensors, bistables and logic are described in Section 7.5. The ESF Instrumentation System actuates (depending on the severity of the condition) the SI System, Containment Isolation System, the Containment Air Cooling System, the Containment Vessel Internal Spray System, reactor trip, feedwater isolation, diesel generator startup, service water and component cooling pumps, auxiliary feedwater (AFW) pumps, the Control Room Ventilation System, safety related area air cooling systems, and the Shield Building as well as Auxiliary Building Special Ventilation Systems.

7.2.1.3 Protection Systems Reliability and Demonstration of Functional Operability of Protection Systems

Criterion: Protection system shall be designed for high functional reliability and in-service testability necessary to avoid undue risk to the health and safety of the public (GDC 19).

Protection channels required for power operation (above P10) are designed with sufficient redundancy to allow individual channel calibration and test to be made by use of signal simulation techniques, which are injected at various points in the loop during power operation without negating the reactor protection.

Superimposing of test signals may be utilized during the testing of the Nuclear Instrumentation System, as can the internally generated test signals, which negate the detector signal.

Removal of one trip channel is accomplished by placing that channel in the tripped mode. For example, a two-out-of-three channel becomes a one-out-of-two channel. Testing will not cause a reactor trip unless a trip condition exists in another channel. The reactor coolant pump breakers are not tested at power. Containment Internal Spray actuation is bypassed for test.

Protection and operational reliability is achieved by providing redundant instrumentation channels for each protective function. These redundant channels are electrically isolated and physically separated. The channel design incorporates separate sensors, separate power supplies, separate rack and panel-mounted equipment and separate relays for the actuation of the protective function. For protective functions where two-out-of-three or two-out-of-four redundant-coincident actuation is provided, a single channel failure will not impair the protective function nor will it cause an unnecessary plant shutdown.

Criterion: Means shall be included for suitable testing of the active components of protection systems while the reactor is in operation to determine if failure or loss of redundancy has occurred (GDC 25).

The signal conditioning equipment of each protection channel in service at power is capable of being calibrated and tested independently by simulated analog input signals to verify its operation without tripping the reactor. The testing scheme includes checking through the trip logic to the trip breakers. Thus, the operability of each trip channel can be determined conveniently and without ambiguity. Functional operation of the power sources for the protection system is discussed in Chapter 8.

7.2.1.4 Protection Systems Redundancy and Independence

Criterion: Redundancy and independence designed into protection systems shall be sufficient to assure that no single failure or removal from service of any component or channel of such a system will result in loss of the protection function. The redundancy provided shall include, as a minimum, two channels of protection for each protection function to be served (GDC 20).

The Protection System consists of two discrete portions of circuitry: an analog portion consisting of two to four redundant channels which monitor various plant parameters in systems such as the Reactor Coolant System (RCS), Steam System, Containment System, etc.; and a digital portion consisting of two redundant logic channels (trains) which receive inputs from the analog protection channels and performs the needed logic to initiate reactor trips, ESF, etc. Each digital channel is capable of actuating a separate and independent trip breaker in the case of the Reactor Protection System or the appropriate equipment required in the case of the ESF. The intent is that “any single failure within the Protection System shall not prevent proper protection system operation when required.”

This includes independent sensing lines installed between the process and the sensors for redundant protection channels. However, two exceptions exist where redundant transmitters share common sensing lines. The first exception is the three reactor coolant flow transmitters on each coolant loop, which share a common sensing line on the high pressure side of each differential pressure transmitter. The justification for this arrangement is that a rupture of the common sensing lines will cause the transmitters to fail in the low flow (fail safe) direction and produce a low flow indication on the control board for the affected RCS loop, which, if reactor power is above permissive seven (P-7) which is set at 10 percent full power, will result in a reactor trip (rather than prevent a trip from occurring). If the power level is below P-7, the operator will bring the plant into the hot shutdown condition as required by Technical Specifications. The reactor is maintained within all operational safety limits. The second exception involves two pressurizer pressure transmitters that share a common sensing line. Similar to reactor coolant flow, a rupture of the common sensing line will cause, rather than prevent, protective action on low pressure. The ability to trip the reactor on high pressurizer pressure will not be affected by the rupture, because the three transmitters that supply the high-pressure reactor trip signal do not share common sensing lines. A ruptured instrument line is a type of loss-of-coolant accident (LOCA) specifically discussed in Section 14.3, wherein it is noted that sufficient coolant makeup capability is available

from charging pumps alone to permit orderly cold shutdown of the plant. A sensing line failure that locks pressure into the flow transmitter is not considered credible because no flow exists in these static-sensing lines; therefore, no credible failure mechanism exists to create a pressure seal/blockage in the common line. Therefore, a single failure will not prevent a protective action from occurring, and the use of shared sensing lines for these transmitters continues to meet single failure criterion.

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

In certain applications, it is considered advantageous to employ control signals derived from individual protection channels through isolation amplifiers contained in the protection channel. In these cases, analog signals derived from protection channels for non-protective functions are obtained through isolation amplifiers located in the analog protection racks. (By definition, non-protective functions include those signals used for control, remote process indication, computer monitoring, etc.). The isolation amplifiers are designed such that a short circuit, open circuit, or the application of 118 VAC or 140 VDC on the isolated output portion of the circuit (i.e., non-protective side of the circuit) will not upset the input (protection) side of the circuit. One type of an isolation amplifier is discussed in Reference 2, another type in Reference 4. Since the signals obtained through isolation amplifiers are never returned to the protection racks, any postulated failure in the control system will not affect the protection channel.

7.2.1.5 Protection Against Multiple Disability for Protection Systems

Criterion: The effects if adverse conditions to which redundant channels or protection systems might be exposed in common, either under normal conditions or those of an accident, shall not result in loss of the protection function or shall be tolerable on some other basis (GDC 23).

Separation of redundant analog channels originates at the process sensors and continues along the field wiring and through containment penetrations to the analog protection racks. Physical separation is used to the maximum practical extent to achieve separation of redundant transmitters. Separation of field wiring is achieved by using separate wireways, cable trays, conduit runs and containment penetrations for each redundant channel. Redundant analog equipment is separated by locating redundant components in different protection rack sets. Each redundant protection channel set is energized from a separate instrument bus.

Redundant analog protection equipment is separated by locating modules in different protection rack sets. Since all equipment within any protection rack is associated with a single protection set, there is no requirement for separation of wiring and components within the rack.

7.2.1.6 Protection System Failure Analysis Design

Criterion: The protection systems shall be designed to fail into a safe state or into a state established as tolerable on a defined basis. If conditions such as disconnection of the system, loss of energy (e.g., electrical power, instrument air), or adverse environments (e.g., extreme heat or cold, fire, steam, or water) are experienced (GDC 26).

Each reactor trip channel is designed on the "de-energize to operate" principle; a loss of instrument power to that channel causes the system to go into its trip mode.

Reactor trip is implemented by simultaneously interrupting power to the magnetic latch mechanisms on all drives allowing the full-length rod clusters to insert by free fall. The Reactor Protection System is thus inherently safe in the event of a loss of power. This equipment is selected to withstand the most adverse environmental conditions to which it will be subjected; this would also include post-accident conditions within the containment if the equipment is required to operate in the post-accident environment.

7.2.1.7 Redundancy of Reactivity Control

Criterion: Two independent control systems, preferably of different principles, shall be provided (GDC 27).

The reactivity control system employing Rod Cluster Control (RCC) assemblies is discussed in Section 7.3 and the control system employing the Chemical and Volume Control System is discussed in Chapter 9.

7.2.1.8 Reactivity Control System Malfunction

Criterion: The reactor protection system shall be capable of protecting against any single malfunction of the reactivity control system, such as unplanned continuous withdrawal (not ejection or dropout) of a control rod, by limiting reactivity transients to avoid exceeding acceptable fuel damage limits (GDC 31).

Reactor shutdown with RCCA is completely independent of the normal control functions since the trip breakers interrupt the power to the full-length rod mechanism regardless of existing control signals. Effects of continuous withdrawal of a RCCA and of deboration are described in Chapter 14.

7.2.1.9 Conformance to IEEE 279 Design

The following paragraphs discuss the principle of the original design as related to the proposed IEEE 279 "Standard, Nuclear Power Plant Protection Systems," August 1968. Detailed descriptions of the implementation of these principles are presented in the remainder of Section 7.2 and in Section 7.4, Section 7.5, and Section 7.7.

7.2.1.9.1 Seismic Design

For either earthquake (operational or design basis) the equipment is designed to assure that it does not lose its capability to perform its function; i.e., shut the reactor down and maintain it in a safe shutdown condition.

For the design basis earthquake, there may be permanent deformation of the equipment provided that the capability to perform its function is maintained.

Typical protection system equipment is subjected to type tests under simulated seismic accelerations to demonstrate its ability to perform its functions.

Type testing has been done on equipment by the vendor or Westinghouse using conservatively large accelerations and applicable frequencies. The peak accelerations and frequencies used were checked against those derived by structural analyses of operational and design bases earthquake loadings.

The qualification testing requirements used to assure that the criteria is satisfied on the two systems is contained in the topical report WCAP-7817, (Reference 1) “Seismic Testing of Electrical and Control Equipment,” Section 3, entitled “Test Procedures.”

The upgraded Nuclear Instrumentation System (NIS) PR drawers meet the intent of IEEE 344-1987 and IEEE 323-1983 (Reference 18 and Reference 19). Qualification testing of these drawers is documented in WCAP-8687, Supplement 2-E47C, Addendum 4 (Reference 20).

The requirements defined by WCAP-7817 fully meet the intent of IEEE Standard 344, August 11, 1971. Equipment in the Reactor Protection System and the Engineered Safety Features Actuation System has been type-tested by Westinghouse to the above referenced qualification testing requirements. Equipment for the nuclear plant was procured on a similar (identical) basis to that which was qualified. Any major design changes in the equipment would require an evaluation to determine if the change were of a nature as to not effect the results of the seismic tests, or would require the equipment to be seismically qualified.

The following considers the performance of the required safety actions during the test. The reactor protection and safeguards actuation logic circuitry was placed in a pre-trip condition before each discrete test. Then, during the actual shaking, the circuitry was deliberately tripped and changed to a post-trip condition. Satisfactory change of state on demand was used as the basis for demonstrating functional integrity. Relay contacts necessary to demonstrate operability were recorded during the tests.

The process control equipment, nuclear instrumentation equipment and pressure and differential pressure transmitter electrical signals were monitored during the test. Both analog and bistable type signals were recorded. The basis for determining the functional integrity of the

reactor trip and safeguards actuation signals was that these signals should remain unchanged during the test and be capable of changing state after the test when called upon to do so.

The following is a list of the types of equipment utilized in the reactor protection, ESF actuation and part of the emergency power systems which have been tested as reported in WCAP-7817. The equipment described below is from the actual test and was chosen to generally represent all types of equipment included in Westinghouse shutdown and engineered safeguards systems.

- Static Inverter - Converts 125V d-c to 118V a-c (60 Hz).
- Process Equipment - Three cabinets used for monitoring reactor coolant flow, temperature and pressure, pressurizer level and pressure, SI flow, and steam generator pressure and feedwater level. The cabinets include at least one of each type of module used in all of the various process protection and safeguards actuation channels.
- Safeguards Actuation Racks - Two cabinets containing relay logic monitors.
- Nuclear Instrumentation System- Two cabinets containing NIS and Radiation Monitoring System (RMS) equipment.
- Pressure and Differential Pressure Transmitters - Used for reactor coolant pressure and flow, pressurizer pressure and water level, and steam generator pressure, steam flow and feedwater level.

7.2.1.9.2 Electrical Isolation

The design criterion used to assure electrical isolation is that no analog signal which is required for initiation of reactor protection or ESF actuation is allowed to leave a set of protection channels. Where protection signal intelligence is required for other than protective functions, an isolation amplifier (part of the protection set) is used to transmit the intelligence. The isolation amplifier prevents the perturbation of the protection channel signal (input) due to any disturbance of the isolated signal (output) which normally could occur near any termination of the output wiring external to the protection racks. A description of some of the nuclear instrumentation isolation amplifiers that are used in this plant is given in Reference 2. A description of the process control system-isolating device is available in Reference 4.

7.2.1.9.3 Protection System Identification

Field mounted protective equipment and components are provided with an identification tag or nameplate, which allows for that item’s function and channel to be determined. Small electrical components such as relays have nameplates on the enclosure, which houses them. All cables are numbered with identification tags. These numbers are cross-referenced with a cable schedule, which specifies cable routing and function.

For protection racks, which house the protection rack mounted equipment; a color-coded nameplate on the rack is used to differentiate between protective and non-protective sets. This provides immediate and unambiguous identification of protection sets.

7.2.1.9.4 Manual Actuation

Redundant means are provided for manual initiation of protection system action. Failure in the automatic system does not prevent the manual actuation of protection functions. Manual actuation is designed to require the operation of a minimum amount of equipment.

7.2.1.9.5 Channel Bypass or Removal from Operation

The system is designed to permit any one analog channel through its bistable to be maintained, tested, and calibrated during power operation without system trip. Channel bypass and/or removal from operation facilitates these procedures.

During such testing operations the active parts of the system using 2/4 logic meet the single failure criterion, when the channel under test is either tripped or makes use of superimposed test signals which do not negate the detector signal. Any other testing condition, such as using internal test circuits, which negate the detector signal, requires the channel to be declared out of service and Technical Specification limits for continued operation to be followed.

EXCEPTION: “One-out-of-two” systems are permitted to violate the single failure criterion during channel bypass provided that acceptable reliability of operation can be otherwise demonstrated, and by-pass time interval is short.

7.2.1.9.6 Additional Considerations for Test and Calibration

The bistable portions of the protection system (e.g., relays, bistables, etc.) provide trip signals only after signals from analog portions of the system reach preset values. Capability is provided for calibrating and testing the performance of the bistable portion of protection channels and various combinations of the logic networks during reactor operation.

Only one logic train is tested at a time and its output relays are prevented from operating by operation of the test switches. The other logic train remains operable.

Control board indication of testing is provided by analog channel partial trip annunciators, status lights and by logic train partial and full trip annunciators and status lights.

When the analog channels for ESF actuation are tested they are tripped by operation of the test switches. They are not bypassed.

Analog channel testing is performed at the analog instrumentation cabinets by individually introducing simulated input signals into the instrumentation channels and observing the tripping of the appropriate output bistables. Process control 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.

EXCEPTION: Analog channels associated with Containment Spray (see below). Refer to WCAP-7671 (Reference 7) for additional details.

For testing of the reactor protection logic circuits (except for the Source and Intermediate range) and engineered safety features logic circuits (except for the Containment Spray), the inputs to the logic relays are interrupted in various combinations by logic cabinet mounted test switches to produce the trip logic and operate the master relays. Alarm annunciation and status lights in the Control Room are actuated for the various partial trip and full trip conditions.

Reactor trip breaker testing is described in Section 7.2.2. An annunciation is provided in the Control Room to indicate when a breaker is bypassed.

During testing of the Containment Spray analog channels (three one-of-two high containment pressures) the initiating output of the channel under test is bypassed. Audible and visual annunciation is actuated if more than one channel at a time is placed in test.

Signal Processor drawers in the source range and intermediate range have internal provisions for generating self-test frequencies. These oscillator circuits are energized by a switch located on the front of the associated processor drawer.

A test generator board is included in each source range and intermediate range drawer for self-check of that particular channel. A multi-position operation selector switch on the front panel controls the operation of the built-in oscillator circuits on this board. An electrical interlock between the trip-bypass switch and the operation selector switch prevents inadvertent actuation of the reactor trip circuits when the operation selector switch is in the level adjust position, (i.e., the channel cannot be put in the variable signal test mode unless the trip is blocked). Removal of the trip bypass also removes the test signal. The trip bypass is annunciated on the source range and intermediate range drawers and on the main control board per Section 4.12 of 1968 IEEE 279 Standard. Status lights indicate which channel is bypassed. Operation of the test generator board is annunciated on the control board as “NIS Channel Test.” This common annunciator for all NIS channels is alarmed when any channel is placed in the test position and alerts the operator that a test is being performed at the NIS racks. It is energized from emergency power.

The test-calibrate module, which is provided on each power range, is capable of injecting test signals at the inputs of the channel.

A test switch is provided to require deliberate operator action to perform testing of the power range channel. Bistables, which are affected during channel test, do not require bypasses since they operate in two-out-of-four logic or do not cause a reactor trip. Individually adjustable test signals can be injected independently or simultaneously at the input of either ammeter-shunt assembly to appear as the individual ion chamber currents. The test signals are continuously adjustable by means of two front panel mounted controls with calibrated dials. Operation of the test switch on any power range causes the "Channel Test" annunciator to be alarmed on the main control board.

Operation of the relay is verified by a control board annunciator and trip status lights.

Separate testing alarms, consisting of a visual annunciator, are provided at the main control board, which indicate whenever an Engineered Safety Feature Actuation System (up to and including the final actuation device) is on test. One alarm is provided for each ESF System train. In addition, "out of service" alarms of the same type are provided for the following ESF equipment:

- AFW pumps
- component cooling pumps
- containment cooling fans
- containment spray pumps
- Residual Heat Removal (RHR) pumps
- SI pumps
- service water pumps

The design provides for controlled access to all trip settings, module calibration adjustments, test points, and signal injection points.

7.2.1.9.7 Information Readout and Indication of Bypass

The protection system provides and displays information pertinent to system status and plant safety, as well as various test conditions when some part of the system has been bypassed or taken out of service. Trips are indicated and identified down to the channel level.

All switches that can be placed in maintained position which inhibit the automatic operation of ESF equipment are monitored by the Control Room annunciator and the sequence of event recorder. Individual sequence of event recorder points are provided to monitor each such ESF's switch located on the Control Room panel. In addition, one annunciator point is provided to monitor Train "A" Control Room switches and a second annunciator point provided for Train "B" Control Room switches.

The local switches, which can inhibit automatic operation of ESF, meet the alarm criterion stated in Section 7.7. This criterion states that when the local-remote switch is rotated to the local position a Control Room annunciator will sound and the Control Room indicating lights associated with the device will go “off.”

7.2.1.9.8 Completion of Protection Action

Where operating requirements (“operating” interpreted as being non-test conditions) 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 protection function are part of the protection system and are designed in accordance with the criteria of this section.

The protection system is so designed that, once initiated, a protection action goes to completion. Return to normal operation requires action by the operator. Operator action to reset the SI System can be accomplished only after a time delay.

7.2.1.9.9 Multiple Trip Settings

For monitoring neutron flux, multiple trip settings are used. When it is necessary to change to a more restrictive trip setting to provide adequate protection for a particular mode of operation or set of operating conditions, the design provides positive means of assuring that the more restrictive trip setting is used. The devices used to prevent improper use of less restrictive trip settings are considered a part of the protection system and are designed in accordance with the criteria presented in this section.

7.2.1.9.10 Protection Actions

The Reactor Protection System is designed to automatically trip the reactor as itemized in Table 7.2-1.

For anticipated abnormal conditions, protection systems, in conjunction with inherent plant characteristics and ESF, are designed to assure that limits for energy release to the containment are not exceeded; and radiation exposure does not exceed 10 CFR 100 guidelines.

7.2.1.9.11 Indication

All transmitted signals (flow, pressure, temperature, etc.) which can lead to a reactor trip are either indicated (indicators, status lights, etc.) or recorded in the Control Room for every channel.

All nuclear flux power range currents (top detector, bottom detector) and individual algebraic differences of calibrated bottom and top detector currents are indicated and/or recorded. The average nuclear power is also indicated and/or recorded.

7.2.1.9.12 Alarms

Alarms are also used to alert the operator of deviation from normal operating conditions so that he may take corrective action to avoid a reactor trip. Further actuation of any abnormal rod stop or trip of any reactor trip channel will actuate an alarm. Alarms and/or annunciators also alert the operator when a protection channel is placed in the test condition.

7.2.2 System Design

7.2.2.1 Reactor Protection System Description

The reactor protection system limits the range of various core and coolant parameters so that the DNBR is not less than the safety limit value during anticipated operating transients. The parameter ranges were determined by a computer code, which mathematically correlated the nuclear and thermal hydraulic properties of the reactor coolant system.

Reactor Core Safety Limit Curves and the Overtemperature and Overpower Delta T Setpoints are provided in the Core Operating Limits Report (COLR). The allowable reactor power, pressure, and temperature conditions are below and to the left of the Reactor Core Safety Limit Curves. The reactor protection trip functions: the overpower ΔT trip, the overtemperature ΔT trip and the nuclear overpower trip ensure reactor operation is in the allowable operating region by tripping the reactor before reaching the conditions defined by the core safety limits. The allowable operating region is designed so that no combination of power, temperature, and pressure could result in a DNBR less than the DNBR limit for any credible operational transient. Reactor Protection System trip functions, in addition to those stated above, are provided to back up the primary tripping functions for specific abnormal conditions. Table 7.2-1 provides a complete list of tripping functions.

Adequate margins exist between the nominal steady state operating point and required trip points to preclude a spurious trip during design transients.

A block diagram of the Reactor Protection System showing various reactor trip functions and interlocks is shown in Figure 7.2-1.

7.2.2.2 Protection Actions

The engineered safety features actuation system detects plant conditions that require automatic ESF equipment operation and actuates the appropriate ESF equipment when preset limits are reached.

The ESF actuation system automatically initiates the following sub-systems of ESF when any of the conditions listed under each exist:

1. Safety Injection Signal (SIS)
   - Low pressurizer pressure (2/3); this can be manually blocked when the pressurizer pressure (2/3) is below preset value;
   - High reactor containment vessel pressure (2/3);
   - Low steam line pressure per loop (2/3); this can be manually blocked when the pressurizer pressure (2/3) is below a given set point.
2. Steam Line Isolation
   - Coincidence of SIS and (1/2) high steam flow (Hi-Hi set point) isolates the faulty steam line;
   - Coincidence of SIS and (2/4) Low-Low T_{avg} and (1/2) high steam flow (Hi set point) isolates the faulty steam line;
   - High containment pressure (2/3); isolates both steam lines.
3. Feedwater Line Isolation

Any SIS will isolate the main feedwater lines by closing all control valves (main and bypass valves), tripping the main feedwater pumps and closing the pump discharge valves.

The manual or automatic SIS provides the following vital functions:

1. Furnishes signal input required for:
   - main feedwater isolation
   - reactor trip
   - start of emergency diesel generators (A and B)
   - start of AFW pumps
   - start of SI pumps
   - start of service water pumps
   - start of containment fan-coil units
   - Start of component cooling pumps
   - containment isolation
   - containment ventilation isolation
   - start of RHR pump

- start of Shield Building Ventilation System
- start of Auxiliary Building Special Ventilation System
- Control Room Ventilation System

2. Provides a signal input for a (2/2) AND gate for:
   - steam line isolation
   - Turbine Building Service Water isolation

   A discussion of the ESF System sequencing is in Section 8.2.3.

7.2.2.3 System Safety Features

7.2.2.3.1 Separation of Redundant Protection Channels

The Reactor Protection System is designed to achieve separation between redundant protection channels. The channel design is applied to the analog and the logic portions of the protection system, and the functions are illustrated by Figure 7.2-2. Although the illustration is for four-channel redundancy and for two-out-of-four coincident logic, the design is applicable to two and three channel redundancy. Separation of redundant analog channels originates at the process sensors and continues along the field wiring and through containment penetrations to the analog protection racks. Separation of field wiring is achieved using separate wireways, cable trays, conduit runs and containment penetrations for each redundant channel. Redundant analog equipment is separated by locating redundant components in different protection racks. Each redundant protection channel set is energized from a separate AC instrument bus. Logic equipment separation is achieved by providing separate racks; each associated with individual trip breakers. Physical separation is provided between these racks. The reactor trip bistables are mounted in the analog protection racks and are the final operational component in an analog protection channel. Figure 7.2-2 depicts the functions of each bistable indicating that each one drives two relays “C” and “D” which have normally open contacts. The contacts from the “C” relays are interconnected to form the required actuation two-out-of-four coincident logic for tripping breaker No. 1. The transition from instrument channel identity to logic identity is made at the logic relay-coil/relay-contact interface. As such, there is both electrical and physical separation between the analog and the logic portions of the protection system. The above logic network is duplicated for reactor trip breaker No. 2 using the contacts from “D” relays. Therefore, the two redundant reactor trip logic channels are physically and electrically separated from one another. The Reactor Protection System is comprised of identifiable channels, which are physically, electrically, and functionally separated from one another (Reference 3).

The orderly arrangement of equipment for the Reactor Protection System and ESF Actuation System helps facilitate testing and maintenance. Large identification plates with the appropriate background color are attached at the front and back surfaces of each analog rack. A color code for these plates of red, white, blue, and yellow is used for analog protection channels

in Sets I, II, III, and IV, respectively. The protection logic cabinets, housing the Train A logic, master relays, and slave relays are physically separated from cabinets housing Train "B" equipment, and identified by large identification plates on the input side of the racks where protection signals from the various protection channels are received. Small electrical components such as relays have nameplates on the enclosure, which houses them. All field cables are identified as described in Section 8.2.

7.2.2.3.2 Loss of Power

The four reactor protection system channels are powered from four separate and independent 120V ac instrument buses. The instrument buses are battery backed.

A loss of power in the Reactor Protection System causes the affected channel to trip. All reactor protection circuits are de-energized to cause a trip. Availability of control power to the ESF trip channels is continuously monitored. The ESF bistables are de-energized to actuate, except for containment spray, which is energized to actuate.

7.2.2.3.3 Reactor Trip Signal Testing

In the source and intermediate ranges where the trip logic is one out of two for each range, bypasses are provided for the testing procedure.

Nuclear instrument power range channels are tested either by superimposing a test signal on the normal sensor signal so that the reactor trip protection is not bypassed or from the internal test circuit provided the channel is first declared out of service. Based upon coincident two-out-of-four logic, this will not trip the reactor; however, a trip will occur if a reactor trip is required.

Provision is made for the insertion of test signals in each analog loop. This enables testing and calibration of meters and bistables. Transmitters and sensors are checked against each other using plant readout equipment during normal power operation.

7.2.2.3.4 Process Analog Protection Channel Testing

Provisions are made, for process variables, to manually place the output of the bistable in a tripped condition for "at power" testing.

The basic arrangement of elements comprising a representative analog protection channel is shown in Figure 7.2-3. These elements include a sensor or transmitter, power supply, bistable, bistable trip switch and proving lamp, test-operate switch, test annunciator, test signal injection jack, and test points. A portion of the logic system is also included to illustrate the overlap between the typical analog channel and the corresponding logic circuits. The analog system symbols are given in Figure 7.2-8.

Each process protection rack includes a test panel containing those switches, test jacks and related equipment needed to test the channels contained in the rack. A hinged cover encloses a portion of the test panel. Opening the cover or placing the test-operate switch in the "TEST" position automatically initiates an alarm. The test panel cover is designed such that it cannot be closed unless the test signal plugs (described below) are removed. Closing the test panel cover mechanically returns the test switches to the "OPERATE" position.

Testing of process analog protection channels requires that the bistable output relays of the channel under test be placed in the tripped mode prior to proceeding with the analog channel tests. Thus, for the channel under test, the relay elements in the two-out-of-three or the two-out-of-four coincident matrices will be in the tripped mode during the entire test of that channel. It is observed that the remaining channels of the two-out-of-three or the two-out-of-four protective functions meet the single failure criterion when a channel is bypassed or tripped. Placing the bistable trip switch in the tripped mode de-energizes (trips) the bistable output relays and connects a proving lamp to the bistable output circuit. This permits the electrical operation of the bistable to be observed and the bistable set point relative to the channel analog signal to be verified. Upon completion of test of the analog channel, the bistable trip switches must be manually reset to their "operate" mode. Closing the cover of the test panel will not transfer the bistable trip switches from their tripped to their "operate" position.

Process analog channel test is accomplished by simulating a process measurement signal, varying the simulated signal over its signal span and checking the correlation of bistable set points, channel readouts and other loop elements with precision portable readout equipment (see Figure 7.2-3). Test jacks are provided in the test panel for injection of the simulated process signal into each process analog protection channel. Test points are provided in the channel to facilitate an independent means for precision measurement and correlation of the test signal. This test procedure does not require any tools nor does it involve in any way the removal or disconnection of wires in the channel under test. In general, the analog channel circuits are arranged so the channel power supply is loaded and is providing sensing circuit power during channel test. Load capability of the channel power supply is thereby verified by channel test.

7.2.2.3.5 Nuclear Instrumentation Channel Testing

NIS channels may be tested by superimposing the test signal on the actual detector signal being received by the channel. The output of the bistable is not placed in a tripped condition prior to testing. A valid trip signal would then be added to the existing test signal, and thereby cause channel trip at a somewhat lower percent of actual reactor power. The NIS channels may also be tested by substituting a test signal from the internal test circuit instead of the detector signal provided the channel is first declared out of service. Protection bistable operation is tested by increasing the test signal (level signal) to the bistable trip level and verifying operation at control board alarms and/or at the NIS racks.

An NIS channel which can cause a reactor trip through 1 of 2 protection logic (source or intermediate ranges) 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. The power range channels do not require bypass of the reactor trip function for test, since two-out-of-four protection logic is used. In all cases the bypass condition and the channel test condition are alarmed on the NIS drawer and at the main control board. An interlock feature between the bypass switch and channel test switch on each channel keeps the test signal from being activated until the bypass function has been inserted. Administrative control is required to ensure that only one protection channel is placed in the bypass condition at any one time. The power range reactor trips are not affected by the bypass function described above.

7.2.2.3.6 Logic Channel Testing

The general design functions of the logic system are described below. The trip logic channels for a typical two-out-of-three and a two-out-of-four trip function are represented in Figure 7.2-4. Contacts from the “A” and “B” relays are arranged in a two-out-of-three trip matrix and contacts from the “C” and “D” relays (not the same as in Figure 7.2-2) are in a 2/4 matrix. This figure is not to show specific actual hardware implementation but to illustrate a typical switching function that causes a reactor trip breaker trip. This approach is consistent with de-energize to trip failure mode. De-energizing a reactor trip relay causes the contacts serving the UV coil to open and those serving the shunt trip coil to close. This action causes both the de-energization of the UV coil and energization of the shunt trip attachment, allowing them to perform their breaker tripping function. Figure 7.2-5 illustrates a simplified shunt trip circuit with the normally energized and open contacts of the reactor trip relays.

The planned logic system testing includes exercising the reactor trip breakers to demonstrate system integrity. Bypass breakers are provided for this purpose. The bypass breakers also provide for maintenance on the main breakers and allow logic system relay testing without actuating an inadvertent reactor trip. During normal operation, these bypass breakers are open. To prevent simultaneous closure of both bypass breakers electrical interlock is used. Indication of a closed condition of either bypass breaker is provided locally and on the Control Room panel.

As shown in Figure 7.2-4, the trip signal from the logic network is simultaneously applied to the main trip breaker (TB) associated with the specific logic train as well as the bypass breaker associated with an alternate-trip breaker (AB). Should a valid trip signal occur while AB-1 is bypassing TB-1, TB-2 will be opened through its associated logic train via the shunt trip coil and the UV coil. The trip signal applied to TB-2 is simultaneously applied to AB-1 thereby opening the bypass around TB-1. TB-1 would either have been opened manually as part of the test or would be opened through its associated logic train, which would be operational or tripped during testing. There is no automatic or manual trip of the bypass breakers by the shunt trip coil.

An auxiliary relay is located in parallel with the undervoltage coils of the trip breakers. This relay is connected to an event recorder and local white test lamp L6 which can each be used to indicate transmission of a trip signal through the logic network during testing. Lights are also provided to indicate the operation of the logic relays.

Through a combination of test pushbuttons, the UV coil tripping function is tested independent of the shunt trip coil. A light is provided to indicate operation of the shunt trip coil.

The following procedure illustrates the typical method used for testing TB-1 and its associated logic network.

1. With the bypass breaker (AB-1) racked in the test position, locally close and trip AB-1 to verify operation.
2. Rack in AB-1. Close AB-1 remotely. Trip AB-1 remotely. Close AB-1 remotely.
3. With the “Block Shunt Trip” switch depressed trip TB-1 via the UV coil. Release “Block Shunt Trip” switch and close TB-1. Trip TB-1 with the “Test Shunt Trip” switch.
4. Select function to be tested.
5. Sequentially de-energize the trip relays (A1, A2, and A3) for each logic combination (1-2, 1-3, 2-3) using test pushbuttons. Verify that the logic network de-energizes the under voltage coil, and energizes the shunt trip coil on TB-1 for each logic combination. Since the local white test lamp L6 monitors the signal applied to the UV coil, operation of the undervoltage coil can be determined from local white test lamp L6 on the test panel. The shunt trip coil status can be monitored by a shunt trip test white light L11 on the test panel.
6. Repeat “e” for each function.
7. Reset TB-1. Trip and rack-out AB-1.

In order to minimize the possibility of operational errors (such as tripping the reactor inadvertently or only partially checking all logic combinations) each logic network includes a logic channel test panel. This panel includes those switches, indicators, and recorders needed to perform the logic system test. The arrangement is illustrated in Figure 7.2-6. The test switches used to de-energize the trip bistable relays operate through interposing relays as shown in Figure 7.2-3. This approach avoids violating the separation philosophy used in the analog channel design. Thus, although test switches for redundant channels are conveniently grouped on a single panel to facilitate testing, physical and electrical separation of redundant protection channels are maintained by the inclusion of the interposing relay which is actuated by the logic test switches.

7.2.2.3.7 Primary Power Source

The primary power sources for the Reactor Protection System are described in Chapter 8. The source of electrical power for the measuring elements and the actuation of circuits in the Engineered Safety Features instrumentation is also from these buses.

7.2.2.4 Protective Actions

7.2.2.4.1 Reactor Trip Description

Rapid reactivity shutdown is provided by the insertion of full-length RCCAs by free fall. Duplicate series-connected circuit breakers supply all power to the full-length RCCA drive mechanisms. The control rod drive mechanisms (CRDMs) must be energized to keep the full-length RCCAs withdrawn from the core. Automatic reactor trip occurs upon the loss of power to the full-length RCCA drive mechanisms. The reactor trip breakers are opened by either the undervoltage coil or the shunt trip coil on each breaker. The undervoltage coils, which are normally energized, become de-energized by any one of the several trip signals. The shunt trip coils, which are normally de-energized, are energized by any one of the several trip signals.

The components providing power to the circuit breakers undervoltage and shunt trip attachment are designed to open the reactor trip breakers on the reactor trip signal. In addition, upon power loss, the undervoltage trip coils will cause the breakers to trip. The shunt trip coils require power from their own circuitry to trip the reactor trip breakers, as shown in Figure 7.2-5. The shunt trip attachment satisfies the requirements of Item 4.3 of Generic Letter 83-28 (see NRC SERs in Reference 9 and Reference 10).

Certain reactor trip channels are automatically bypassed at lower power where they are not required for safety. Nuclear source range and intermediate range trips are specifically provided for protection at low power or sub-critical operation. For higher power operations they are bypassed by manual action.

During power operation, a sufficient amount of rapid shutdown capability in the form of control rods whose positions are administratively maintained by means of the control rod insertion limit monitors. Administrative control requires that all shutdown group rods be in the fully withdrawn position during power operation.

A list of reactor trips, means of actuation, and the coincident circuit requirements is given in Table 7.2-1. The interlock circuits, referred to in Table 7.2-1 (e.g., P7, are listed in Table 7.2-2).

7.2.2.4.2 Manual Reactor Trip

The manual actuating devices (reactor trip pushbuttons) are independent of the automatic trip circuitry. Either of two manual trip devices located in the Control Room can initiate a reactor trip. These manual trip devices energize the shunt trip and de-energize the undervoltage trip coils on the reactor trip breakers.

7.2.2.4.3 Power Range High Neutron Flux Reactor Trip

The purpose of this trip is to protect against reactivity excursions during subcritical to low power operation (low setting) and power operation (high setting) to prevent departure from nucleate boiling (DNB).

This circuit trips the reactor when two-out-of-four power-range channels are above the trip setpoint. There are two independent trip settings, a high and a low setting. The high trip setting provides protection during normal power operation. The low setting, which provides protection during startup, can be manually blocked when two-out-of-four power range channels are above the P10 permissive of approximately 10 percent full power. Three-out-of-four channels, below approximately 10 percent full power, automatically reinstates the low trip setting function. The high setting is always active.

7.2.2.4.4 Intermediate Range High Neutron Flux Reactor Trip

The purpose of this trip is to protect against reactivity excursions during reactor startup from subcritical conditions proceeding into the power range.

This circuit trips the reactor when one-out-of-two intermediate range channels is above the trip setpoint. This trip, which provides protection during reactor startup, can be manually blocked when two-out-of-four power range channels are above the P10 permissive of approximately 10 percent full power. Three out of four channels below the P10 permissive setpoint automatically reinstates the trip function. The intermediate channels (including detectors) are separate from the power range channels.

7.2.2.4.5 Source Range High Neutron Flux Reactor Trip

The purpose of this trip is to protect against reactivity excursions during subcritical to low power operation to prevent DNB.

This circuit trips the reactor when one-out-of-two source range channels is above the trip setpoint. This trip, which provides protection during reactor startup, can be manually blocked when one of two intermediate range channels is above the P6 permissive setpoint value. This trip is automatically reinstated when three-out-of-four power range channels are below the P10 permissive and when both intermediate range channels are below the P6 permissive. This trip is also automatically blocked when two out of four high-power range signals are above the P10 permissive setpoint of approximately 10 percent. The trip point is set between the source range cutoff power level P6 and the maximum source range power level detection limit.

7.2.2.4.6 Power Range Fast Flux Rate Trip

Two sustained-rate protective trip functions have been incorporated in the Reactor Protection System. As implemented, these protective channels do not require differentiator circuits and are not highly sensitive to process noise or electronics noise. Furthermore, trip

initiation requires two-out-of-four logic so that spurious actuation of any single channel will not trip the reactor.

This basic circuit has been used in Westinghouse reactors for many years in the “dropped rod alarm” feature, which has proved to be trouble-free. Setpoints for the new trip functions are comparable to those in the “dropped rod alarm” feature.

The Fast Flux Rate Trip is functionally similar to the dropped rod sensor discussed in WCAP-7380-L “Topical Report, Nuclear Instrumentation System” (Reference 8). The unit compares the actual power signal with the delayed power signal received through the lag network and amplifies the difference. The amplified signal is delivered to two bistable units. One of these units trips when the signal represents a positive change for one bistable; the other trips for a negative change. Tripping of either of these units represents abnormal rod motion, either motion in or out.

7.2.2.4.7 Positive Sustained Rate Trip

The positive portion of the high flux rate trip provides an added measure of protection against hypothetical rod ejection accidents. The rate trip function assures an immediate reactor trip independent of the initial operating state of the reactor. In addition, the rate trip function provides functional diversity in support of the high-flux-level trip functions for the rod ejection events that would give the worst consequences, full-power and zero-power ejection.

The rod ejection accident is a hypothetical accident, which is analyzed for the Kewaunee Plant (see Section 14.2.6 for description of accident and analysis). The accident is a Condition IV (Limiting Fault) event under the American Nuclear Society (ANS) “Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants.” For the rod ejection, DNB is allowed, however, gross core melting must not occur. The criteria for this accident, are described in Chapter 14.

For rod ejections from 0 percent power (just critical) the plant is typically tripped by the power range high neutron flux trip (low setpoint). For rod ejections from near full power, the plant is typically tripped by the power range high neutron flux trip (high setpoint). During studies of the rod ejection accident, it was found that there were rods which could be ejected from powers between approximately 20 and 80 percent of rated power which would not bring the average core power up to the power range high neutron flux trip setpoint but could result in steady-state power in excess of the value used in the safety analyses.

The results of the Westinghouse Rod Ejection Studies are presented in WCAP-7588, December 1971: “An Evaluation of the Rod Ejection Accident in Westinghouse Pressurized Water Reactors Using Spatial Kinetics Methods.” The hot channel for rod ejection is bounded by the limiting hot channel factors for Westinghouse PWRs given in WCAP-7588.

As protection against the rod ejection from partial power, the positive rate trip was derived. This will trip the reactor on the rapid flux increase, which occurs when a rod is ejected from any power level. The positive rate trip insures that the criteria appropriate for an ANS Condition IV event are met even for rod ejections from partial power.

7.2.2.4.8 Negative Sustained Rate Trip

The negative portion of the high-flux rate reactor trip function provides protection for the core (protection against low DNBR) in the event that two or more RCCAs fall into the core. No protection is required for a single RCCA drop.

This circuit trips the reactor when an abnormal rate of decrease in nuclear power occurs in two-out-of-four power range channels and is always active.

For a dropped control rod, the basic problem is that power distributions worse than design core power distribution can occur after the rod is dropped. If the automatic control system and/or the negative moderator temperature co-efficient of reactivity cause the core power to return to full power, the minimum DNBR may fall below the DNBR limit. For early Westinghouse plants, rod drop protection was provided via the use of a turbine runback and a block of automatic rod withdrawal following the detection of a dropped control rod. The analytical studies of dropped control rod accidents were confined to the assumption of a single rod being dropped. Since the event was credible (ANS Condition II), the criteria was that the minimum DNBR not fall below the DNBR limit during the transient.

As analytical methods were improved it became apparent that no protection was required for single rod drop accidents. However, in order to protect against multiple rod drop from a group or bank, Westinghouse recommended the negative power range nuclear flux rate trip. This trip function will insure that the DNBR remains above the DNBR limit for all multiple rod drop accidents.

Analyses have been performed to assure that following the core power decrease caused by a single dropped rod, a return to full power initiated by the automatic reactor control system (responding to continued full power turbine load demand) will not result in a DNBR less than the DNBR limit. The analyses were performed at steady state, full power operation, with error allowances for appropriate plant variables. The full power condition represents the maximum power following the rod drop and gives the minimum margin to DNB. Core radial heat flux peaking factors were obtained with a two-neutron group multi-dimensional digital computer code. DNBR was calculated using a digital computer code which models three-dimensional core thermal-hydraulic conditions along parallel flow channels.

If a single RCCA is dropped, the resultant power tilt is only about 5 percent and no protective action is required. It would of course be necessary for the operator to retrieve the dropped RCCA. Alarms alert the operator to the dropped RCCA.

The setpoints for the rate trips are approximately as follows:

- Rate Time = constant five seconds
- Delta-Power = 15 percent of full power for the positive rate trip and 10 percent of full power for negative rate trip

With these setpoints a step or rapid change in excess of either +15 percent or –10 percent in core nuclear power will actuate the trip. Smaller and/or slower power changes will not actuate the trip.

Accuracy (reproducibility) of the flux rate signal is within ±5 percent, and the power range rate trip is actuated within 0.2 seconds which is the delay time for the signal to reach the reactor trip breakers following a 20 percent step input at the sensor output. Sensor delay is no greater than fifty microseconds.

7.2.2.4.9 Overtemperature ΔT Reactor Trip

The purpose of this trip is to protect the core against DNB. This circuit trips the reactor on coincidence of two-out-of-four signals, with two temperature measurements per loop above the trip setpoint. Two set points for this reactor trip are continuously calculated for each loop by solving the following equation:

$$\Delta T_{setpoint} = K_1 - K_2 \left(\frac{1+\tau_1 S}{1+\tau_2 S} \right) \left(T_{avg} - T_{avg_o} \right) + K_3 \left(P - P_1 \right) - f\left(\Delta q \right)$$

Where:

T_{avg} = average temperature, °F.

T_{avg_o} = nominal loop full power T_{avg}, °F.

P = Pressurizer pressure (psig).

P_1 = 2235 psig

K_1 = setpoint bias, °F.

K_2,K_3 = constants based upon the effects of temperature and pressure on the DNB limit, °F/°F, °F/psig.

f(Δq) = a function of flux difference between upper and lower long ion chamber sections, four independent measurements, °F.

τ_1,τ_2 = lead-lag time constants, sec.

The four long ion chamber units separately feed one overtemperature ΔT trip channel. Thus, a single failure neither defeats the trip function nor causes a spurious trip. Resultant changes in the f(Δq) can only lead to a decrease in trip setpoint.

In addition to the reactor trip, a rod stop and turbine runback are initiated when:

$\Delta T > \Delta T_{rod\ stop}$

Where:

$\Delta T_{rod\ stop} = DT_{setpoint} - B_p$

B_p = a setpoint bias

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, e.g., this gives the operator the opportunity to adjust the rods to reshape the flux before a reactor trip occurs.

7.2.2.4.10 Overpower ΔT Reactor Trip

The purpose of this trip is to protect against excessive power level (fuel rod rating protection). This circuit trips the reactor on coincidence of two-out-of-four (2/4) signals, when two sets of temperature measurements per loop are above the trip setpoint.

The set point for this reactor trip is continuously calculated for each channel by solving equations of the form:

$$\Delta T_{setpoint} = K_4 - K_5 \left(\frac{\tau_3 S}{\tau_3 S + 1} \right) T_{avg} - K_6 \left(T_{avg} - T_{ave_o} \right) - f\left(\Delta q \right)$$

Where:

T_{avg}	=	operating average temperature, °F.
T_{avg_o}	=	nominal loop full power T_{avg}, °F.
f(Δq)	=	is a function of flux difference between upper and lower ion chamber sections, four independent measurements, °F.
K_4	=	setpoint bias, °F.
K_5	=	a constant based upon the effect of temperature rate on the overpower setpoint, °F/°F.
K_6	=	a constant based upon the effect of temperature on the overpower setpoint, °F/°F.

τ_3 = time constant, sec.

In addition to the reactor trip, a rod stop and turbine runback are initiated on approach to overpower ΔT actuation.

For T_{avg}/ΔT Control and Protection System diagram see Figure 7.2-7.

7.2.2.4.11 Pressurizer Low Pressure Reactor Trip

The purpose of this trip is to protect against excessive core steam voids and to limit the necessary range of protection provided by the overtemperature ΔT trip.

The circuit trips the reactor on coincidence of two-out-of-four low pressurizer pressure signals. This trip is blocked when three-out-of-four power range channels and two-out-of-two turbine first stage pressure channels are below the P7 permissive of approximately 10 percent power. Each channel is lead-lag compensated.

7.2.2.4.12 Pressurizer High Pressure Reactor Trip

The purpose of this trip is to limit the range of required protection from the overtemperature ΔT trip and to protect against RCS overpressure. The reactor is tripped on coincidence of two-out-of-three pressurizer high-pressure signals above the setpoint.

7.2.2.4.13 Pressurizer High Water Level Reactor Trip

This trip is provided as a backup to the pressurizer high-pressure reactor trip. The coincidence of two-out-of-three pressurizer high water level signals above their setpoint trips the reactor. This trip is blocked when three out of four power-range channels and two of two-turbine first stage pressure channels are below the P7 permissive of approximately 10 percent power.

7.2.2.4.14 Reactor Coolant Low-Flow Reactor Trip

This trip protects the core from DNB due to low coolant flow or a loss-of-coolant flow. The means of sensing coolant low flow are as follows:

1. Low-Reactor-Coolant-Flow Reactor Trip

   The coolant low-flow signal is actuated by the coincidence of 2/3 low-flow signals from either reactor coolant loop. The loss of flow in a single loop causes a reactor trip if operating above the P8 permissive of approximately 10 percent power. **Note:** At Kewaunee the permissive P7 and P8 are set at approximately the same point (approximately 10 percent power).

2. Reactor Coolant Pump Breakers-Open Reactor Trip

   Opening of the reactor coolant pump breakers, results in a reactor trip by acting directly in the reactor trip circuits. Above the P7 setpoint the reactor is tripped on both open breaker signals. Above the P8 setpoint, the reactor is tripped when either reactor coolant pump breaker is open. See note in paragraph 1. above. One open breaker signal is generated for each reactor coolant pump.

3. Reactor Coolant Pump Bus Underfrequency Reactor Trips

   An underfrequency signal from both 4160V buses (Buses 1-1 and 1-2) results in the trip of both reactor coolant pump breakers. There are two underfrequency relays per bus.

4. Reactor Coolant Pump Bus Undervoltage Reactor Trip

   Above the P7 setpoint an undervoltage signal from both 4160V buses (Buses 1-1 and 1-2) results in a reactor trip. There are two undervoltage relays per bus.

7.2.2.4.15 SI System Actuation Reactor Trip

A reactor trip occurs when the SI System is actuated by signals listed in Table 7.2-1.

7.2.2.4.16 Turbine Generator Trip, Reactor Trip

A turbine trip is sensed by two out of three signals that monitor turbine auto-stop oil pressure below the setpoint or when two out of two turbine stop valves close. A turbine trip causes a direct reactor trip (when operation is above the P7 power level). A turbine trip may result in a controlled short-term release of steam, which removes sensible heat from the RCS and thereby avoids steam generator safety valve actuation. The logic circuitry of the reactor trip that occurs meets the IEEE-279 August 1968 criteria.

The turbine control system automatically trips the turbine generator under any of the following conditions:

- generator electrical faults
- low condenser vacuum
- thrust bearing failure
- low lube oil pressure
- turbine overspeed
- reactor trip
- manual trip
- steam generator feedwater pump breakers open

- loss of internal E-H power
- low auto-stop oil pressure
- steam generator high-high level
- steam generator low-low level Anticipated Transient Without Scram (ATWS) Mitigating System Actuation Circuitry (AMSAC) initiation
- SI (not credited in safety analysis)

In addition, an independent emergency overspeed protective system is used to provide independent and physically separate redundant sensing and tripping circuits to trip the turbine generator by closing all turbine steam admission valves.

Further details on these trips are discussed in Chapter 10. For further information on AMSAC, see Section 14.1.11.

7.2.2.4.17 Low Feedwater Flow Reactor Trip

This trip protects the reactor from a sudden loss of its heat sink. The trip is actuated by a steam/feedwater flow mismatch (1/2) in coincidence with low water level (1/2) in either steam generator being below the trip setpoint.

7.2.2.4.18 Low-Low Steam Generator Water Level Reactor Trip

The purpose of this trip is to protect the steam generators in the case of a sustained steam/feedwater flow mismatch of insufficient magnitude to cause a flow mismatch reactor trip. The trip is actuated on two out of three (2/3) low-low water level signals in either steam generator being below the trip setpoint.

7.2.2.4.19 Rod Stops

Rod withdrawal stops are utilized to prevent a reactor trip or to prevent an abnormal condition from increasing in magnitude and causing a reactor trip.

A list of rod stops is given in Table 7.2-3. Some of these have been previously noted under permissive circuits, but are listed again for completeness.

7.2.2.4.20 Automatic Turbine Load Runback

A turbine runback is initiated by an approach to an overpower or overtemperature ΔT condition. This will prevent high power operation, which might lead to a DNBR less than 1.3.

7.2.2.5 Control Bank Rod Insertion Monitor

The control bank rod insertion limits, Z_{LL}, are calculated as a linear function of power and reactor coolant average temperature. The equation is:

$$Z_{LLi} = K_{1i}\ \Delta T_{avg} + K_{2i}\ T_{avg_{auct}} + K_{3i}$$

where:

i = Banks A, B, C, and D, respectively,

where K_{1i} and K_{2i} are preset manually adjustable gains and K_{3i} is a preset manually adjustable bias. The (ΔT) and (T_{avg}) are the average of the individual temperature differences and the coolant average temperatures respectively measured from the reactor coolant hot leg and the cold leg. The highest T_{avg} used for control is the same T_{avg} applied to Z_{LL}.

An insertion limit monitor with two alarm set points is provided for the control banks. A description of control and shutdown rod banks is provided in Section 7.3. The “low” alarm alerts the operator of an approach to a reduced shutdown reactivity situation requiring boron addition by following the proper Chemical and Volume Control System procedure. If the actuation of the “low-low” alarm occurs, the operator will take immediate action to add boron to the system.

7.2.3 System Evaluation

7.2.3.1 Reactor Protection System and DNB

The following is a description of how the reactor protection system prevents DNB.

The plant variables that affect the DNB ratio are:

- Thermal power
- Coolant flow
- Coolant temperature
- Coolant pressure
- Core power distribution

These DNBR related parameters are monitored by the reactor protection system: nuclear overpower trip, RCS flow trip, pressurizer pressure trip, and overpower and overtemperature ΔT trips. In addition, reactor power distribution measurements using the in-core instrumentation system verify that the core power distribution is within COLR design limits. The reactor protection trip functions ensure reactor operation is in the allowable operating region so that no

combination of power, temperature, and pressure could result in a DNBR less than the DNBR limit for any credible operational transient.

Reactor trips for a fixed high pressurizer pressure and for a fixed low pressurizer pressure are provided to limit the pressure range over which core protection depends on the overpower and overtemperature ΔT trips.

Reactor trips on nuclear overpower and reactor coolant low flow are provided for direct, immediate protection against rapid changes in these parameters. However, for cases in which the calculated DNBR approaches 1.30, a reactor trip on overtemperature ΔT would also be actuated.

For the postulated abnormal conditions, the exact combination of conditions (reactor coolant pressure, temperature and core power, instrumentation inaccuracies, etc.) will not cause DNBR to go below 1.30 before a reactor trip. The simultaneous loss of power to all of the reactor coolant pumps is the accident condition most likely to cause an approach to a DNBR of 1.30 for the calculated worst fuel rod.

In any event the DNBR is near 1.30 for only a few seconds.

The ΔT trip functions are based on the differences between measured hot leg and cold leg temperatures. These differences are proportional to core power. The ΔT trip functions are provided with nuclear differential flux signals from the upper and lower ion chambers to reflect a measure of axial power distribution. This aids in preventing an adverse axial flux distribution, which could lead to exceeding allowable core conditions.

7.2.3.2 Specific Control and Protection Interactions

7.2.3.2.1 Nuclear Flux

Four power-range nuclear flux channels are provided for overpower protection. Isolated outputs from all four channels are averaged to provide for automatic rod control. If any channel fails in such a way as to produce a low output, that channel is incapable of proper overpower protection. In principle, the same failure may cause rod withdrawal and hence, overpower. Two out of four overpower trip logic will ensure an overpower trip if needed, even with an independent failure in another channel.

In addition, the control system will respond only to rapid change in indicated nuclear flux; slow changes or drifts are compensated by the temperature control signals. Finally, an overpower signal from any nuclear power channel will block both automatic and manual rod withdrawal. The set point for this rod withdrawal stop is below the reactor trip set point.

7.2.3.2.2 Coolant Temperature

Hot leg and cold leg temperature measurements are made for each reactor coolant loop to provide reactor protection. In addition, by use of isolation amplifiers located in the Protection

rack, the temperature signals are used for control. The temperature-average measurements and temperature-difference measurements for each loop are used for overpower ΔT and overtemperature ΔT reactor protection with two channels per loop and 2/4 reactor trip logic. The reactor control system uses the highest auctioneered of the four isolated temperature average measurements.

The hot and cold leg Resistance Temperature Detectors (RTDs) are inserted into reactor coolant bypass loops, a bypass loop from upstream of the steam generator to downstream of the steam generator is used for the hot leg RTDs, and a bypass loop from downstream of the reactor coolant pump to upstream of the pump is used for the cold leg RTDs. The RTDs are located in manifolds within the containment and are directly inserted into the reactor coolant bypass loop flow without thermowells. Thermowells are *not* used in order to improve the detector's time response to temperature changes by keeping the detector thermal lag small. The bypass arrangement permits replacement of defective temperature elements while the plant is at hot shutdown without draining or depressurizing the reactor coolant loops.

Three sampling probes are installed in a cross-sectional plane of each hot leg at approximately 120° intervals. Each of the sampling probes, which extend several inches into the hot leg coolant stream, contains five inlet orifices distributed along its length. In this way a total of 15 locations in the hot leg stream are sampled providing a representative coolant temperature measurement. The 2-inch diameter pipe leading to the manifold containing the temperature measuring elements (RTDs) provides mixing of the samples to give an accurate temperature measurement. Care has been taken to distribute the flow evenly among the five orifices of each probe by effectively restricting the flow through the orifices. This has been done by designing a smaller overall orifice flow area than that of the common flow channel within the probe. This arrangement has also been applied to the flow transition from the three probe flow channels to the pipe leading to the temperature element manifold. The total flow area of the three probe channels has therefore been designed to be less than that of 2-inch pipe connecting the probes to the manifold.

The cold-leg reactor coolant flow is well mixed by the reactor coolant pumps. Therefore, the cold-leg sample is taken directly from an ordinary 2-inch pipe tap off the cold-leg downstream of the pump.

The main requirement for reactor protection is that the temperature difference between the hot leg and cold leg vary linearly with power. All ΔT setpoints are in terms of the full power ΔT; thus, absolute ΔT measurements are not required. Linearity of ΔT with power was verified during Startup Tests.

Reactor Protection logic using reactor coolant loop temperatures is 2/4 with two channels per reactor coolant loop with separate RTDs for each reactor protection channel. This complies with all applicable IEEE 279 criteria.

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

Since reactor control is based on the highest average temperature from the four temperature average measurements, the control rods are always moved based upon the most conservative temperature measurement with respect to DNB margins. A spurious low average temperature measurement from any loop temperature control channel will not result in any control action. A spurious high average temperature measurement will cause rod insertion (safe direction).

Individual annunciators and indicators for each reactor coolant loop bypass flow are provided on the main control board and vertical panels. The alarms provide the operator with immediate indication of a low flow condition in the bypass loops associated with either reactor coolant loop. The indicators provide accurate flow indication for each individual bypass flow loop.

Local indicators are provided to monitor total flow through the RTD bypass manifolds for each loop. The indicators are located inside containment but are accessible during power operations. Flow will be monitored:

1. Prior to restoring temperature channels to normal service following reopening of bypass loop isolation valves whenever a bypass loop has been out of service.
2. On a periodic basis.
3. Following any bypass loop low flow alarm.

In addition, channel deviation signals in the control system provide an alarm if any temperature channel deviates significantly from the other. Automatic rod withdrawal blocks also occur if any one-out-of-four nuclear channels indicates an overpower condition or if any two-out-of-four temperature channels indicate an overtemperature or overpower ΔT condition. Two-out-of-four (2/4) trip logic is used to ensure that an overtemperature or overpower ΔT trip occurs if needed even with an independent failure in another channel. Finally, as shown in Section 14.1, the combination of trips on nuclear overpower, high pressurizer water level, and high pressurizer pressure also serve to limit an excursion for any credible rate of reactivity insertion.

7.2.3.2.3 Pressurizer Pressure

The four pressurizer pressure protection channel signals are used for low-pressure protection and as inputs to the overtemperature ΔT trip protection function (see Figure 7.2-9). Three of the four pressure channels are used for high-pressure protection. Isolated output signals from these channels are used for pressure control. These are used to control pressurizer spray and heaters and power-operated relief valves. Pressurizer pressure is sensed by fast response pressure transmitters with a time response of better than 0.2 seconds.

7.2.3.2.4 Low Pressure

A spurious high-pressure signal from one channel can cause low pressure by actuation of spray and/or a relief valve. Additional redundancy is provided in the protection system to ensure low-pressure protection, i.e., two out of four low-pressure reactor trip logic, and two-out-of-three logic for SI.

7.2.3.2.5 High Pressure

The pressurizer heaters are incapable of overpressurizing the RCS. Maximum steam generation rate with heaters is about 8200 lb/hr, compared with a total relieving capacity of two orders of magnitude greater for the two safety valves and for the two power-operated relief valves as shown in Table 4.1-3. Therefore, overpressure protection is not required for a pressure control failure that could cause the heaters to energize; however, two-out-of-three (2/3) high-pressure trip logic is used.

In addition, either of the two relief valves can easily maintain pressure below the high-pressure trip point. The two relief valves are controlled by independent pressure channels one, of which is independent of the pressure channel used for heater control. Finally, the rate of pressure rise achievable with heaters is slow, and ample time and pressure alarms are available for operator action.

7.2.3.2.6 Pressurizer Level

Three pressurizer level channels are used for reactor trip (2/3 high level). Isolated output signals from these channels are used for level control, increasing or decreasing the pressurizer water level as required. 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). (See Figure 7.2-10)

The design of the pressurizer water level instrumentation is a slight modification of the usual tank level arrangement using differential pressure between an upper and a lower tap (see Figure 7.2-11). The modification consists of the use of a sealed reference leg instead of the conventional open column of water.

Experience has shown that hydrogen gas can accumulate in the upper part of the condensate pot on conventional open reference-leg systems in pressurizer level service. At RCS operating pressures, high concentrations of dissolved hydrogen in the reference-leg water are possible. On sudden depressurization accidents, it has been hypothesized that rapid effervescence of the dissolved hydrogen could blow water out of the reference leg and cause a large level error, measuring higher than actual level. To eliminate the possibility of such effects, a bellows is used in a pot at the top of the reference legs to prevent dissolving of hydrogen gas into the reference-leg water.

The reference-leg operating temperature remains at the local ambient temperature. This temperature varies somewhat over the length of the reference-leg piping under normal operating conditions but does not exceed approximately 140°F. During a blowdown to atmospheric pressure, any reference-leg boil-off is confined to the condensate-steam interface in the condensate pot at the top of the temperature barrier leg, with only negligible effects on the accuracy of the level sensors. Flashing or effervescence within the reference leg itself does not occur. Therefore, the instrumentation provided will sense low pressurizer level.

Prior to operation at KNPP, the pressurizer level sealed reference-leg design had been in successful operation for over seven years at other plants. Supplier tests were run originally to confirm less than one-second-time response.

Calibration of the sealed reference leg system was done in place after installation by application of known pressure to the low-pressure side of the transmitter and measurement of the height of the reference column. The effects of static pressure variations were predictable. The largest effect is due to the density change in the saturated fluid in the pressurizer itself. The effect is typical of level measurements in all tanks with two-phase fluid and is not peculiar to the sealed reference-leg technique. In the sealed reference leg, there is a slight compression of the fill water with increasing pressure, but this is taken up by the flexible bellows. A leak of the fill water in the sealed reference leg can be detected by comparison of redundant channel readings on line and by physical inspection of the reference-leg off line with the channel out of service. Leaks of the reference leg to atmosphere will be detectable by off-scale indications of the level on the control board. Further detection of leakage is provided by the plant computer alarms for deviation between redundant channels.

If an assumed break is at the top of the pressurizer instrument line, the affected pressure channel would be subjected to containment pressure and initiate a partial reactor trip on low pressure. If the break is on a level instrument line, the affected sealed reference-leg will indicate high water level because of the resulting pressure imbalance, and this will generate a partial reactor trip. In either case, the resulting action is in the “safe” direction, producing a trip of the affected channel bistable.

A break in a non-instrument line will not effect the capability of either the pressure or level instruments to function properly in their calibrated range, as noted. Regardless of the particular line severed there is sufficient redundancy of both pressure and level instrumentation to initiate a reactor trip on low-pressure (2/4) or high water level (2/3) and for SI on low pressurizer pressure (2/3).

Furthermore, core DNB protection is provided by the ΔT overtemperature reactor trip. The ΔT overtemperature trip setpoint will be adjusted downward (safe direction) as the system pressure decreases.

A typical depressurization incident caused by opening a line at the top of the pressurizer would be an accidental opening of a relief valve. Studies of this hypothetical accident occurring under full power assuming conservative conditions and maximum instrument errors reveals that the event results in a rapidly decreasing reactor coolant system pressure causing a slight increase in pressurizer water level as the overpressure is released. Reactor trip occurs on overtemperature ΔT as the DNBR goes down with the pressure. (If the low-pressure trip set point is high enough it will trip the reactor before the ΔT overtemperature trip). Following the trip, both T_{avg} and the pressure continue to decrease rapidly. Eventually the pressure decreases to the saturation point of the hot leg, at which point boiling in the hot leg causes the water level in the pressurizer to rise again. Throughout the transient, the core remains covered and DNB does not occur. Depending on plant design and/or setpoints, the time scale of events is typically up to one minute to reach reactor trip and five minutes to reach saturation pressure in the hot leg.

7.2.3.2.7 High Level

A reactor trip on pressurizer high level is provided to prevent filling the pressurizer in the event of a rapid thermal expansion of the reactor coolant. A rapid change from high rates of steam-relief to water-relief could be damaging to the safety valves, relief piping, and pressure relief tank. However, a level control failure cannot actuate the safety valves because the high-pressure reactor trip is set below the safety valve set pressure. With the slow rate of charging available, overshoot in pressure, before the trip is effective, is much less than the difference between reactor trip and safety valve set pressures. Therefore, a control failure does not require protection system action. In addition, alarms occur in ample time for corrective manual action.

7.2.3.2.8 Low Level

For control failures, which tend to empty the pressurizer, independent low- level channels ensure that the protection system can withstand an independent failure in another channel. In addition, alarms occur in ample time for corrective manual action.

7.2.3.2.9 Steam Generator Water Level

7.2.3.2.10 Feedwater Flow

Before describing control and protection interaction for these channels, it is beneficial to review the protection system basis for this instrumentation (see Figure 7.2-12).

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 with no protective action, the steam generators would boil dry and cause an overtemperature-overpressure excursion in the RCS. Reactor trips on temperature, pressure, and pressurizer water level will trip the unit before there is any damage to

the core or RCS. Redundant AFW pumps are provided to remove and thus prevent residual heat, after trip, from causing thermal expansion and discharge of the reactor coolant through the pressurizer relief valves. Reactor trips act before the steam generators are dry to reduce the required capacity and starting time requirements of these pumps and to minimize the thermal transient on the RCS and steam generators. Independent trip circuits are provided for each steam generator for the following reasons:

1. Should severe mechanical damage occur to the feedwater line to one steam generator, it is difficult to ensure the functional integrity of level and flow instrumentation for that unit. For instance, a major pipe break between the feedwater flow element and the steam generator would cause high flow through the flow element. The rapid depressurization of the steam generator would drastically affect the relation between downcomer water level and steam generator water inventory.
2. It is desirable to minimize thermal transients on a steam generator for credible loss-of-feedwater accidents. It should be noted that controller malfunctions caused by a protection system failure affect only one steam generator.

7.2.3.2.11 Feedwater Flow

A spurious high signal from the feedwater flow channel being used for control would cause a reduction in feedwater flow and prevent that channel from tripping. A reactor trip on low-low water level, independent of indicated feedwater flow, will ensure a reactor trip if needed.

7.2.3.2.12 Steam Flow

A spurious low steam flow signal would have the same effect as a high feedwater signal, discussed above.

7.2.3.2.13 Steam Generator Level

A spurious high water level signal from the protection channel used for control will tend to close the feedwater valve. This level channel is independent of the level and flow channels used for reactor trip on low flow coincident with low level.

1. A rapid increase in the level signal will completely stop feedwater flow and lead to an actuation of a reactor trip on low feedwater flow coincident with low level.
2. A slow drift in the level signal may not actuate a low feedwater signal. Since the level decrease is slow, the operator has time to respond to low-level alarms. Since only one steam generator is affected, automatic protection is not mandatory and reactor trip on two-out-of-three low-low level is acceptable.

7.2.3.2.14 Steam Line Pressure

Three pressure channels per steam line are used for steam break protection (two out of three (2/3) low-pressure signals for any steam line actuates SI). One of these channels is used to control

the power-operated relief valves on the steam line. A spurious high-pressure signal from the channel used for control will open the power operated relief valve and cause steam line low-pressure. In the analysis of steam breaks of this size, no credit is taken for the steam line pressure instrumentation. SI is actuated by the pressurizer instrumentation. Therefore, control failure does not create a need for the steam break protection, and two-out-of-three (2/3) logic is acceptable.

7.2.3.3 Normal Operating Environment

Temperature in the Control Room and relay room is maintained for personnel comfort at 75°F ±10°. Protective equipment in this space is designed to operate within design tolerance over this temperature range. This equipment will perform its protective function in an ambient of 110°F.

Temperatures for specific areas are provided in Appendix C of the Environmental Qualification (EQ) Plan.

Within containment, the normal operating temperature for protective equipment except out-of-core neutron detectors is maintained below 135°F.

Protective instrumentation is designed for continuous operation within design tolerance in this environment. Out-of-core neutron detectors are designed for continuous operation at 135°F, and the normal operating temperature is maintained below this value. The reactor gap and neutron detector cooling system has two 100 percent capacity fans, with operation of only one of the fans being sufficient to maintain the temperature below that specified. Should both fans fail, an alarm is initiated in the Control Room. Therefore, it is not necessary to consider any error induced as a result of loss of cooling. The detectors will withstand operation at 175°F for short durations (eight hours). Process instrumentation in containment, which is vital to monitoring plant status following a LOCA, is designed to operate within design tolerances in the post-accident environment.

Qualification testing has been performed on various safety system components such as process instrumentation, nuclear instrumentation, and relay racks. This testing involved demonstrating operation of safety functions at elevated ambient temperatures at 110°F for Control Room equipment and in full post-accident environment for required equipment in containment. Detailed results of some of these tests are proprietary to the suppliers, but are kept on file by the suppliers and are available for audit by qualified parties. Qualification of sensors required to operate in the post-accident environment is discussed in Reference 5.

7.2.3.4 Protection System Reliability

A detailed failure analysis of the reactor protection system is presented in WCAP-7486 (Reference 6), which considers both random component failures and systematic or common-mode failures. The Indian Point Unit 2 plant was originally used as a basis for the study, but results are

generally applicable to the present generation of Westinghouse Pressurized Water Reactor Plants including the Kewaunee Nuclear Power Plant.

A program has been established to assess unscheduled reactor trips. This program, ensures that adequate procedures, data and information sources exist to ensure an understanding of the cause(s) and progression of a trip. This includes the capability to determine whether safety limits had been exceeded and if so, to what extent.

If the cause of a trip cannot be determined or if all problems are not resolved, then the Plant Manager or his designate must give approval to restart the plant. In addition, the Plant Operations Review Committee will perform an independent assessment of all reactor trips. These procedures, implemented to ensure RTS reliability, have been approved by the NRC and fulfill the requirements of Items 1.1 and 1.2 of Generic Letter 83-28 (see NRC SERs in Reference 11, Reference 12 and Reference 13).

The reactor trip breakers, located in the switchgear room through which the feedwater line passes, are protected from physical damage from pipe whip or jet impingement in the event of failure of this line. Reactor trip is initiated by steam flow-feedwater flow mismatch coincident with low steam generator level in the event of a feedwater line break. This signal is backed up by a low-low steam generator level trip. Both signals have been designed to comply with IEEE-279.

The control rod drive equipment room is approximately 50 feet by 50 feet in area, is ventilated through the normal Turbine Building Ventilation System, and can provide 4000 cfm of air. The control rod drive equipment room fan-coil units can provide an additional 4000 cfm of air to the room.

In the event of a small feedwater line break, the feedwater flashing to steam will be contained in a guard pipe, which provides small feedwater break protection to the CRDM Equipment room. This guard pipe totally encloses the feedwater line inside the CRDM room. Consequently, the steam or water will be directed to the adjacent non-steam exclusion areas (see Section 10A.4 for more detail).

7.2.3.5 Tests and Inspections

A plan for periodic component and system testing and material examinations was prepared prior to plant operation for use throughout plant life.

In accordance with Items 4.5.2 and 4.5.3 of Generic Letter 83-28, on-line testing of the Reactor Trip System (RTS), including testing of the diverse trip features of the reactor trip breakers, is performed periodically. The surveillance test intervals for the RTS are determined by the NRC approved topical report located in Reference 14. These test intervals are consistent with achieving high RTS reliability and an increase in the testing frequency would not appreciably lower the estimates of failure probability (see NRC SERs in Reference 15 and Reference 16).

Periodic maintenance of the reactor trip breakers (RTBs), including lubrication, housekeeping and other items recommended by the vendor, is performed during the refueling outage. The interval between maintenance checks satisfies the NRC requirements of Item 4.2.1 of Generic Letter 83-28 provided that 200 RTB trips are not exceeded in the interval. The original commitment (annual testing) was updated to allow RTB testing to be performed on a refueling outage basis, which is currently 18 months. As required by Item 4.2.2 of the same letter, maintenance work requests and incident reports, as well as test results, are trended in accordance with the general requirements of the plant's general Quality Assurance Program Description to forecast the degradation of operability of the RTBs (see NRC SER in Reference 17). It should be noted that the incident report program was replaced in 1995 by the Kewaunee Assessment Program.

7.2 References

1. Vogeding, E., "Seismic Testing of Electrical and Control Equipment," WCAP 7817, December 1971
2. Lipchak, J., R. Bartholomew, "Test Report Nuclear Instrumentation System Isolation Amplifier," WCAP 7819, January 1972
3. Burnett, T. W. T., "Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors," WCAP 7306, April 1969
4. Gerber, "Isolation Amplifier," WCAP 7685, June l971
5. Locante J., E.G. Igne, "Environmental Testing of Engineered Safety Features Related Equipment," WCAP 7744, September 1971
6. Gangloff, W. C., "An Evaluation of Anticipated Operational Transients in Westinghouse Pressurized Water Reactors," WCAP 7486, May 1971
7. Nay, J. H., "Topical Report, Process Instrumentation for Westinghouse NSSS Four Loop Plants," WCAP 7671, April 1971
8. Lipchak, J. B., R. A. Stokes, W. Patalon, "Topical Report, Nuclear Instrumentation Systems," WCAP-7380-L, January 1971
9. NRC Safety Evaluation Report, S. A. Varga (NRC) to D. C. Hintz (WPS), Letter No. K-84-239, November 26, 1984
10. NRC Safety Evaluation Report, M. B. Fairtile (NRC) to D. C. Hintz (WPS), Letter No. K-86-168, August 21, 1986
11. NRC Safety Evaluation Report, S. A. Varga (NRC) to D. C. Hintz (WPS), Letter No. K-85-212, October 9, 1985

12. NRC Safety Evaluation Report, J. G. Giitter (NRC) to C.R. Steinhardt (WPS), Letter No. K-89-60, March 27, 1989

13. NRC Safety Evaluation Report, S. A. Varga (NRC) to D.C. Hintz (WPS), Letter No. K-85-104, May 15, 1985

14. Andre, G. R., R. C. Howard, R. L. Jansen, K. Leonelli, "Evaluation of Survey Frequencies and Out of Service Times for the Engineered Safety Features Actuation System," WCAP-10271, May 1989

15. NRC Safety Evaluation Report, M. B. Fairtile (NRC) to D. C. Hintz (WPS), Letter No. K-87-24, January 28, 1987

16. NRC Safety Evaluation Report, J. G. Giitter (NRC) to C. R. Steinhardt (WPS), Letter No. K-89-129, June 2, 1989

17. NRC Safety Evaluation Report, S. A. Varga (NRC) to D. C. Hintz (WPS), Letter No. K-85-150, July 18, 1985

18. IEEE 344-1987, "Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generation Stations"

19. IEEE 323-1983, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations"

20. WCAP-8687, Supplement 2-E47C, Rev. 0, Addendum 4, "Equipment Qualification Test Report Nuclear Instrumentation System (NIS) Power Range Drawer Assemblies Environmental and Seismic Testing," May 1992

Table 7.2-1
List of Reactor Trips and Causes of Actuation of Engineered Safety Features,
Containment and Steam Line Isolation and Auxiliary Feedwater

	Coincidence Circuitry and Interlocks	Comments
	Reactor Trip	
1. Manual	1/2, no interlocks	
2a. High Neutron Flux (Low Set Point)	2/4, low setting interlocked with P10	Manual block and automatic reset of low setting by P10, Table 7.2-2
2b. Power Range High Neutron Flux (High Set Point)	2/4, no interlocks	
3. Overtemperature ΔT	2/4, no interlocks	
4. Overpower ΔT	2/4, no interlocks	
5. Pressurizer Low Pressure	2/4, interlocked with P7	
6. Pressurizer High Pressure	2/3, no interlocks	
7. Pressurizer High Water Level	2/3, interlocked with P7	
8a. Reactor Coolant Low-Flow[a]	2/3 per loop, interlocked with P7 and P8	Both loops blocked below P7 Single loop blocked below P8
8b. Monitored Electrical Supply for Reactor Coolant Pumps		
8b1. RCP Bus Undervoltage	2/2 buses sensed by 1/2 sensors per bus, interlocked with P7	Blocked below P7

Table 7.2-1
List of Reactor Trips and Causes of Actuation of Engineered Safety Features,
Containment and Steam Line Isolation and Auxiliary Feedwater

	Coincidence Circuitry and Interlocks	Comments
8b2. RCP Breakers Open[b]	Interlocked with P7 and P8	Underfrequency or undervoltage on 2/2 buses, sensed by 1/2 sensors per variable per bus, trips both RCP breakers. Both loops blocked below P7. Single loop blocked below P8.
8b3. RCP Bus Underfrequency	2/2 buses sensed by 1/2 sensors per bus, interlocked with P7	Blocked below P7
9. SIS (Actuation) (S)	Low pressurizer pressure (2/3); 2/3 high containment pressure or manual 1/2; or 2/3 low steam pressure from either loop	An S signal results in the following actions: Trips main feedwater pumps and associated discharge valves, closes all feedwater control valves, trips reactor, actuates AFW pumps, isolates steam lines in coincidence with other signals.
10. Turbine-Generator Trip	2/3 low auto-stop oil pressure or 2/2 stop valve closure indication, both interlocked with P7	
11. Steam/Feedwater Flow Mismatch	1/2 steam/feedwater flow mismatch in coincidence with 1/2 low steam generator water level per loop	
12. Low-Low Steam Generator Water Level	2/3 either loop	
13. Intermediate Range Neutron Flux	1/2, manual block permitted by P10	Manual block and automatic reset
14. Source Range Neutron Flux	1/2, manual block permitted by P6, interlocked with automatic block with P10	Manual block and automatic reset

Table 7.2-1

List of Reactor Trips and Causes of Actuation of Engineered Safety Features, Containment and Steam Line Isolation and Auxiliary Feedwater

	Coincidence Circuitry and Interlocks	Comments
15. Power Range Positive Neutron Flux Rate	2/4, no interlocks	
16. Power Range Negative Neutron Flux Rate	2/4, no interlocks	
	Containment Isolation Actuation	
17. SIS	See Item 9	
18. Manual Containment Isolation	One out of two (1/2)	
19. Containment Ventilation Isolation Actuation	High activity signal, from air particulate detector or radiogas detector or 1/2 manual with containment isolation or 2/2 manual with spray actuation or safety injection	This additional signal closes containment purge supply, exhaust ducts and pressure relief ducts only
	Engineered Safety Features Actuation	
20. SIS (S)	See Item 9	
21a. Containment Spray Signal (P)	Three - 1/2 containment pressure (Hi- Hi) in coincidence	
21b. Manual Spray	Two out of two (2/2)	
22. Containment Air Cooling Signal	SIS initiates starting of all fans in accordance with the Safety Injection Starting Sequence	

Table 7.2-1

List of Reactor Trips and Causes of Actuation of Engineered Safety Features, Containment and Steam Line Isolation and Auxiliary Feedwater

	Coincidence Circuitry and Interlocks	Comments
	Steam Line Isolation Actuation	
23. Steam Flow	Coincidence of Hi-Hi steam flow (1/2) in the respective line and SIS or Coincidence of (1/2) high steam flow in the respective line and SIS and (2/4) low T_{avg}	
24. Containment Pressure, Hi-Hi Set Point	2/3 Hi-Hi containment pressure signal	
25. Manual, per steam line	1/1 per steam line	
	AFW Actuation	
26. Turbine Driven Pump	Low-Low level in both steam generators; AMSAC low-low level in both steam generators; or loss of voltage on 2/2 4-kv volt buses	For further information on AMSAC, see Section 14.1.11.
27. Motor Driven Pumps	Low-Low level in either steam generators; AMSAC low-low level in both steam generators; or trip of 2/2 main feedwater pumps if no S signal or blackout signal is present. SI sequence or blackout sequence signals if present	

Table 7.2-1
List of Reactor Trips and Causes of Actuation of Engineered Safety Features,
Containment and Steam Line Isolation and Auxiliary Feedwater

	Coincidence Circuitry and Interlocks	Comments
	Main Feedwater Isolation	
28. Close Main Feedwater Control Valves, Trip Main Feedwater Pumps	1. S Signal 2. Reactor trip coincident with low T_{avg} 3. 2/3 Hi-Hi steam generator level closes the valves to the faulty steam generator	Reactor trip coincident with low T_{avg} low T_{avg} does not trip the main feedwater pumps.
	Turbine Building Service Water (SW) Isolation	
29. Close Turbine Building SW Supply Valves	1. S Signal 2. Low SW header pressure (respective header)	Redundant on system level

Definition of “S,” “T,” and “P” signals:

Signal:	Initiated by:	Action:
“S”	SIS	Actuates SI
“T”	Containment Isolation Signal	Actuates containment isolation
“P”	3-1/2 Hi-Hi containment pressure	Activates containment spray

a. In the plant, P7 and P8 are set at approximately the same point.
b. In the plant, P7 and P8 are set at approximately the same point.

Table 7.2-2
Permissive Interlock Circuits

Number	Function	Required Input
P1	Prevent rod withdrawal on over-power	1/4 high neutron flux (power range); or 1/2 high nuclear flux (intermediate range); or 2/4 over-temperature ΔT; or 2/4 overpower ΔT
P2	Auto-rod withdrawal stop at low power	Low MWe (15% power) load signal (turbine pressure)
P4	Actuate turbine trip; closes main feedwater valves on T_{avg} below setpoint; prevents opening of main feedwater valves which were closed by SI or high steam generator water level; allows manual block of the automatic re-actuation of SI.	Reactor trip
	Defeats the block of the automatic re-actuation of SI.	Reactor not tripped
P5	Steam dump interlocks	Rapid decrease of MWe load signal (turbine pressure)
P6	Allows manual block of source range trip	1/2 high intermediate range flux allows manual block, 2/2 low intermediate range defeats block
P7	Block various trips at low power	3/4 low-low neutron flux (power range) and 2/2 low MWe load signal (turbine pressure)
P8[a]	Block single primary loop loss-of-flow trip	3/4 low neutron flux (power range)
P9[b]		
P10	Allows manual block of power range trip (low setpoint); and allows manual block of intermediate range trip; actuate blocked source range trip	2/4 power range neutron flux allows manual block; 3/4 low neutron flux (power range) defeats manual block of power range and of intermediate range trips

a. In this plant, P7 and P8 are set at approximately the same point.
b. Not applicable to this plant.

Table 7.2-3
Rod Withdrawal Stops

Rod Stop	Actuation Signal	Rod Motion To Be Blocked
1. Nuclear Overpower	1/4 high power range neutron flux or 1/2 high intermediate range neutron flux	Automatic and Manual Withdrawal
2. High ΔT	2/4 overpower ΔT or 2/4 over-temperature ΔT (initiates turbine load reduction)	Automatic and Manual Withdrawal
3. Low Power	Low MWe load signal (below 15%) for low turbine impulse pressure	Automatic Withdrawal

Figure 7.2-1 Reactor Protection Systems

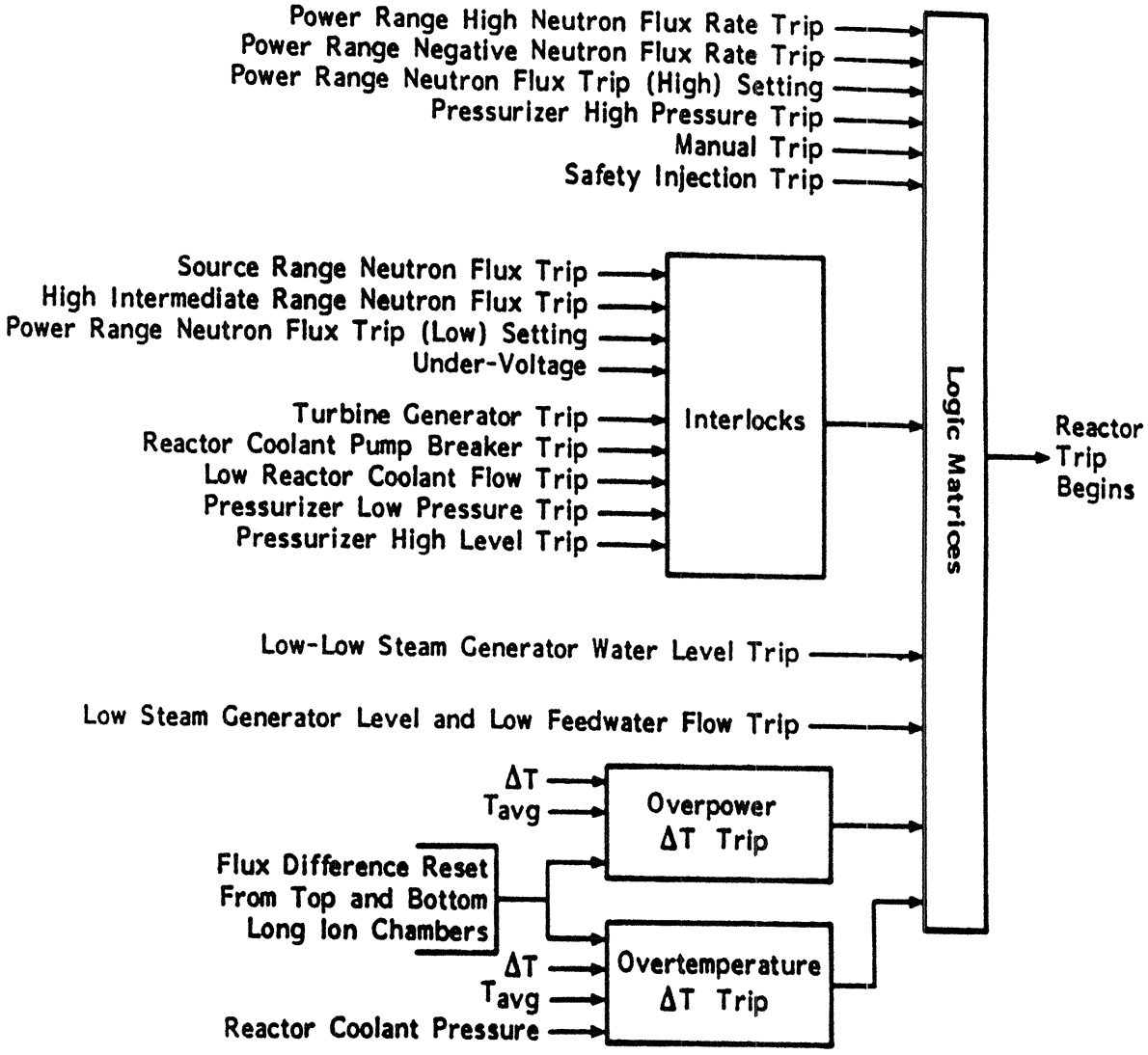


Figure 7.2-2 Design Philosophy to Achieve Isolation Between Channels

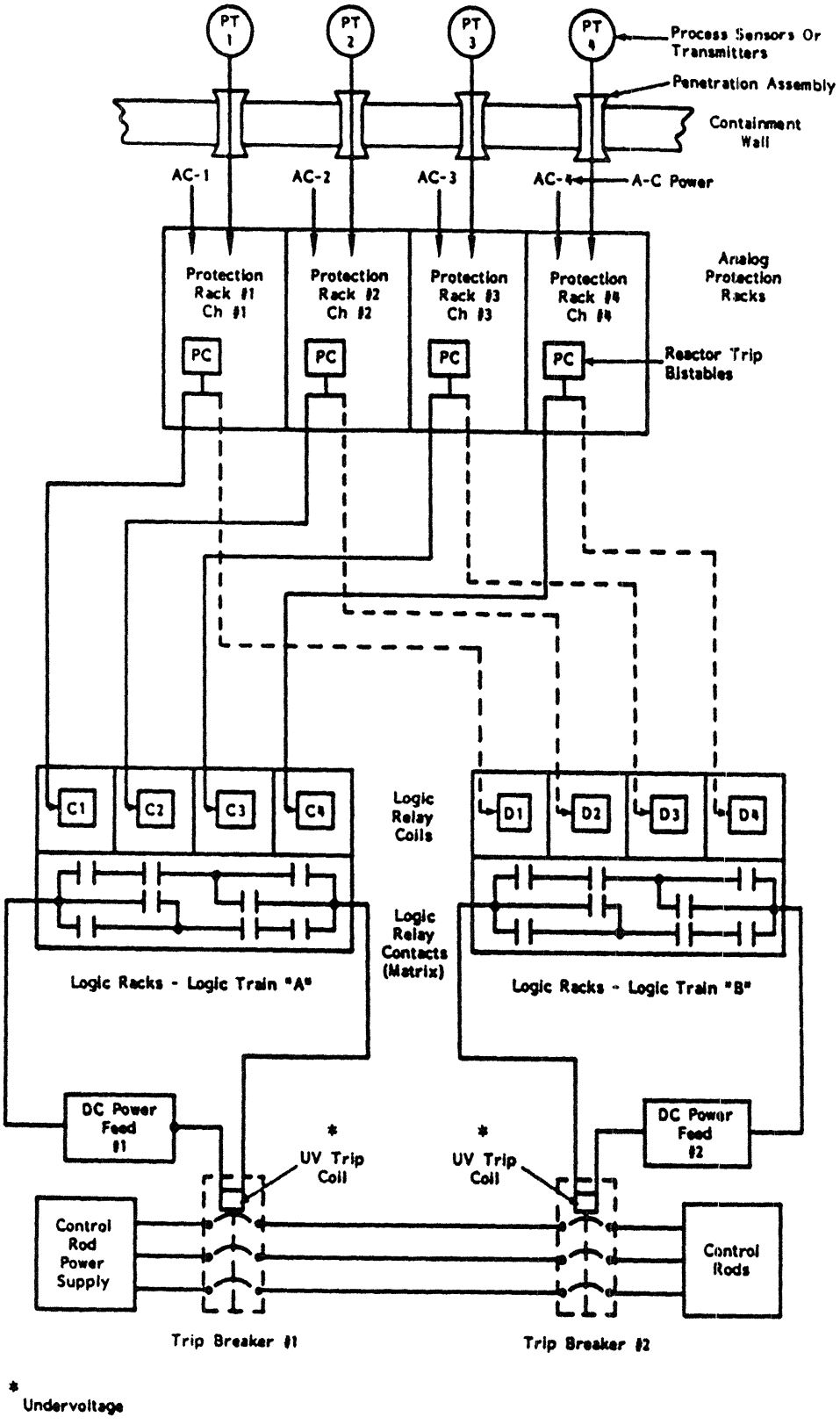


Figure 7.2-3 Typical Channel Testing Arrangement

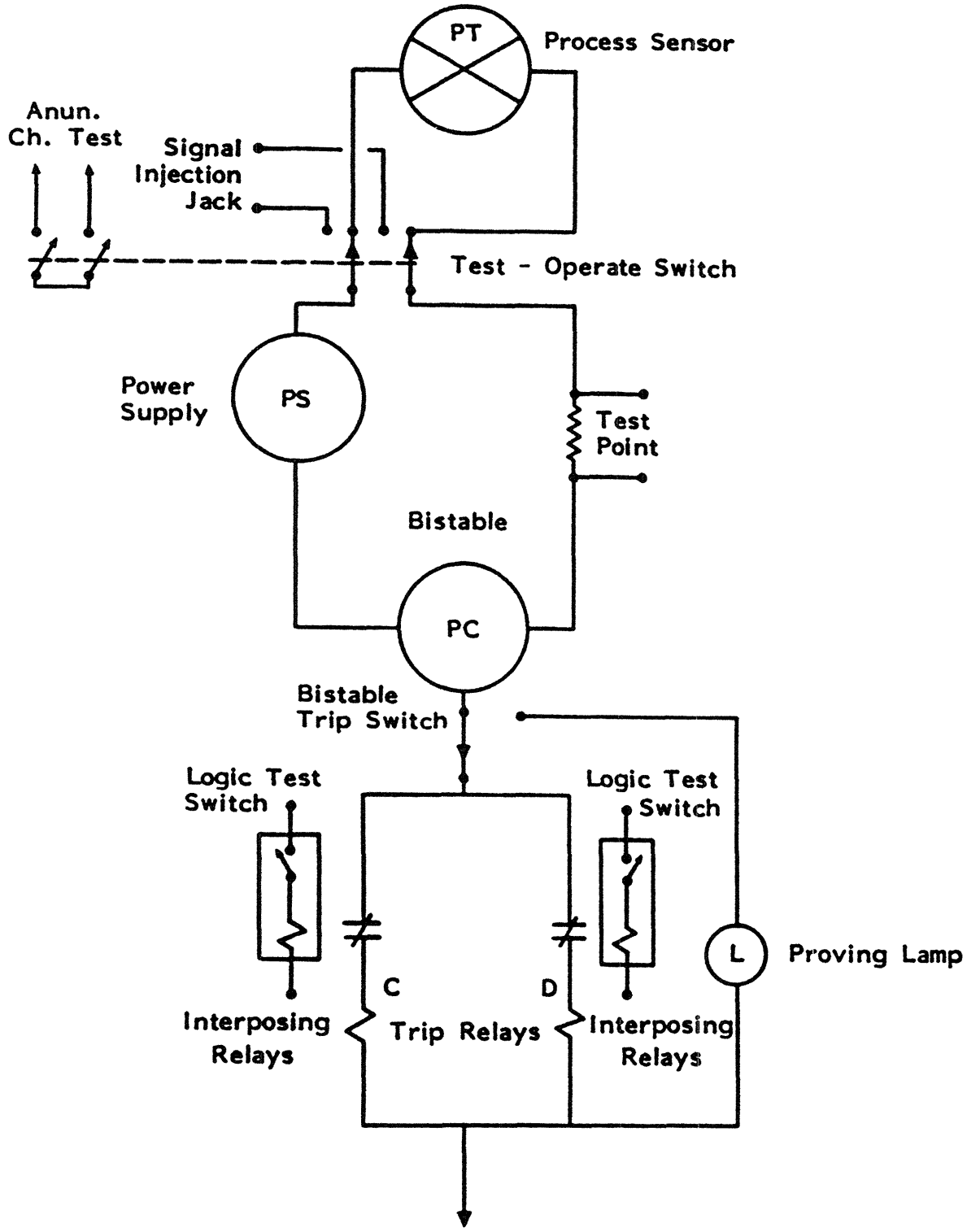


Figure 7.2-4 Trip Logic Channels

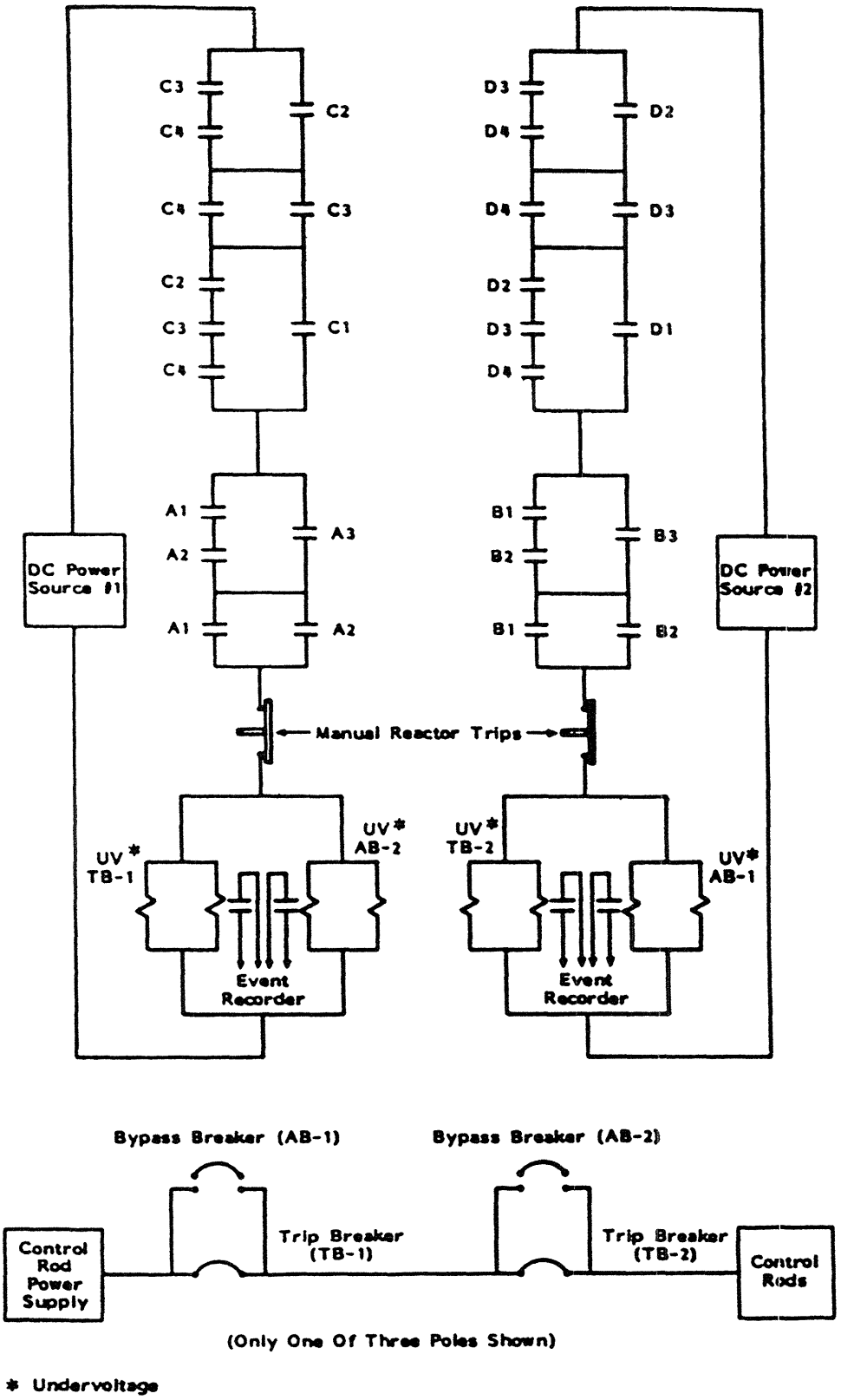
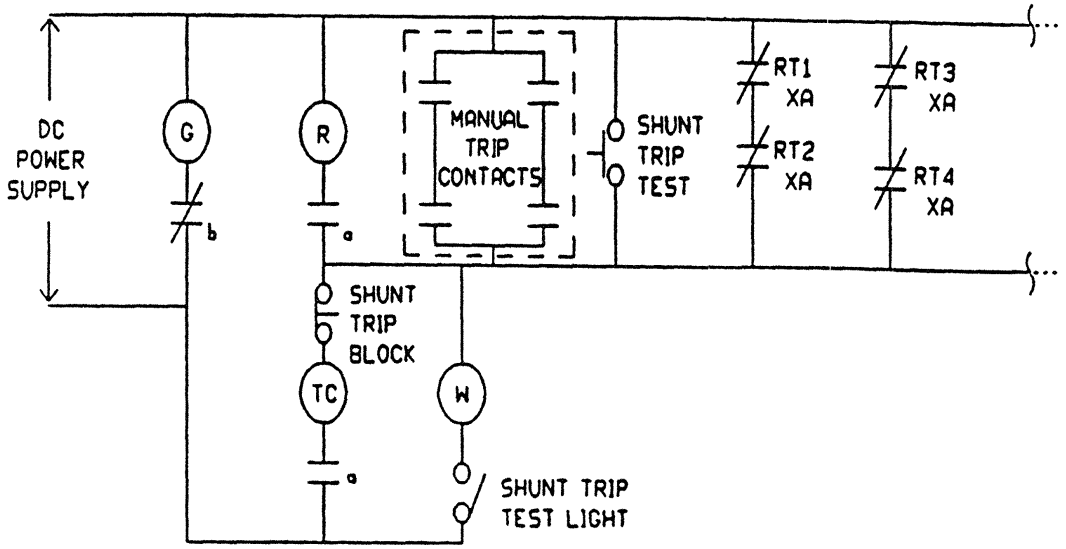


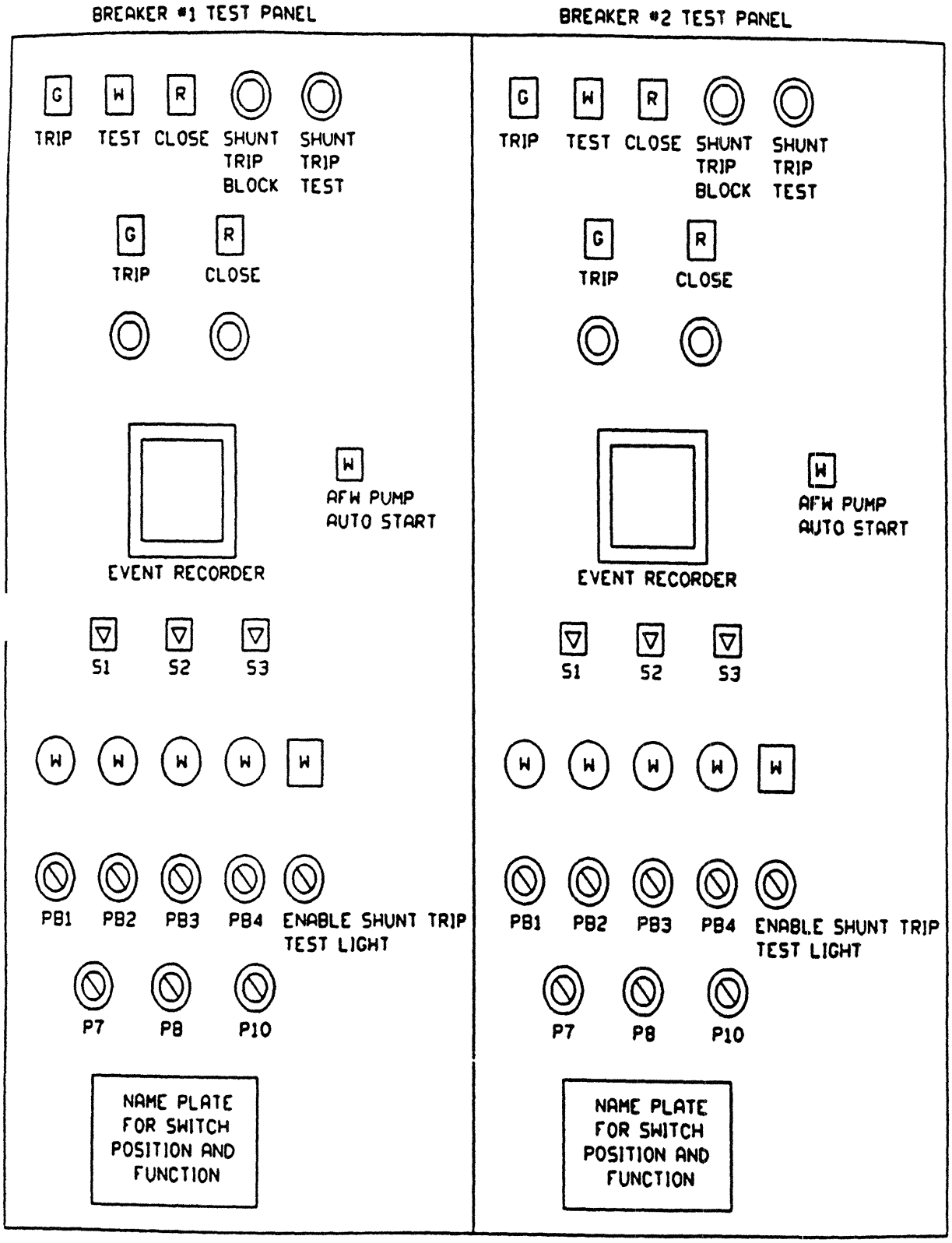
Figure 7.2-5 Shunt Trip Circuit (Shown with Train A Reactor Trip Relays)



LEGEND

RT(N) - Reactor Trip Relay, N=1 through 12, A or B train
X (A or B)
R - red
G - green
W - white
TC - trip coil
a, b - auxiliary contacts from reactor trip breaker

Figure 7.2-6 Logic Channel Test Panels



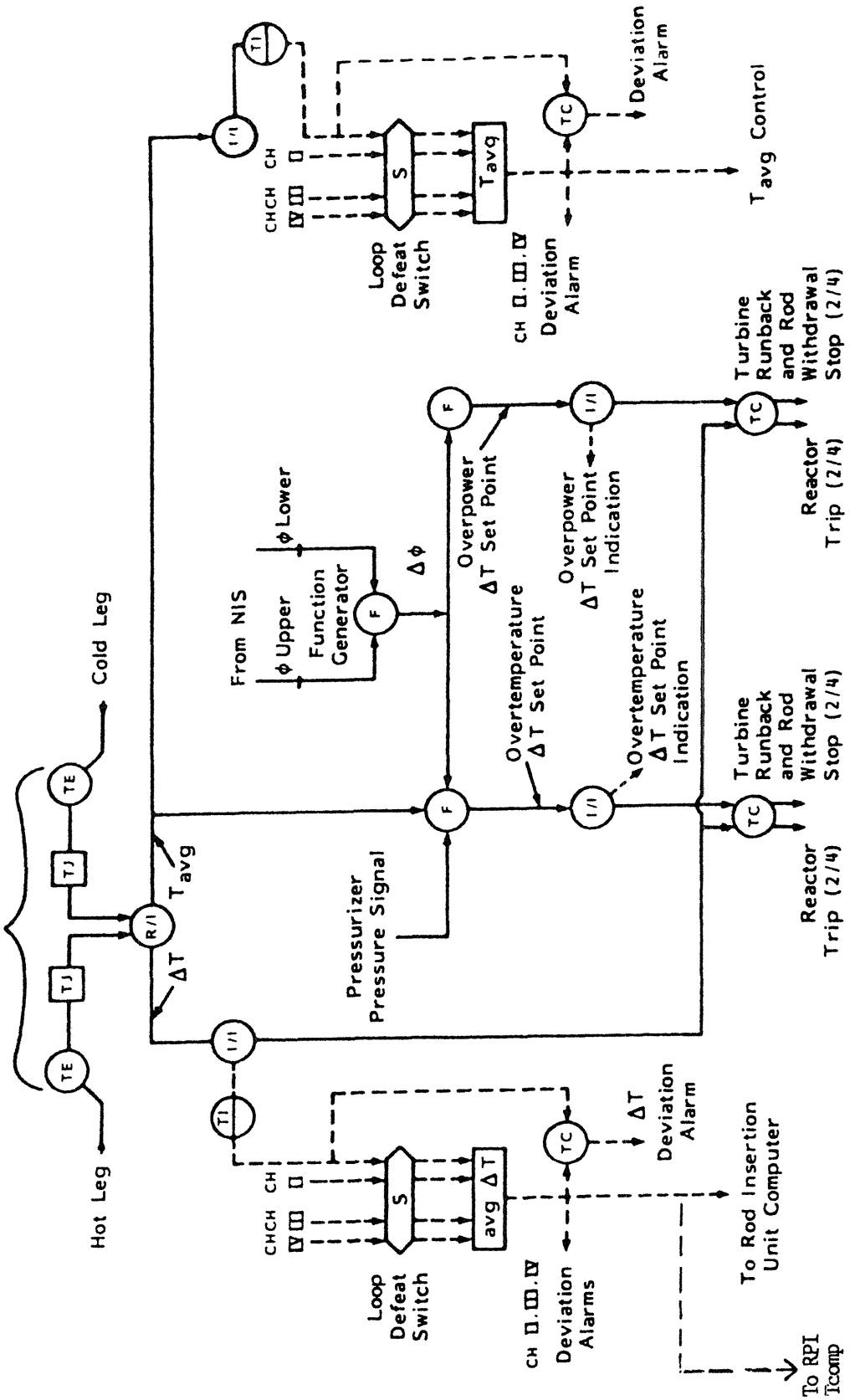


Figure 7.2-7 $T_{avg}/\Delta T$ Control and Protection System (Single Channel)

Figure 7.2-8 Analog System Symbols

AI - Alarm
Buf - Buffer
F - Special Function (such as a pressure compensation unit, lead/lag compensator, multiplier/Sq. Rt. Extractor)
FC - Flow Controller (off-on unless output signal is shown)
FI - Flow Indicator
FT - Flow Transmitter
Hi LRT - High Level Reactor Trip
Hi PRT - High Pressure Reactor Trip
I/I - Isolation Current Repeater
ISOL - Isolation (other than I/I)
LC - Level Controller (off-on unless output signal is shown)
LI - Level Indicator
L/L - Lead/Lag
L-Low; LOL - Low Level
Lo LRT - Low Level Reactor Trip
Lo PRT - Low Pressure Reactor Trip
L_{ref} - Programmed Reference Level
LT - Level Transmitter
NC - Neutron Flux Controller
NE - Neutron Flux Detector
NI - Neutron Flux Indicator
NM - Neutron Flux Signal Modifier
NQ - Nuclear Instrumentation Power Supply
PC - Pressure Controller (off-on unless output signal is shown)
PI - Pressure Indicator
PM - Pressure Signal Modifier
P_{ref} - Programmed Reference Pressure
PS - Power Supply
PI - Pressure Indicator
PT - Pressure Transmitter
QM - Neutron Flux Signal Modifier
R/I - Resistance to Current Converter
RTD - Resistance Temperature Detector
S - Control Channel Transfer Switch (used to maintain auto channel during test of the protection channel)
SI - Safety Injection
T - Built-in Test Point
TC - Temperature Controller
TE - Temperature Element
TI - Temperature Indicator
TJ - Test Signal Insertion Jack
TM - Temperature Signal Modifier
TP - Test Point
T_{ref} - Reference Temperature
ϕU,L - Out of Core Upper Or Lower Ion Chamber Flux Signals

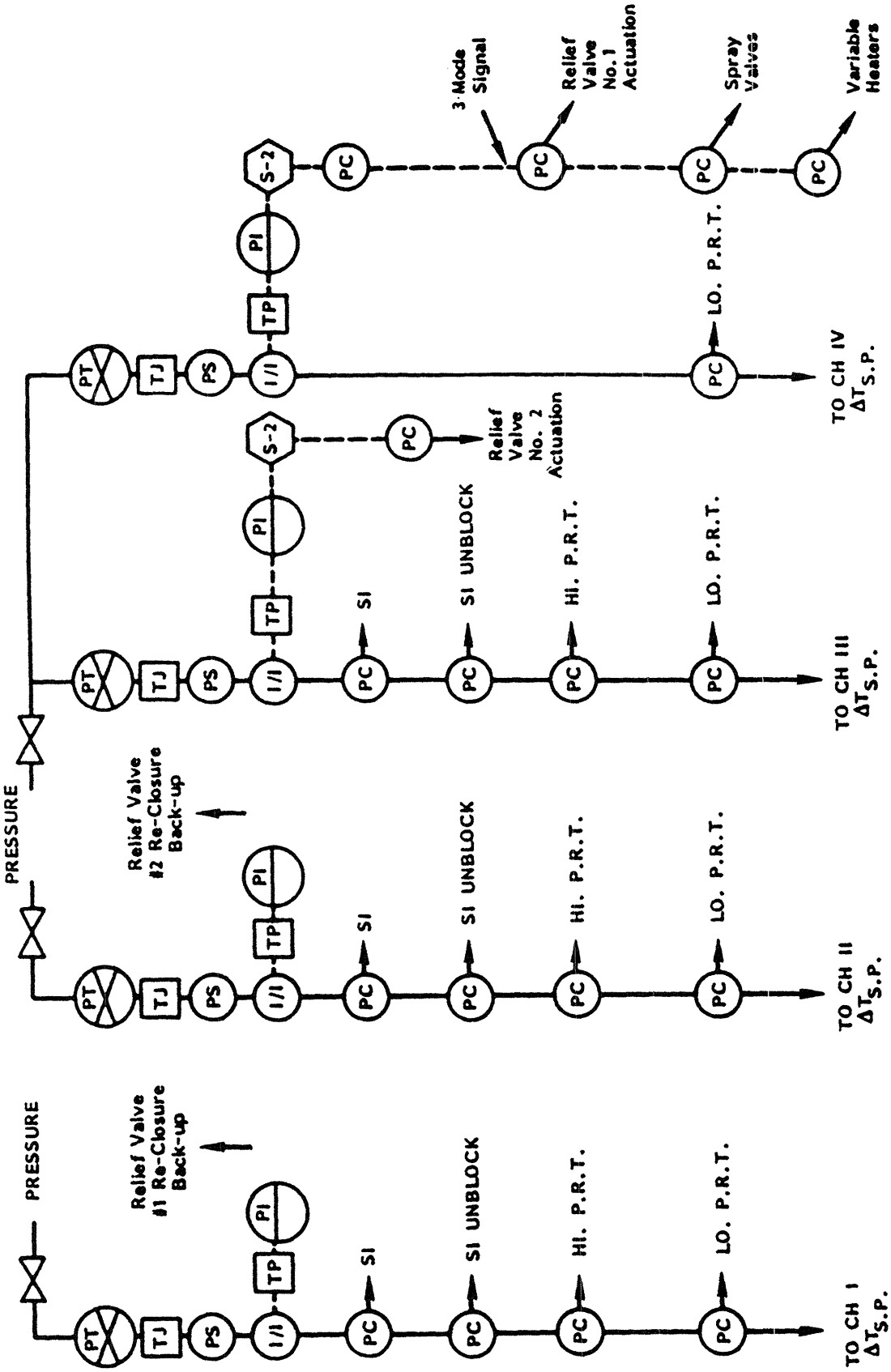


Figure 7.2-9 Pressurizer Pressure Control and Protection System

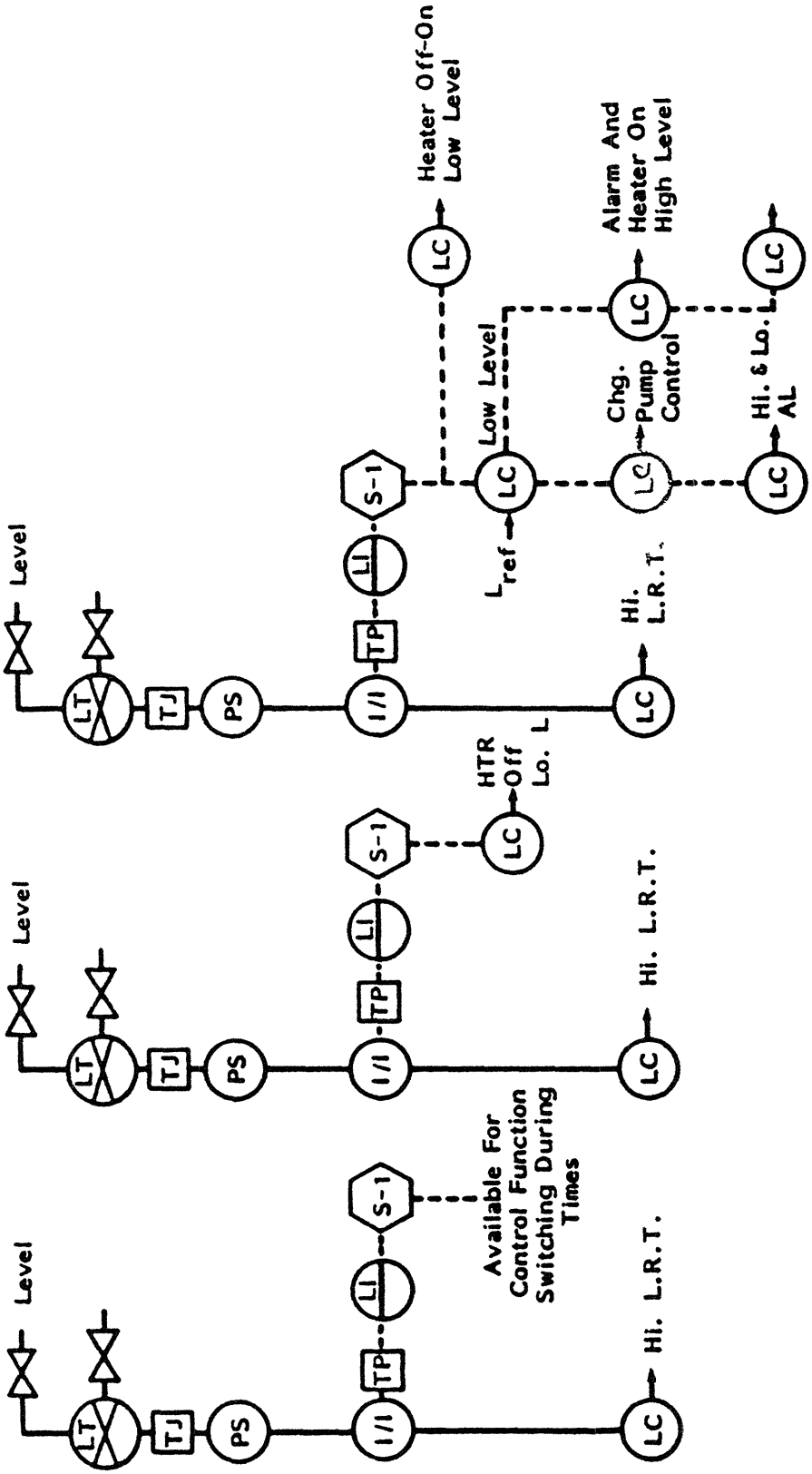
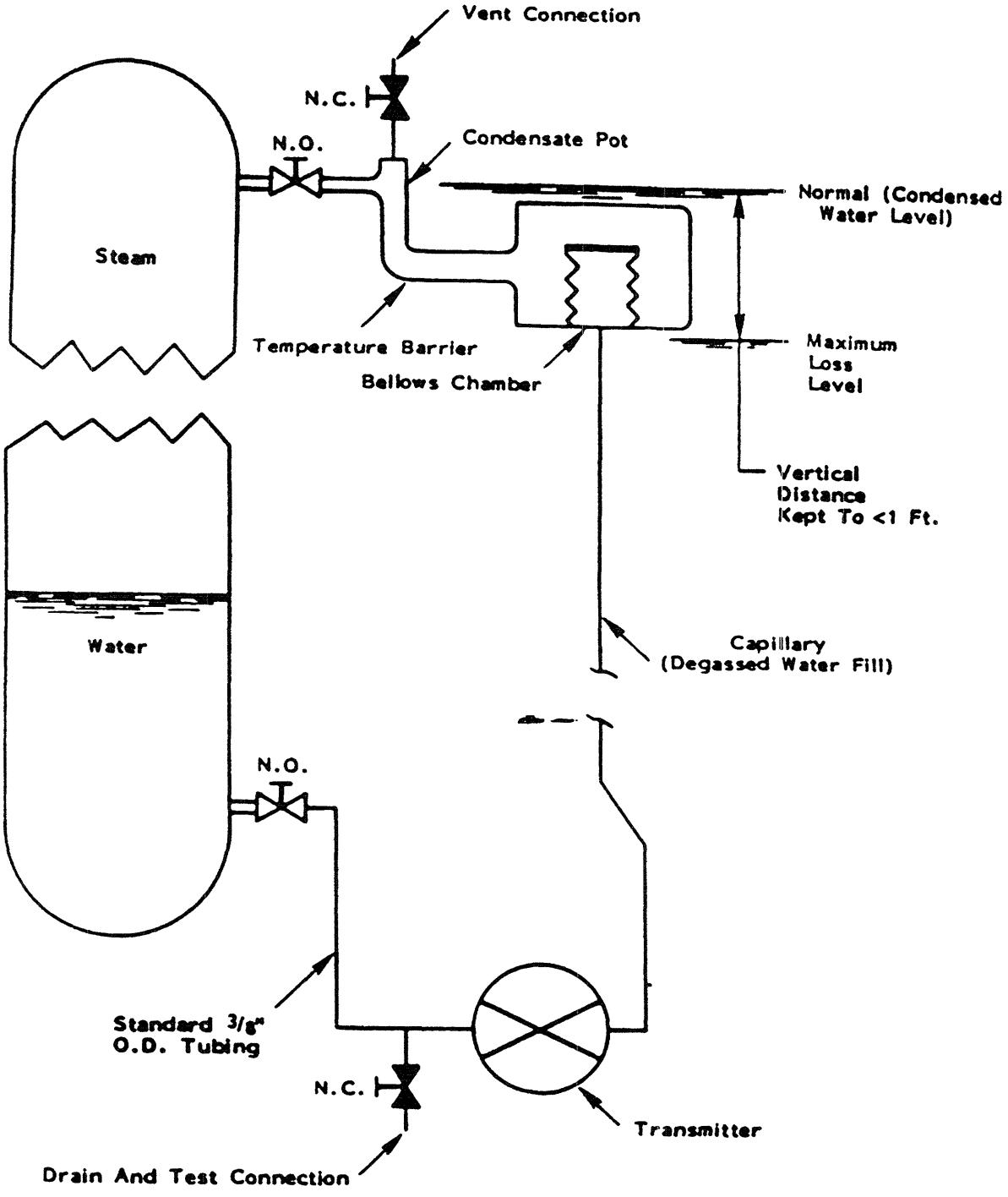


Figure 7.2-10 Pressurizer Level Control and Protection System

Figure 7.2-11 Pressurizer Level Measurement Reference-Leg Typical Arrangement



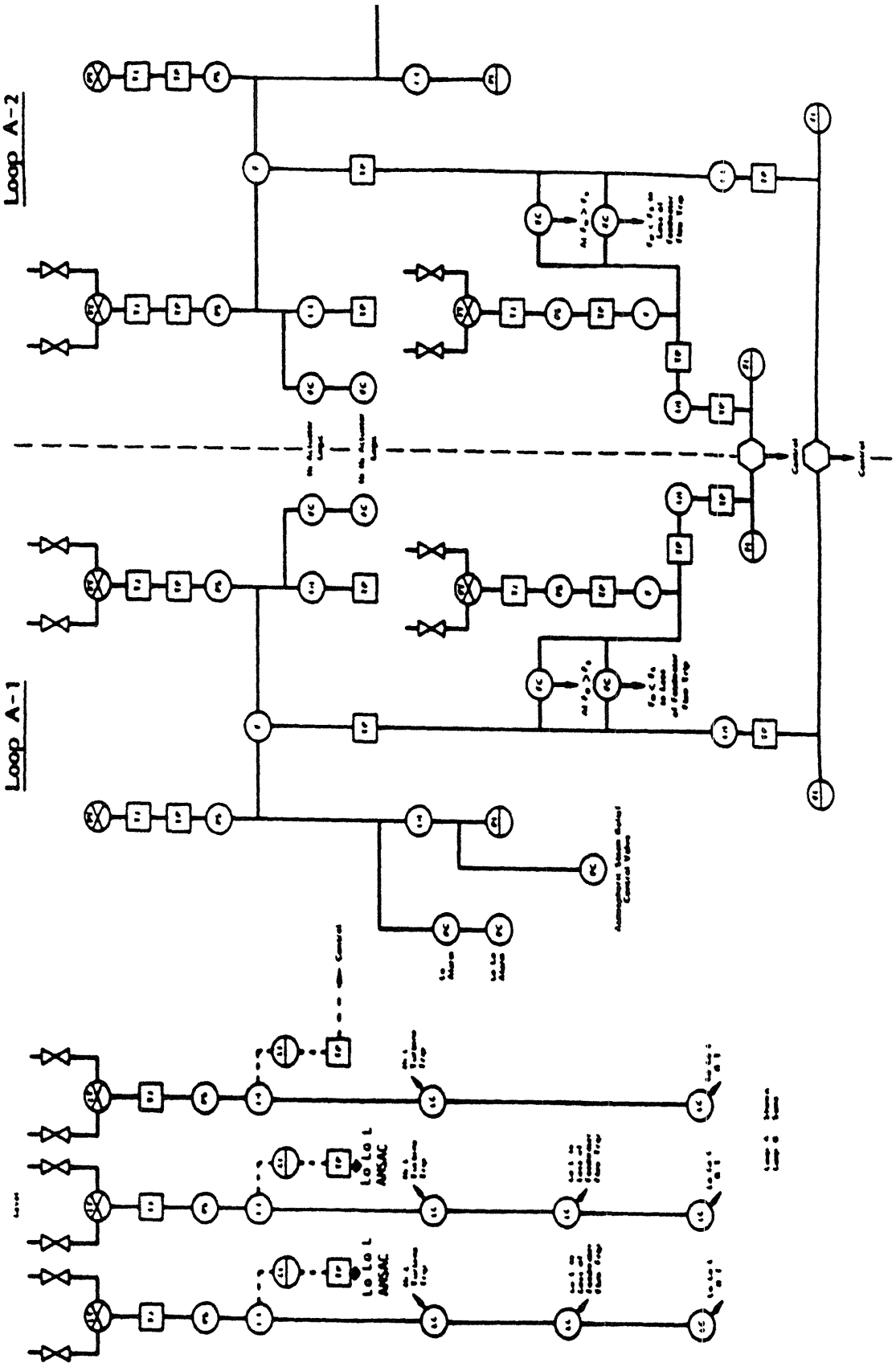


Figure 7.2-12 Steam Generator Level Control and Protection System

7.3 REGULATING SYSTEMS

7.3.1 Design Basis

The reactor automatic control system is designed to reduce transients for the design load perturbations, so that reactor trips will not occur for these load changes.

Overall reactivity control is achieved by the combination of chemical shim 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 or reactor trip is accomplished by moving RCCAs.

The function of the RCS is to provide automatic control of the RCCAs during power operation of the reactor. The system uses input signals including neutron flux, coolant temperature and turbine load. The Chemical and Volume Control System (Chapter 9) supplements the reactor control system by the addition and removal of varying amounts of boric acid solution.

When the reactor is critical, the best indication of reactivity status in the core is the position of the control group in relation to plant power and average coolant temperature. There is a direct relationship between control rod position and power and it is this relationship which establishes the lower insertion limit calculated by the rod insertion limit monitor. There are two alarm setpoints to provide warning to take corrective action in the event a control group approaches or reaches its lower limit.

Any unexpected change in the position of the control group 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. Periodic samples of coolant boron concentration are taken. The variation in concentration during core life provides a further check on the reactivity status of the reactor including core depletion.

The Reactor Control System is designed to enable the reactor to follow load changes automatically when the plant output is above approximately 15 percent of nominal power. Control rod positioning may be performed automatically when plant output is above this value, and manually at any time.

The system enables the nuclear plant to accept a step load increase of 10 percent and a ramp increase of 5 percent per minute within the load range of 15 to 95 percent without reactor trip, subject to possible xenon limitations. Similar step and ramp load reductions are possible within the range of 100 percent to 15 percent of nominal power without steam dump. The steam dump system permits the plant to accept a 50 percent loss of load without reactor trip. This is further discussed in Section 7.3.2, Section 7.3.3, and Chapter 10. The control system is designed to restore coolant average temperature to within the programmed temperature limits, following any of the above changes in load.

The pressurizer water level is programmed to be a function of the auctioneered coolant average temperature. This is to minimize the requirements on the Chemical and Volume Control and Waste Disposal System resulting from coolant density changes during loading and unloading from full power to zero power.

Following a reactor and turbine trip, sensible heat stored in the reactor coolant is removed without actuating the steam generator safety valves by means of a steam dump system. RCS temperature is reduced to the no-load condition. This no-load coolant temperature is maintained by the steam dump system.

The Control System provides operation as a stable system over the full range of automatic control throughout core life without requiring routine operator adjustments of set points.

7.3.2 System Design

The Power Regulating System can be broken down into two subsystems as follows:

1. Rod Control System
   a. Rod Drive Programmer
      (i) Full Length rod control
   b. Rod Position Indication
      (i) Individual (Actual rod position)
      (ii) Bank (Demand rod position)
2. Steam Dump Control

A simplified block diagram of the RCS is shown in Figure 7.3-1.

7.3.2.1 Rod Control

There are a total of 29 full-length RCCAs. The 4 part-length rods have been removed and are not used in this reactor. Full-length RCCAs are divided into:

1. 2 shutdown banks with 4 assemblies in each bank; and
2. 4 control banks containing 8, 4, 5 and 4 assemblies, respectively.

Figure 3.2-1 shows the location of the full-length RCCAs in the core. The four control banks are the only rods that can be manipulated under automatic control. The banks are divided into groups to obtain smaller incremental reactivity changes. All RCCAs in a group are electrically paralleled to step simultaneously.

The drive mechanisms used in conjunction with full-length RCCAs are capable of permitting free fall of the assemblies.

The automatic rod control system maintains the coolant average temperature by adjusting the RCC assembly positions.

The RCS is capable of restoring programmed average temperature following a change in load. The coolant average temperature increases linearly from zero power to full power.

The control system could also initially compensate for reactivity changes caused by fuel depletion and/or xenon transients. Final compensation would then be made by adjusting the boron concentration. The control system then readjusts the control banks in response to changes in coolant average temperature resulting from changes in boron concentration. The normal practice is to use control rods to maintain nuclear axial flux within a specified band and use boron to adjust for xenon and fuel depletion changes.

The coolant temperatures are measured by the hot-leg and cold-leg resistance temperature detectors, which are averaged for each loop. The highest of the four measured average temperatures is the control signal.

This signal is sent to the T_{avg} controller through a lead/lag compensation unit where it is compared with the reference temperature average set by the turbine power. This controller commands the direction and speed of control group rod motion. A power-load mismatch signal is also employed as control signals to improve the plant performance. The power-load mismatch compensation serves to speed up system response and to reduce transient peaks.

The full-length RCCAS are divided into four banks with one or two groups per bank. Each group in a bank is driven by the same variable speed rod drive control unit, which moves the groups sequentially, one step at a time. The sequence of motion is reversible; that is, a withdrawal sequence is the reverse of the insertion sequence. The variable speed sequential rod control affords the ability to insert a small amount of reactivity at low speed to accomplish fine control of reactor coolant average temperature about a small temperature deadband.

Manual control is provided to move a control bank in or out at a pre-selected fixed speed.

Proper sequencing of the RCCAs is assured by fixed programming equipment in the Rod Control System. Startup is accomplished by first manually withdrawing the shutdown rods to the full out position. This action requires that the operator select one of the shutdown banks on a control board mounted selector switch and then position the IN-HOLD-OUT lever (which is spring returned to the HOLD position) to the OUT position. The operator then selects the other shutdown bank and repeats the process.

The control banks are then withdrawn manually by the operator by first selecting the MANUAL position on the control board mounted selector switch and then positioning the IN-HOLD-OUT lever to the OUT position. In the MANUAL selector switch position, the rods

are withdrawn (or inserted) in a predetermined programmed sequence by the automatic programming equipment.

When the reactor power reaches approximately 15 percent, the operator may select the AUTOMATIC position, where the IN-HOLD-OUT level is out-of-service, and rod motion is controlled by the Rod Control System. An interlock limits automatic rod withdrawal to reactor power levels above 15 percent. In the AUTOMATIC position, the rods are again withdrawn (or inserted) in a predetermined programmed sequence by the automatic programming equipment.

The Bank D Rod Withdrawal Limit at 220 steps ensures that the control rods do not automatically withdraw beyond the fully withdrawn position. At about 220 steps, the operator must manually withdraw the control rods.

Programming is set so that as the first bank out reaches a preset position near the top of the core, the second bank out begins to move out simultaneously with the first bank. This staggered withdrawal sequence continues until control rods reach their desired position to control axial flux, normally fully withdrawn at full power. The programmed staggered insertion sequence is the opposite of the withdrawal sequence, i.e., the last control bank out is the first control bank in.

With the simplicity of the rod program, the minimal amount of operator selection, and two separate position indications available to the operator, there is very little possibility that rearrangement of the control rod sequencing could occur.

7.3.2.1.1 Shutdown Groups Control

The shutdown groups of control rods together with the control groups are capable of shutting the reactor down. They are used in conjunction with the adjustment of chemical shim and the control groups to provide shutdown margin of at least 1 percent following reactor trip with the most reactive control rod in the fully withdrawn position.

The shutdown groups are manually controlled during normal operation and are moved at a constant speed. Any reactor trip signal causes them to fall into the core. They are fully withdrawn during power operation and are withdrawn first during startup.

7.3.2.1.2 Full-Length RCC Assembly Position Indication

Two separate systems are provided to sense and display control rod position as described below:

1. Analog System - An analog signal of actual position is produced for each RCCA by a linear position transmitter.

   An electrical coil stack linear variable differential transformer is placed above the stepping mechanisms of the control rod magnetic jacks external to the pressure housing. When the associated control rod is at the bottom of the core, the magnetic coupling between primary and secondary windings is small and there is a small voltage induced in the secondary. As the control rod is raised by the magnetic jacks, the relatively high permeability of the lift rod causes an increase in magnetic coupling. Thus, an analog signal proportional to rod position is derived.

   Direct, continuous readout of every RCCA position is presented to the operator by individual meter indications, without need for operator selection or switching to determine rod position.

   Lights are provided for rod bottom positions for each rod. The lights are operated by bistable devices in the analog system.

2. Digital System - The digital system counts pulses generated in the rod drive control system. One counter is associated with each group of RCCAs. Readout of the digital system is in the form of add-subtract counters reading the number of steps of rod withdrawal with one display for each group. These readouts are mounted on the control panel.

   The digital and analog systems are separate systems; each serves as backup for the other. Operating procedures require the reactor operator to compare the digital and analog readings upon receiving a rod deviation alarm. Therefore, a single failure in rod position indication does not in itself lead the operator to take erroneous action in the operation of the reactor. A detailed description of the control rod drive power supply is presented in Reference 1.

7.3.2.2 Steam Dump

A steam dump system is provided to increase plant operating flexibility for large load reductions of up to 50 percent. The steam dump system removes steam to reduce the transient imposed upon the RCS. The RCS can then reduce the reactor power to a new equilibrium value without causing overtemperature and/or overpressure conditions (see Chapter 10).

Steam dump is actuated when the compensated coolant average temperature exceeds the programmed value by a given amount and electrical load decrease is greater than a given value. All the steam dump valves stroke to full open immediately upon receiving the maximum by-pass demand signal. Steam dump valves are then modulated by the compensated coolant average temperature signal or by the steam header pressure. The steam dump flow decreases proportionally as the control rods act to reduce the coolant average temperature. The artificial

load is therefore removed as the coolant average temperature is restored to its programmed equilibrium value.

7.3.2.3 Feedwater Control

Each steam generator is equipped with a feedwater controller, which maintains a constant water level on the secondary side of the steam generator. The feedwater controller regulates the feedwater valve by continuously comparing the feedwater flow signal, the water level signal and the steam flow signal. The steam generators are operated in parallel, both on the feedwater and on the steam side.

Continued delivery of feedwater to the steam generators is required as a sink for the heat stored and generated in the reactor coolant following a reactor trip and turbine trip. Continued feedwater delivery is assured by the main feedwater pumps and/or AFW System. An override signal closes the feedwater valves upon reactor trip when the coolant average temperature is below a given temperature or when the respective steam generator level rises to a given value (which initiates turbine trip) or upon SIS. Manual override of the feedwater control systems is also provided.

7.3.2.4 Pressure Control

The RCS pressure is maintained at a constant value by using either the heaters (in the water region) or the spray (in the steam region of the pressurizer). The electrical immersion heaters are located near the bottom of the pressurizer. A portion of the heater groups are proportionally controlled to correct small pressure variations. These variations are due to heat losses, including heat losses due to a small continuous spray. The remaining (backup) heaters are turned on either when the pressurizer pressure controller signal is below a given value or when pressurizer level is above a given level.

The spray nozzle is at the top of the pressurizer. Spray is initiated when the pressure controller signal is above a given set point. The spray rate increases proportionally with increasing pressure 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.

Two power relief valves limit system pressure during large load reduction transients. They were designed to open in two seconds or less over the range 2000 to 2400 psig, but can open more slowly and still meet safety analysis assumptions.

Two spring-loaded safety valves limit system pressure following a complete loss of load without direct reactor trip or turbine by-pass.

7.3.2.5 Pressurizer Level Control

A programmed pressurizer water level as a function of auctioneered average reactor coolant temperature is provided in conjunction with the programmed coolant temperature. This minimizes the demands upon the Chemical and Volume Control System and the Waste Disposal System imposed by coolant density changes during loading and unloading. The pressurizer water level decreases as the load is reduced from full load. This is the 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 permit manual control of pressurizer level during startup and shutdown operations, the charging-pump speed can be manually regulated from the main Control Room.

7.3.3 System Design Evaluation

7.3.3.1 Plant Stability

The Rod Control System is designed to limit the amplitude and the frequency of continuous oscillation of coolant average temperature about the control system set point within acceptable values. Because stability is more difficult to maintain at low power under automatic control, rod withdrawal under automatic control is prevented below 15 percent of full power.

7.3.3.2 Step Load Changes Without Turbine Bypass

A typical power control requirement is to restore equilibrium conditions, without a reactor trip, following a plus or minus 10 percent step change in load demand, over the 15 to 95 percent power range for automatic control.

The design must necessarily be based on conservative conditions and a greater transient capability is expected for actual operating conditions.

The function of the control system is to avoid reactor trip through keeping the reactor coolant average temperature deviation during the transient within a given value and to restore average temperature to the programmed set point within a given time. Excessive pressurizer pressure variations are prevented by using spray and heaters in the pressurizer.

The margin between the overtemperature ΔT setpoint and the measured ΔT is of primary concern for the step load changes. This margin, is influenced by neutron flux, pressurizer pressure, reactor coolant average temperature and temperature rise across the core.

7.3.3.3 Loading and Unloading

Ramp loading and unloading is provided under automatic control. The function of the control system is to maintain the coolant average temperature and pressure as functions of turbine generator load. The minimum control rod speed provides a sufficient reactivity rate to compensate for the reactivity changes resulting from the moderator and fuel temperature changes.

The coolant average temperature increases during loading and causes a continuous in-surge 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 out-surge from the pressurizer resulting from coolant contraction. The heaters limit the resulting system pressure decrease. The pressurizer level is programmed such that the water level is above the setpoint at which the heaters cut out during the loading and unloading transients.

The primary concern for the loading rate is to limit the overshoot in coolant temperature so that a margin is provided for the overtemperature ΔT setpoint.

7.3.3.4 Loss of Load With Turbine By-Pass (Steam Dump)

The RCS can prevent reactor trip upon loss of 50 percent load at any reactor power level. The automatic steam dump system is able to accommodate this abnormal load rejection and to reduce the effects of the transient imposed upon the RCS. The reactor power is reduced at a rate consistent with the capability of the rod control system. Reduction of the reactor power is automatic down to 15 percent of full power. Manual control must be used when the power is below this value.

The pressurizer relief valves might be actuated for the most adverse conditions, e.g., the most negative Doppler coefficient, minimum incremental rod worth and smallest moderator coefficient. The relieving capacity of the power-operated relief valves is adequate to limit the system pressure to prevent actuation of high-pressure reactor trip for the above conditions.

7.3.3.5 Turbine - Generator Trip With Reactor Trip

Whenever the turbine-generator unit trips at an operating level above 10 percent power, the reactor also trips. The plant is operated with a programmed average temperature as a function of load, with the full load average temperature significantly greater than the saturation temperature corresponding to the steam generator pressure at the safety valve set point. 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 steam temperature, a heat sink is required to remove heat stored in the reactor coolant to prevent actuation of steam generator safety valves for this trip from full power. This heat sink is provided by the combination of controlled steam release by the steam dump system by makeup of cold feedwater to the steam generators and by relief through the atmospheric relief valves if necessary.

The steam dump system is controlled from the reactor coolant temperature average signal whose set point values are reset upon trip to the no-load value. Actuation for the turbine bypass is rapid to prevent actuation of the steam generator safety valve. With the dump valves open, the average coolant temperature starts to reduce quickly to the no-load set point. A direct feedback of temperature acts to modulate the valves to minimize the total amount of steam, which is by-passed.

Following the turbine trip, the steam voids in the steam generators will collapse and the fully opened valves will provide sufficient feedwater flow to restore water level in the downcomer. The feedwater flow is cut off when the coolant average temperature decreases below a given temperature value or when the steam generator water level reaches a given high level. This latter condition also initiates turbine trip.

Additional feedwater makeup is then controlled manually to restore and maintain steam generator level while assuring that the reactor coolant temperature is at the desired value. RHR is maintained by the steam generator pressure controller (manually selected) which controls the amount of steam dumped. This controller operates the same dump valves, which are used during the initial transient following turbine and reactor trip.

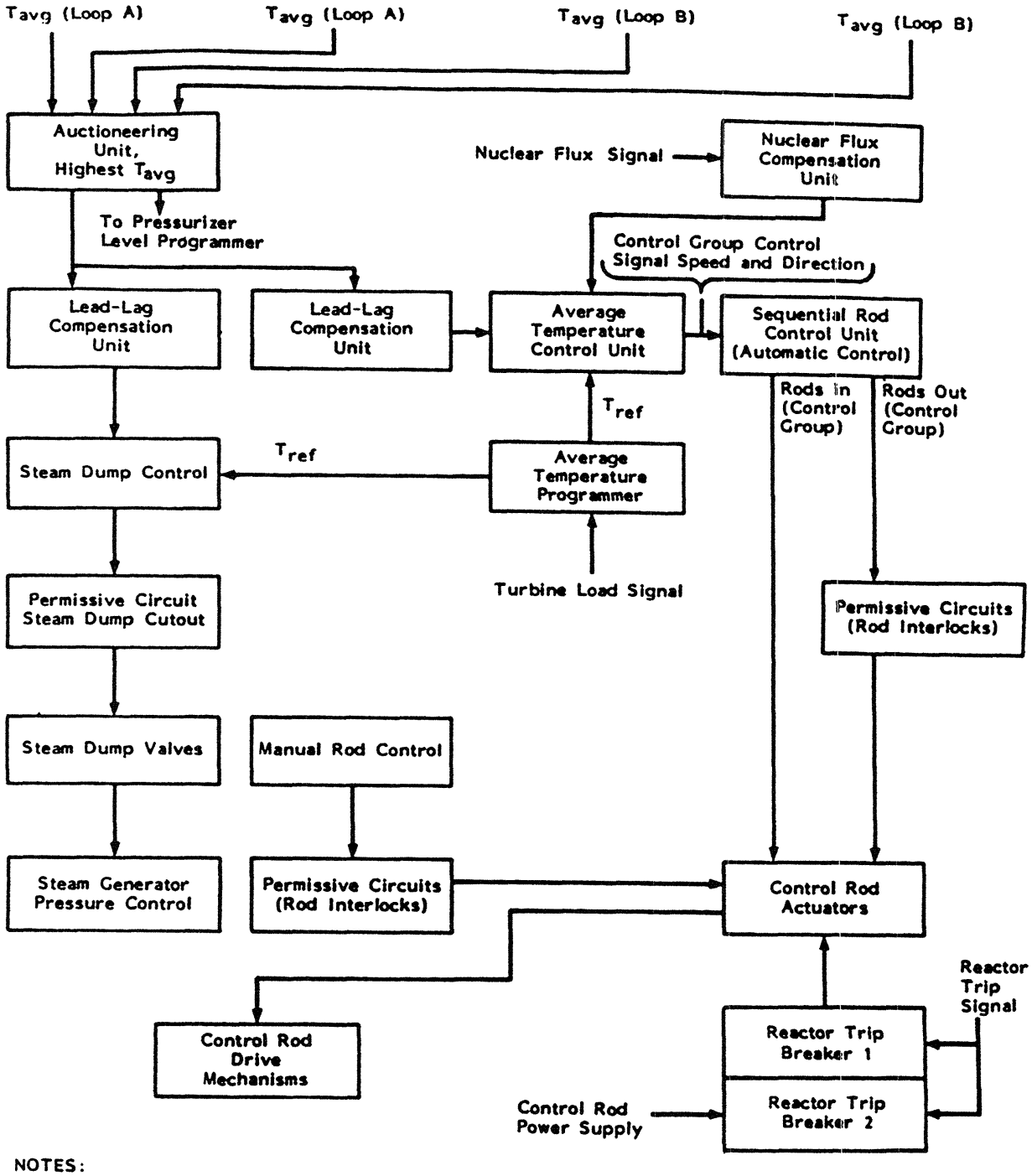
The pressurizer pressure and level fall rapidly during the transient because of coolant contraction. The pressurizer water level is programmed so that the level following the turbine and reactor trip is above the low-level SI set point. If heaters become uncovered following the trip, the Chemical and Volume Control System will provide full charging flow to restore water level in the pressurizer. Heaters are then turned on to restore pressurizer pressure to normal.

The steam dump and feedwater control systems are designed to prevent the average coolant temperature from falling below the programmed no-load temperature following the trip to ensure adequate reactivity shutdown margin.

7.3 References

1. Blanchard, A., D. N. Katz, “Solid State Rod Control System Full Length,” WCAP 7778, December 1971

Figure 7.3-1 Simplified Block Diagram of Reactor Control Systems



NOTES:
1) Temperatures are measured in the hot and cold legs.
2) Pressure is measured at the pressurizer.

7.4 NUCLEAR INSTRUMENTATION

7.4.1 Design Basis

7.4.1.1 Fission Process Monitors and Controls

Criterion: Means shall be provided for monitoring or otherwise measuring and maintaining control over the fission process throughout core life under all conditions that can reasonably be anticipated to cause variations in reactivity of the core (GDC 13).

The design basis of the Nuclear Instrumentation (NI) System is for reactor protection, and control functions, and is discussed in Reference 1.

7.4.2 System Design

The detailed description of the NI System is presented in Reference 1 and discussed in Reference 2.

7.4.2.1 Overall System Design

The primary design function of the NI System 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. The design also provides a control function and indication of reactor status during startup and power operation.

The NI System consists of eight channels: two source range, two intermediate (wide) range, and four power range channels. In addition, there are five auxiliary channels:

- the audio count rate channel,
- the timer/scaler channel,
- the comparator channel,
- the startup rate channel, and
- the flux deviation channel.

The NI System monitors the neutron flux level outside the reactor using information from three 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 Source Range (SR) covers the first six decades of flux. The Intermediate Range (IR) or wide range covers the entire range of leakage flux, overlapping both the source and power ranges. The Power Range (PR) covers approximately the upper two decades. The overlap of instrument ranges provides reliable continuous protection beginning with source level through the intermediate (wide range) and low power level.

Two types of detectors with associated solid-state electronics circuitry are used to monitor the neutron flux from completely shutdown conditions to 200 percent of full power. The detectors utilized are fission chambers for the SR and IR, and ion chambers for the PR.

The NI System 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 refueling operations. Startup rate indication for the source and intermediate range channels is provided at the control board. Reactor trip, rod stop, control and alarm signals are transmitted to the Reactor Control and Protection System for automatic plant control. Information associated with equipment failures and test status is indicated in the Control Room.

7.4.2.2 Controls and Alarms

Various control and alarm functions are obtained from the three ranges of nuclear instrumentation during shutdown, startup, and power operation. These functions are used to alert the operator of conditions, which may require administrative action and to alert personnel of unsafe reactor conditions. They also provide signals to the rod control system for automatic blocking of rod withdrawal during plant operation to avoid unnecessary reactor trips. The following briefly describes the primary functions of the three ranges of instrumentation.

- Source Range Channels

  There are no control functions associated with the SR channels. Alarm functions are provided to alert the operator of inadvertent changes in shutdown reactivity. Visual indication of this condition is provided at the control board, with audible annunciation in the Containment Building and the Control Room. This audible alarm can be blocked prior to startup.

- Intermediate Range Channels

  Both alarm and control functions are provided by the two IR channels. Blocking of the rod withdrawal is initiated by either IR channel on high flux level. This condition is alarmed at the control board to alert the operator that a rod stop has been initiated. The IR channels also provide a visual indication when either channel exceeds the P-6 permissive level. This alerts the operator to take action to manually block the source range trips to prevent an inadvertent trip during normal power increase.

- Power Range Channels

  Both alarm and control functions (similar to intermediate range) are provided by the PR channels. An overpower rod stop function from any of the four power range channels inhibits rod withdrawal and is alarmed at the control board. The PR channels also provide a visual indication when two-out-of-four channels exceed the permissive P-10 level. The P-10 permissive alerts the operator to take action to block the IR flux trip and PR low range flux trip before any further power increase.

Permissive P-10 also provides an input to the P-7 permissive, which provides for blocking trips at low power to allow plant startup and shutdown. Permissive P-8 is provided for blocking a single primary loop loss-of-flow reactor trip.

Another function provided is the PR channel deviation alarms. These alarms are initiated by the comparator channel and flux deviation drawer, through a comparison of the average power level signals and individual detector signals. Actuation of these alarms alert the operator to a power imbalance between the power range channels.

Each PR channel provides three signals to the reactor control and protection system, one signal from each individual detector isolation amplifier, and one signal from the average power isolation amplifier. The isolated average power signal is transmitted to the control system, where the average of all four of the isolated average power signals is used for the rod speed control function. Any one of the individual signals can be defeated via a defeat switch. The individual detector signals are used for the ΔT over-power over-temperature compensation which initiates rod stops and turbine runbacks.

7.4.3 Design Evaluation

Design evaluation considerations are discussed in Reference 1 and Reference 3.

Reference 1 is applicable to the NI System currently installed in the plant, with the following exception. In a 1991 plant design change, a Gamma-Metrics Flux Indication System was installed for the SR and IR channels. The new design utilizes fission chamber detectors, and eliminates the use of Boron-Trifloride and compensated ion chamber detectors. Also, the range and engineering units for the IR channels was changed from ion chamber amps to percent power over 10 decades.

7.4 References

1. Lipchak, J. B., R. A. Stokes, “Nuclear Instrumentation System,” WCAP 7380-L, June, 1970
2. NRC SER, M. J. Davis (NRC) to K. H. Evers (WPS), Letter No. K-91-041, March 4, 1991
3. NRC SER, A. G. Hansen (NRC) to K. H. Evers (WPS), Letter No. K-91-232, November 12, 1991

Intentionally Blank

7.5 ENGINEERED SAFETY FEATURES INSTRUMENTATION

7.5.1 Design Basis

The ESF instrumentation measures temperatures, pressure, flows, and levels in the RCS, steam system, reactor containment and auxiliary systems, actuates the ESF, and monitors their operation. Process variables required on a continuous basis for the startup, operation, and shutdown of the plant are indicated, recorded, and controlled from the Control Room. The quantity and types of process instrumentation provided ensures safe and orderly operation of all systems and processes over the full operating range of the plant.

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.

7.5.1.1 Engineered Safety Features Protection Systems

Criterion: Protection systems shall be provided for sensing accident situations and initiating the operation of necessary ESF (GDC 15).

Instrumentation and controls provided for the protective systems are designed to trip the reactor, when necessary to prevent or limit fission product release from the core and to limit energy release; to signal containment isolation; and to control the operation of ESF equipment.

ESF is actuated by the ESF actuation channels. Each coincidence network actuates an ESF actuation device that operates the associated ESF equipment, motor starters and valve operators. The channels are designed to combine redundant sensors, and independent channel circuitry, coincident trip logic and different parameter measurements so that a safe and reliable system is provided in which a single failure will not defeat the channel function. The action-initiating sensors, bistables, and logic are shown in the figures included in the detailed ESF Instrumentation Description given in this Section. The ESF Instrumentation System actuates the equipment and/or systems discussed under Section 7.2.1.

Availability of control power to the ESF trip channels is monitored. The loss of instrument power to the sensors, instruments, or logic devices in the ESF instrumentation, places that channel in the trip mode, except for containment spray initiating channels which require instrument power for actuation.

The passive accumulators of the SI System do not require signal or power sources to perform their function. The actuation of the active portion of the SI System is from signals described in Table 7.2-1.

The containment air fan-coil units are normally in use during plant operation. These units are in the automatic sequence, which actuates the ESF upon receiving the necessary signals indicating an accident condition.

The process instrumentation required for ESF actuation is given in Table 7.5-1.

The logic diagram for containment spray actuation as well as for safety injection, steam line isolation, and containment isolation, is shown in Figure 7.5-1.

The containment isolation signals provide the means of initiation of isolation of the various pipes passing through the containment walls as required to prevent the release of radioactivity to the outside environment in the event of a LOCA.

The ESF actuation circuits are designed on the principle that the safeguard bistables (see Figure 7.5-2) are de-energized to actuate, with the exception that the containment pressure bistables for spray actuation are energized to operate in order to avoid spray operation on inadvertent power failure.

The dc control supply associated with the ESF is designed to meet the single failure criterion.

7.5.2 System Design

7.5.2.1 Engineered Safety Features Actuation Instrumentation Description

Figure 7.5-2 shows the sensors, bistables, and logic matrix for the ESF.

The same channel isolation and separation criteria as described for the reactor protection circuits are applied to the ESF actuation circuits.

The ESF actuation instrumentation automatically initiates the protective actions as noted in Table 7.2-1.

7.5.2.1.1 Indication

All transmitted signals (flow, pressure, temperature, etc.) which can cause actuation of the ESF are either indicated or recorded for every channel.

7.5.2.2 Engineered Safety Features Instrumentation Equipment

Table 7.5-1 provides information on the process instrumentation, which provides signals to the ESF actuation circuitry.

The following instrumentation ensures monitoring of the effective operation of the ESF.

7.5.2.3 Containment Pressure

Six channels, monitoring containment pressure and derived from six pressure taps, reflect the effectiveness of the containment and cooling systems and other ESF. High-pressure indicates high temperatures and reduced pressure indicates reduced temperatures. Indicators and alarms are provided in the Control Room to inform the operator of system status and to guide actions taken during recovery operations. Containment pressure indication will be used to distinguish between various incidents.

Redundant containment pressure signals are provided to isolate the containment. Each of the three pairs of differential pressure transmitters external to the containment in the Auxiliary Building have their own connection to the containment. Remote indicating facilities, and alarm signals are provided from each transmitter.

The pressure setpoint for containment isolation of nonessential penetrations satisfies the requirements of Position Statement 5 of Item II.E.4.2 of NUREG-0737 as being the minimum setpoint compatible with normal operating conditions (see NRC SER in Reference 3).

In response to the requirements of NUREG-0737, Item II.F.1.4, two redundant wide-range containment pressure monitoring systems were installed which provide continuous display and recording in the Control Room. Each system has a calibrated span of 5 to 200 psig. The wide-range pressure monitors are designed to allow plant operators to adequately assess containment pressure under both normal and post-LOCA operating conditions (see NRC SER in Reference 2).

7.5.2.3.1 Refueling Water Storage Tank Level

Level instrumentation on the RWST consists of two channels. Each channel provides remote Control Room indication as well as low and low-low level annunciation in the Control Room. One channel also provides indication on the plant process computer. Both channels are energized from emergency power.

7.5.2.3.2 Safety Injection System Pumps Discharge Pressure

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

7.5.2.3.3 Pump Energization

All pump motor power feed breakers indicate that they have closed by energizing indicating lights on the control board.

7.5.2.3.4 Radioactivity

Means are provided to measure the radioactivity in the containment atmosphere after the incident, since this information will be required for any subsequent entry into the Containment following a LOCA.

7.5.2.3.5 Valve Position

All ESF remote-operated valves have position indication on the control board. Air-operated, and solenoid-piloted air-operated valves move in a preferred direction on loss of air or power. After a loss of power, motor-operated valves remain in the same position as they were prior to the loss of power. All motor valves, which do not receive an accident signal, but are to be in a specific position prior to operating the plant, are monitored in the Control Room.

7.5.2.3.6 Containment Air Recirculation Cooling System

Flow indication is provided outside containment for service water to each fan coil unit. A failure in a service water header will be detected by containment sump level instrumentation. The magnitude of the leak is estimated using the containment sump level change with time. Leaks of greater magnitude can be detected by sequentially isolating each header discharge and comparing the flow rate through each header. Leaks of smaller magnitude are detected by isolating each header sequentially and trending containment level versus time. The exit temperature of each of the fan-coils are alarmed in the Control Room if the airflow exit temperature is high. In addition, the exit flow is monitored for radiation and alarmed in the Control Room if high radiation should occur. This is a common monitor and the faulty coil can be isolated locally by manually valving each one out in turn.

7.5.2.3.7 Service Water Header Pressure

Individual header pressure indication and control is provided to supply an input to the Turbine Building service water isolation actuation. A safety injection sequence concurrent with the low header pressure is required to isolate the non-safety Turbine Building service water supply, thus ensuring that adequate service water cooling is provided to safety features equipment under accident conditions. Under SI actuation, the service water system is split into two separate and independent headers, thus redundancy for each header pressure signal is not required, but rather the independent headers provide for meeting the single failure criteria on the system level.

7.5.2.3.8 Alarms

Visual and audible alarms are provided to call attention to abnormal conditions.

7.5.2.3.9 Sump Instrumentation

The sump level indicator is a switch activated series of six lights on the main control board, installed to provide additional operator information, which indicate when a sufficient water level exists in containment which will support the net positive suction head required by the RHR pumps

for post-LOCA recirculation. The activated limit switches are verified each refueling for a proper setting within one inch. Sump B level instrumentation is energized by emergency power. The transmitter housings for the sump level indicators are located above any possible flooding level (see NRC SER in Reference 2).

7.5.2.3.10 Wide-Range Containment Water Level Monitor

In response to the requirements of Item II.F.1.5 of NUREG-0737, a wide-range level indication system was installed in the basement (the containment sump) area of containment. This system consists of two redundant trains of level monitors capable of measuring the containment water level in the range of 0 to 22 feet above the basement level. The water level signal receiver and meter accuracy is ±3 percent (see NRC SER in Reference 2).

7.5.2.4 Instrumentation Used During Loss-of-Coolant Accident

Instruments, which are designed to function for various periods of time following the major LOCA are those which initiate or otherwise govern operation of ESF. Pressurizer pressure and level, and steam generator pressure sensors are located inside the containment because an equivalent signal cannot be obtained from a sensor location more isolated from the reactor.

It should be emphasized, however, that for the large loss-of-coolant incidents the initial suppression of the transient is independent of any detection or actuation signal, because the water level will be restored to the core by the passive accumulator system.

Pumps used for SI and containment spray are located outside the Containment. The operation of the equipment is verified by Control Room instrumentation.

Depending upon the magnitude of the LOCA, information relative to the pressure of the RCS is required to determine which pumps will be used for recirculation and also to decide if the SI pumps are required for long-term recirculation.

The RWST level instrumentation provides information, which is used to evaluate the reactor loop conditions as a backup to reactor system instrumentation. Core recirculation and containment spray recirculation (if necessary) is manually initiated when the RWST is almost emptied.

Considerations have been given to the instrumentation and information that will be necessary for the recovery time following a loss-of-coolant incident. Instrumentation external to the reactor containment will not be damaged by this postulated incident and will be available to the operator.

The sources of power for the control of the instrumentation system above are derived from four independent static inverters which take normal operating power from the 4160V ESF buses but automatically switch to the 125V dc System upon loss of ac power supply. The redundancy of

power sources serving the instrumentation system including its control power is arranged such that complete loss of one instrument bus will still provide sufficient ESF to safely control the plant. The power sources are shown on Figure 8.2-4.

7.5.3 System Evaluation

Redundant instrumentation has been provided for all inputs to the protective systems and vital control circuits.

Where wide process variable ranges and precise control are required, both wide-range and narrow-range instrumentation is provided.

All electrical and electronic instrumentation required for safe and reliable operation is supplied from the vital instrumentation buses.

7.5.3.1 Pressurizer Pressure

Any accident condition requiring emergency core cooling would involve low pressurizer pressure. Emergency core cooling is accomplished by the SIS actuation from the RCS variables. Actuation is initiated by low pressurizer pressure, two out of three signals.

A SI block switch is provided to permit the RCS to be depressurized and its water level lowered for maintenance and refueling operations without actuation of the SI System. This manual block switch is interlocked with pressurizer pressure in such a way that the blocking action is automatically removed above a preset pressure as operating pressure is approached. If two out of three pressure signals are above this preset pressure, blocking action cannot be initiated. The block condition is annunciated in the Control Room.

7.5.3.2 Motor and Valve Control

For starting pump and fan motors, the slave relays, when energized, cause closing coils on the motor starters or circuit breakers to be energized. When motor starters are used the starter operating coil will be supplied by power from the same source as the subject motor. When circuit breakers are used for motor control the circuit breakers close and trip coils will be supplied by power from a 125V dc battery bus as outlined in Chapter 8.

Air actuated solenoid piloted containment vent and purge isolation valves are spring loaded to close upon loss of air pressure.

7.5.3.3 Environmental Capability

The ESF instrumentation equipment inside the containment is designed to operate under the accident environment. Electrical equipment for the ESF is located inside the Containment, and the Class I section of the Auxiliary and Turbine Buildings. The equipment located inside the Containment, which must function in the post-accident environment was originally transmitted and docketed in response to Bulletin 79-01B. Current information is maintained in the KPS EQ

Program. The expected length of time that the equipment will be required to function following an accident is also given.

Extensive studies and tests have been conducted to verify that equipment required to operate during and post-LOCA and HELB has been environmentally qualified.

All air-operated isolation valves inside the containment required to isolate post-accident are either normally closed or fail closed (see KPS EQ program). Solenoid valves are installed so that it takes an electrical signal to operate (energize) the solenoid and place the air-operated valve in its operational mode (open in this case). Conversely, a loss of electrical signal de-energizes the solenoid causing the air-operated valve to go into its failure (closed) mode. Thus, a loss of electrical power, a loss of air pressure, or a containment isolation signal, which, in this case, de-energizes the solenoid, will cause the letdown valve to go closed. The valve response is rapid enough to insure its function, before an adverse environment has rendered the valve inoperable. In the highly unlikely event an air-operated isolation valve should fail, independent isolation valves outside containment are provided.

All instrument cables are run in conduit or in armor cable from the termination of the cable tray to the connection of the instrument housing. Cable trays are also provided with covers in the vicinity of fluid-carrying pipes, such as steam or water lines, to preclude fluid impingement on the cables.

The first two sub-headings below give design basis for environmental capability of the Reactor Protection System and ESF Actuation System, respectively. The next subheading identifies and discusses safety related equipment and components. The last subheading discusses qualification and testing of safety related equipment and components.

7.5.3.3.1 Reactor Protection System Environmental Requirements

In addition to environmental design basis listed in IEEE-279, the following additional environmental requirements shall be applicable:

1. During the initial phase of either LOCA or steam line break accident, pressurizer pressure channels must operate under all expected post-accident coolant system conditions with transmitters located in a steam-air mixture and radiation environment such that it is ensured that reactor trip and SI has been actuated.[1]
2. Containment pressure signal transmitters[2] must remain operable to monitor containment pressure in the post-accident phase of a LOCA or steam line break accident.

1. These instruments are required to be operable up to approximately thirty minutes after the accident or until the pressure and water level are reduced beyond the span of the instruments, whichever happens first. Additional instrumentation exists outside containment, which provides sufficient information to monitor long-term cooling of the core directly.
2. Signal transmitters are outside the containment.

3. During the initial phase of a steam line break accident, steam generator outlet flow channels must operate in accordance with design requirements to insure steam line stop valve closure.

7.5.3.3.2 Engineered Safety Features Actuation System Environmental Requirements

In addition to environmental design basis listed in IEEE-279, the following additional environmental requirements shall be applicable:

1. During the initial phase of either LOCA or steam line break accident, ESF Actuation System must provide the required protective action. ESF Actuation System components will be designed and arranged so that mechanical and thermal environment accompanying any emergency situation in which components are required to function does not interfere with that function.
2. Pressurizer pressure and level sensors which will be required to operate during the first one-half hour following an accident, or until pressure and water level are reduced beyond instrument span, whichever happens first.
3. High-head injection line valves must open on SIS.
4. The containment sump level instrumentation must function for two hours to give backup information to the RWST level indicators as to when injection can be terminated and recirculation initiated.
5. The air and motor operated containment isolation valves must function on initiation from an SIS or a hi-hi containment pressure signal.
6. Containment fan-coil units must function for one year.
7. Containment dome ventilation fans must function for one year.
8. The Containment sump isolation valves must be available for one year.
9. The reactor vessel low head SI line isolation valves are required to open upon receipt of an SIS.

7.5.3.3.3 Instrumentation Used During Loss-of-Coolant Accident

Instruments designed to function for various periods of time at the onset of a major or LOCA govern the operating of ESF. Electrical equipment for ESF is located inside the Containment and Auxiliary Building.

1. Pressurizer pressure transmitters are required to actuate ESF for in-containment accident. Transmitters are located inside Containment because an equivalent signal cannot be obtained from sensor location more isolated from the reactor. Transmitters are designed and qualified to operate for 30 days post-accident, which is more than sufficient to provide their functions.

It should be emphasized, however, that for the large LOCA the initial suppression of the transient is independent of any detection or actuation signal because water level will be restored to the core by the passive accumulator system.

2. All pumps used for SI and containment spray are located outside Containment. Operation of equipment can be verified by instrumentation that reads in the Control Room. This instrumentation will not be affected by the accident.

3. Depending upon the magnitude of the LOCA, information relative to pressure of the RCS will be useful to the operator to determine which pumps will be used for recirculation in event of a small break. RCS pressure, as read on instrumentation outside Containment, will serve this purpose. RWST instrumentation will also provide information for evaluating conditions necessary to initiate recirculation mode of operation. See Chapter 6 for further details.

4. RWST level instrumentation provides additional information to determine relative size of a reactor coolant leak. Core recirculation and containment spray recirculation (if necessary) can be manually initiated when the RWST is empty.

5. Considerations have been given to all the instrumentation and information that will be necessary for the recovery time following a LOCA. Instrumentation external to the reactor containment required to function post-accident will be available to the operator.

7.5.3.3.4 Qualification and Testing

ESF instrumentation equipment inside containment is designed to operate under accident environment of steam-air mixture, radiation, chemical spray, high temperature, high-pressure conditions, and possible submergence.

All power, control and instrument cable used on the project was purchased from vendors who produced QA documentation including test data showing that the materials used in the cables was the same as the materials tested to meet the specifications. Originally, the specifications required exposure to 5E+7 rads and an exposure to an ambient as follows:

Time After Accident (Hours)	Ambient Temperature °F	Relative Pressure (psig)	Humidity%
0-1	270	46	100
1-48	160	5	100
48-1 yr.	140	4	100

The electrical penetrations were specified to be capable of withstanding an integrated radiation exposure of 5E+7 rads. The current integrated dose to which equipment must be

qualified inside Containment is 5.2E7 rads gamma. This dose was evaluated in response to IE Bulletin 79-01B and is documented in Reference 4.

For ESF electrical components, current information on environmental qualification testing is maintained in the KPS EQ Program, as required.

Failure of the above equipment after the specified time will not increase severity or consequence of the accident. Reactor protection control and instrumentation equipment and electrical equipment for ESF located in Auxiliary Building will operate in a normal ambient environment (harsh for radiation) following a major LOCA. Auxiliary Building equipment in the containment sump water recirculation loop is listed below:

- RHR pumps, heat exchangers, and spray pumps.
- Flow, temperature, and pressure instrumentation for the RHR System.
- Power and instrument cables for the above.

Shield Building Vent System filters and fans are required to operate following a LOCA. These filters and fans are located outside of Containment and will not be subject to any of the adverse environmental conditions of the containment vessel atmosphere other than high radiation.

These assemblies and their components (filter medium, filter cell material, frame material, separator material, adhesive material, gasket material, motor windings, etc.) are specified to function after a total dose of 1E+7 rads corresponding to the dose from deposited radioactive iodine on the charcoal filters from the containment post-DBA leakage. Materials of the type used in the construction of the filter and fan assembly have been successfully tested at exposure levels above 1E+7 rads. This system is available for one year.

Auxiliary Building SV System filters and fans are required to operate following a LOCA. These filters and fans are located outside of containment and will not be subject to any of the adverse environmental conditions of the containment vessel atmosphere other than high radiation.

These assemblies and their components are specified to function after a total dose of 1E+6 rads corresponding to the dose from deposited radioactive iodine. Materials of the type used in the construction of the filter and fan assemblies have been successfully tested at levels above 1E+6 rads. This system is available for one year.

Following a major LOCA, areas of high radiation would exist inside the Containment; in those portions of the Auxiliary Building near RHR System equipment; near the SI and ICS System equipment; near Shield Building Vent System filters and fans; and near Auxiliary Building SV System filters and fans. The maximum dose levels within the containment would be approximately 3.8E+6 rads during one hour or 3.6E+7 rads during one week. The maximum dose rates in high radiation areas of the Auxiliary Building (RHR compartments) would be less than

1 percent as high. The ability of electrical equipment in the Emergency Core Cooling System to withstand radiation exposure would be limited by radiation effects on electrical insulation materials and motor and equipment bearing lubrication.

The design considerations and specifications to be used in the selection of motors, which must function in the post-accident environment are discussed in Section 6.2, 6.3, and 6.4. Similar application criteria apply to the specifications of control and instrumentation equipment and other electrical equipment.

The electrical equipment for Emergency Core Coolant System located in the containment will only use radiation resistant insulating materials. These insulating materials have a threshold for radiation damage, which might affect their functioning at 108 rads or higher. They would therefore provide considerable margin above the maximum post-accident radiation dose that would result from the exposure times specified earlier.

The lower ambient temperatures and radiation levels in most areas of the Auxiliary Building will permit the use of normal elastomer or plastic insulation materials. These materials have a threshold for radiation damage of 106 rads or higher. Where required, because of location in possible high radiation areas, motor bearings are lubricated with radiation-rated lubricants.

The original environmental testing, along with the additional requirements of Bulletin 79-01B, were completed. Results can be found in the KPS FSAR, WCAP-7744 (Reference 1), and the KPS QA Records Vault. Current information on environmental qualification testing is maintained in the KPS EQ Program.

7.5.3.3.5 Instrumentation

For instrumentation, current information on environmental qualification testing is maintained in the KPS EQ Program, as required.

7.5 References

1. Locante, J., E. G. Igne, “Environmental Testing of Engineered Safety Features Related Equipment,” WCAP 7744, September 1971
2. NRC Safety Evaluation Report, S. A. Varga (NRC) to C. W. Giesler (WPS), Letter No. K-83-10,1 May 2, 1983
3. NRC Safety Evaluation Report, S. A. Varga (NRC) to E. R. Mathews (WPS), Letter No. K-81-188, November 17, 1981
4. Fluor Pioneer Services Letter, F. Afshar (FPS) to C. A. Schrock (WPS), Letter No. KPS-6258, March 13, 1981

Table 7.5-1
Process Instrumentation For RPS And ESF Actuation

Parameter	Transmitter Sensors	Read-Out	Power	Prot/Safety Features	
				Use	Taps
Reactor Coolant Temperature	8 RTDs	C.B. Meter	Ext.	ΔT trips, T_{avg} permissives	1 each
Pressurizer Pressure	4 Transmitters	C.B. Meter	Ext.	Hi/Lo Pressure Trips, SIS	3 (Top Level) One Shared
Steam Flow	4 ΔP Transmitters	C.B. Meter	Ext.	Mismatch Trip	1 Pair Each
Feedwater Flow	4 ΔP Transmitters	C.B. Meter	Ext.	Mismatch Trip	1 Pair Each
Steam Pressure	6 Transmitters	C.B. Meter	Ext.	SIS	1 Each
Steam Generator Level	6 ΔP Transmitters	C.B. Meter	Ext.	Mismatch Trip, Low Level Trip	1 Pair Each
Reactor Coolant Flow	6 ΔP Transmitters	C.B. Meter	Ext.	Low Flow Trip	1 High Pressure Shared/ Loop, 1 Low Pressure Each
Containment Pressure	6 Transmitters	C.B. Meter	Ext.	SIS (3) Spray (3+3)	3 Shared
Turbine First Stage Pressure	2 Transmitters	C.B. Meter	Ext.	Set Point Programs and Turbine Power Permissives	1 Each

C.B. = Control Board

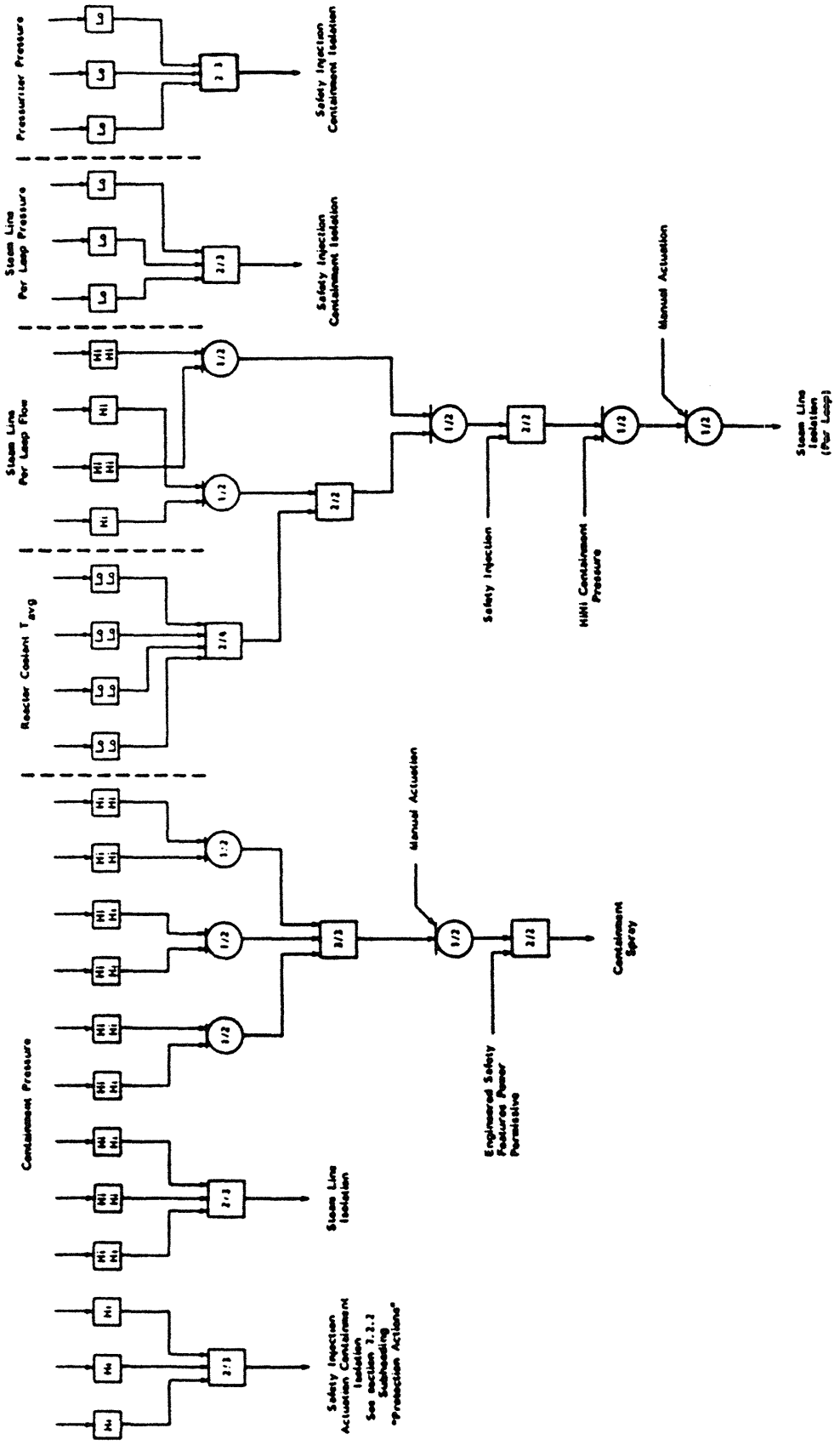
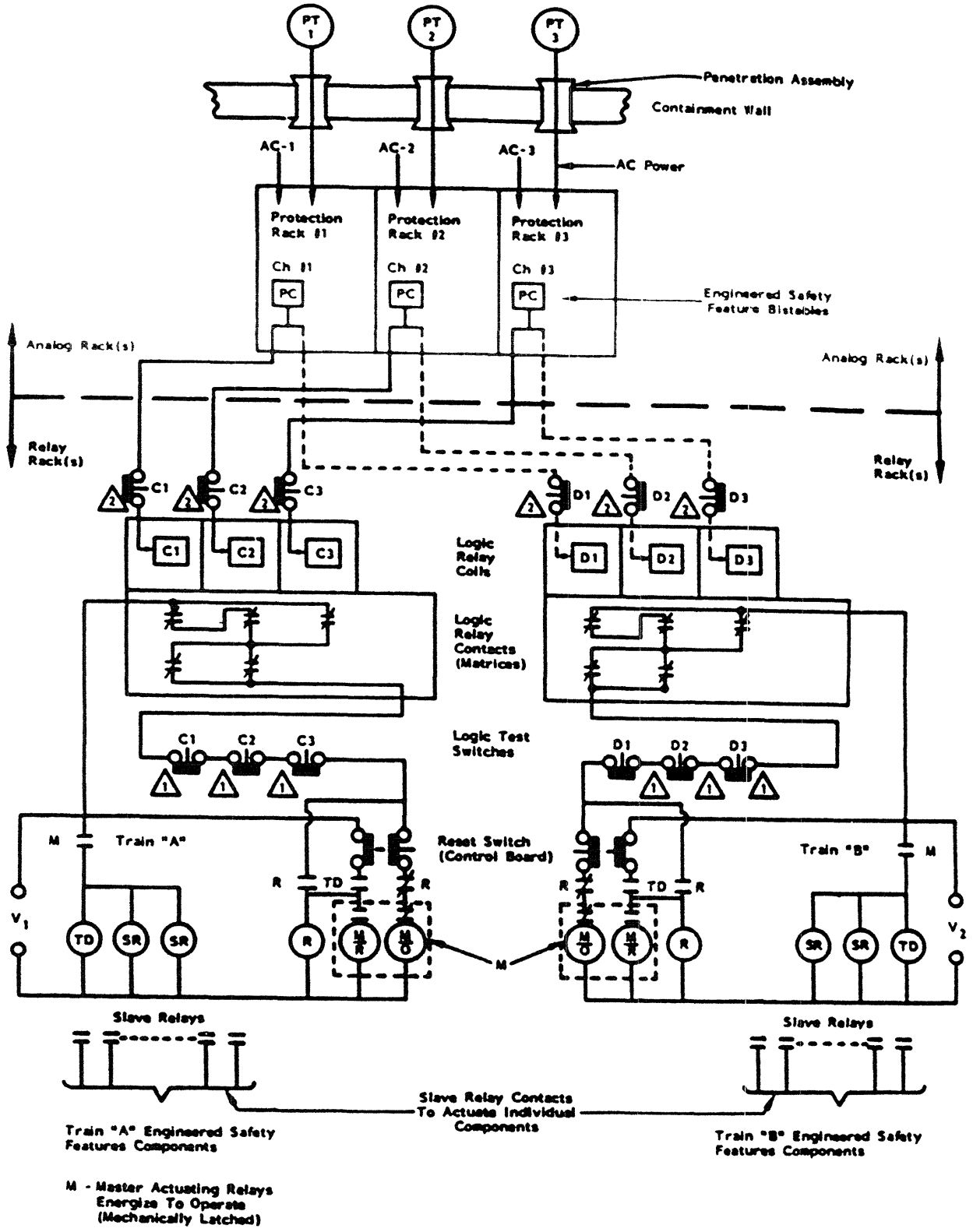


Figure 7.5-1 Engineered Safety Feature Logic Diagram

Figure 7.5-2 Engineered Safety Features Actuation Circuits



7.6 IN-CORE INSTRUMENTATION AND INADEQUATE CORE COOLING MONITORING SYSTEM

7.6.1 Design Basis

The in-core instrumentation is designed to yield information on the neutron flux distribution and fuel assembly outlet temperatures at selected core locations. Using the information thus obtained, it is possible to confirm the reactor core design parameters.

The Inadequate Core Cooling Monitoring System (ICCMS) is designed to provide advanced warning of the approach of inadequate core cooling (ICC) caused by various phenomena (i.e., high void fraction pumped flow as well as stagnant boil off). The system provides the reactor operator with a continuous indication of the thermal-hydraulic state within the reactor vessel during the progression of an event leading to and from ICC. The ICCMS has been approved by the NRC and satisfies the requirements of NUREG-0737, Item II.F.2 (see NRC SERs in Reference 1, Reference 2 and Reference 3). Both the in-core instrumentation and the ICCMS provide means for acquiring data only. They perform no operational plant control.

7.6.2 System Design

7.6.2.1 General

The in-core instrumentation system consists of thermocouples positioned to measure fuel assembly coolant outlet temperature at pre-selected locations; and flux thimbles, which run the length of selected fuel assemblies to permit the measurement of the neutron flux distribution within the reactor core. Space was provided for 39 thermocouples and 36 flux thimbles. The high-pressure seals for the thermocouples and flux thimbles are shown on Figure 7.6-1.

The Incore Instrumentation System was designed with substantial redundancy. However, to minimize measurement uncertainties, a minimum of half of the installed core exit thermocouples (CETs) and flux thimbles should be operable. Plant Technical Specifications provide specific operability requirements.

The data obtained from the in-core temperature and flux distribution instrumentation system, in conjunction with previously determined analytical information, can be used to determine the fission power distribution in the core at any time throughout core life. This method is more accurate than using calculational techniques alone. Once the fission power distribution has been established, the maximum power output is primarily determined by thermal power distribution and the thermal and hydraulic limitations, which determine the maximum core capability.

The in-core instrumentation provides information, which may be used to calculate the coolant enthalpy distribution, the fuel burnup distribution, and to estimate the coolant flow distribution.

Both radial and azimuthal symmetry of power distributions may be evaluated by comparing the detector and thermocouple information from one quadrant with similar data obtained from the other three quadrants.

The ICCMS monitors the full range of ICC conditions from normal operation to complete core uncovery. The information provided by the ICCMS is obtained through the following processes:

- CET monitoring
- core sub-cooling margin monitoring
- Reactor Vessel Level Indication System (RVLIS)

The ICCMS provides information to the plant operators on the status of core heat removal capability. The system monitors all core exit thermocouples and calculates the core sub-cooling margin utilizing redundant channels of instrumentation. The information is provided on displays in the Control Room. Information on the reactor vessel water level is provided by the RVLIS. The RVLIS measures the liquid level and void fraction within the reactor vessel and routes this information to redundant displays in the Control Room.

7.6.2.2 Core Exit Thermocouple Monitors

Thirty-five chromel-alumel CETs, with a temperature range of 0 to 2300°F, are located at fixed core outlet positions with their measurement junctions positioned a couple of inches above the fuel assemblies. One additional CET location (I-4) is capped and not available. The CETs 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 enclosed in stainless steel sheaths within the guide tubes to facilitate replacement when necessary. The support of the thermocouple guide tubes in the upper core support assembly is described in Chapter 3.

At the top of the guide tubes, a connection is made to the CETs via stainless steel connectors and routed to two reference junction boxes located inside containment via mineral insulated, stainless steel sheathed cable. Copper field wiring runs from the reference junction boxes to the relay room where Class 1E redundant microprocessors provides readouts for Control Room displays. From the Control Room displays the operator can choose to view the information from a particular thermocouple or to display the average or highest thermocouple temperature. A data link is provided between the Class 1E microprocessors and the plant process computer. This link allows display of CET information on the plant process computer display screens.

7.6.2.3 Core Sub-Cooling Margin Monitor

The sub-cooling margin monitor calculates the margin to saturation temperature or pressure using RCS wide range and pressurizer pressure inputs lowest pressure, and core temperature based upon core exit thermocouples highest temperature. The sub-cooling margin calculated

values are routed to redundant displays in the Control Room, as well as the plant process computer.

7.6.2.3.1 Reactor Vessel Level Indication System

The RVLIS consists of two redundant independent trains that monitor the reactor vessel water level. The indication range is from the bottom of the hot leg to the top of the reactor vessel head. The "pumps off" inventory reading provides an indication of reactor vessel water level when both reactor coolant pumps are off. The "pumps on" reading provides an indication of reactor void fraction for use when one or both of the reactor coolant pumps are running. The RVLIS readings are routed to redundant displays in the Control Room, as well as the plant process computer.

7.6.2.4 Moveable Miniature Neutron Flux Detectors

7.6.2.4.1 Mechanical Configuration

Miniature neutron flux detectors, suitable for the application and remotely positioned in the core, provide remote readout for flux mapping. The basic system for the insertion of these detectors is shown in Figure 7.6-2. Retractable thimbles, into which the miniature detectors are driven, are pushed into the reactor core through conduits that extend from the bottom of the reactor vessel down through the concrete shield area, then to a thimble seal table.

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 the refueling to avoid interference within the core. A space above the seal is provided for the retracted operation.

The drive system for the insertion of the miniature detectors consists of four combinations of drive assemblies, five-path rotary transfer devices, and ten-path rotary transfer devices, as shown in Figure 7.6-2. The drive system pushes hollow helical-wrap drive cables into the core. Miniature detectors are attached to the leading ends of the cables and small diameter sheathed coaxial cables threaded through the hollow centers back to the ends of the drive cables. Each drive assembly consists of a gear motor, which pushes a helical-wrap drive cable and detector through a selected thimble path by means of a special drive box, which includes a storage device that accommodates the total drive cable length. Further information on mechanical design and support is provided in Chapter 3.

7.6.2.4.2 Control and Readout Description

The control and readout system provides means to rapidly transverse the miniature neutron detectors to and from the reactor core at 72 feet per minute and to traverse the reactor core at 12 feet per minute. The control system consists of two sections: one physically mounted with

the drive units, and the other contained in the Control Room. Limit switches in each tubing run provide signals to the path display to indicate the active detector path during the flux mapping operation. Each gear box drives an encoder for position indication. One five-path group path selector is provided for each drive unit to route the detector into one of the flux thimble groups or to storage. A ten-path rotary transfer assembly is used to route a detector into any one of up to ten thimbles. Manually operated isolation valves on each thimble allow free passage of the detector and drive cable when open. When closed, these valves prevent steam leakage from the core in case of a thimble rupture. Provision is made to separately route each detector into a common flux thimble to permit cross calibration of the detectors.

The Control Room contains the necessary equipment for control, position indication and flux recording. Panels are provided to indicate the position of the detectors, and for plotting the flux level versus the detector position. Additional panels are provided for such features as drive motor controls, core path selector switches, plotting and gain controls. A “flux-mapping” operation consists of selecting (by panel switches) flux thimbles in given fuel assemblies at various core locations. The detectors are driven to the top of the core and stopped automatically. An x-y plot from each detector (position vs. flux level) is initiated with the slow withdrawal of the detectors, through the core from the top to a point below the bottom. All four detectors or any combination of them may be used simultaneously for flux plotting. In a similar manner, other core locations are selected and plotted.

Each detector provides axial flux distribution data along the center of a fuel assembly. Various radial positions of detectors are then compared to obtain a flux map for a region in the core.

7.6.3 System Evaluation

The thimbles are distributed nearly uniformly over the core, with about the same number of thimbles in each quadrant. The number and location of these thimbles have been chosen to permit measurement of local to average peaking factors to the accuracies specified in Section TS 3.10 of the Technical Specifications. The DNBR calculated with the measured hot channel factor will be compared to the DNBR calculated from the design nuclear hot channel factors. If the measured power peaking is larger than expected, reduced power capability will be indicated.

7.6 References

1. NRC Safety Evaluation Report, T. R. Quay (NRC) to D. C. Hintz (WPS), Letter No. K-87-105, June 10, 1987
2. NRC Safety Evaluation Report, S. A. Varga (NRC) to D. C. Hintz (WPS), Letter No. K-84-244, November 30, 1984
3. NRC Safety Evaluation Report, S. A. Varga (NRC) to C. W. Giesler (WPS), Letter No. K-84-100, May 18, 1984

Figure 7.6-1 In-Core Instrumentation Details

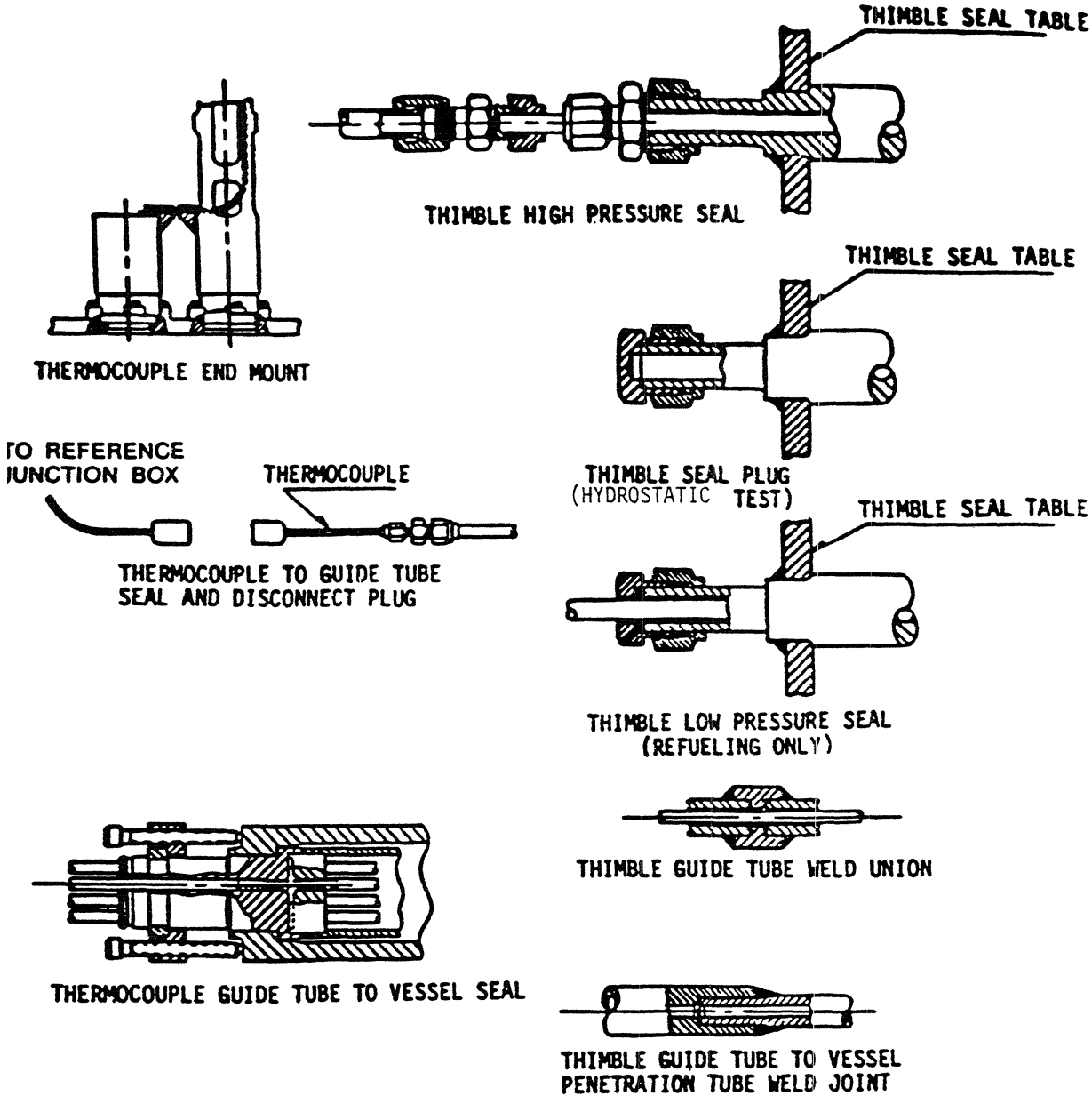
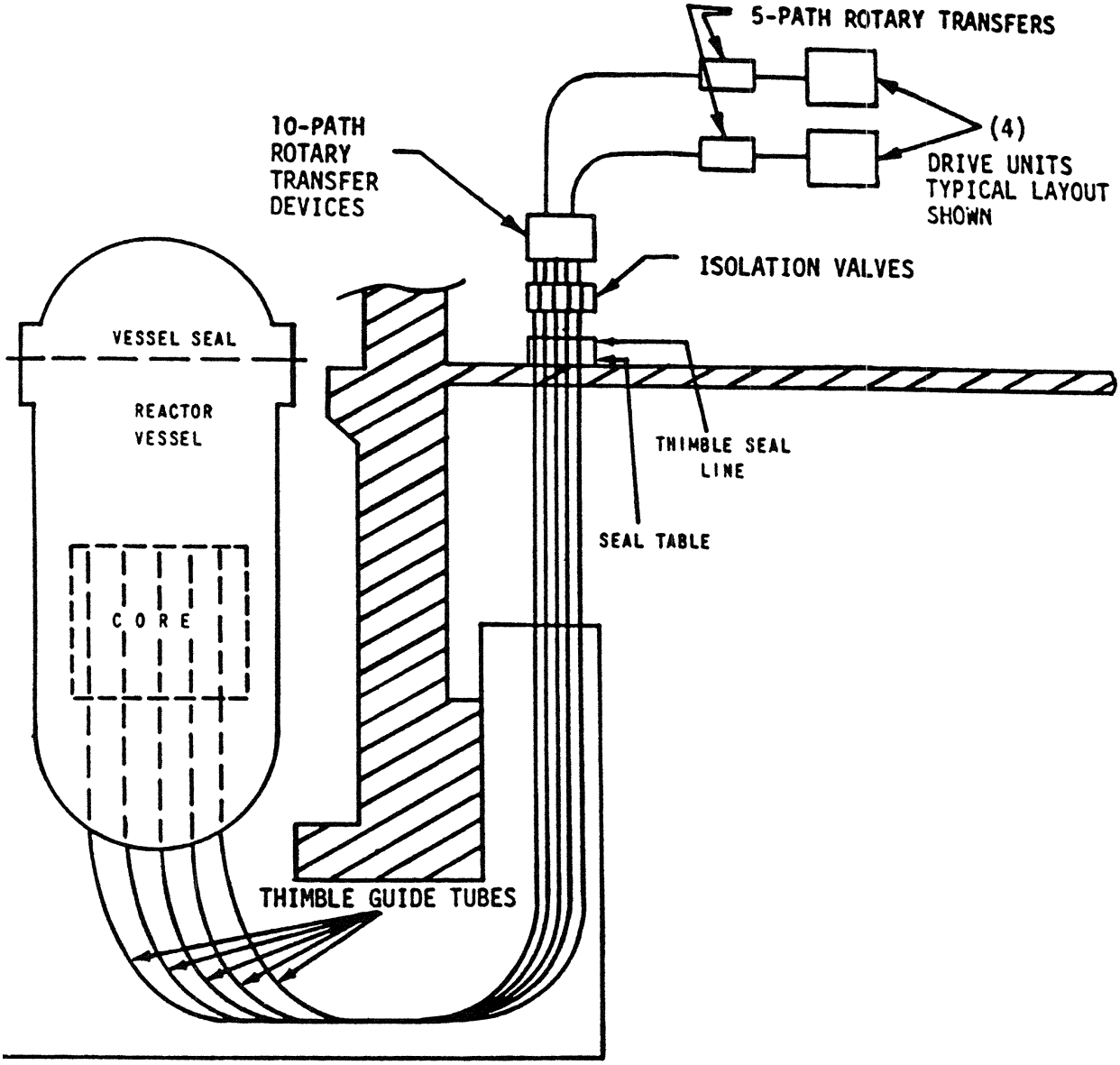


Figure 7.6-2 Typical Arrangement of Movable Miniature Neutron Flux Detector System Elevation View



Intentionally Blank

7.7 OPERATING CONTROL STATIONS

7.7.1 Control Room

Criterion: The facility shall be provided with a control room from which actions to maintain safe operational status of the plant can be controlled. Adequate radiation protection shall be provided to permit continuous occupancy of the control room under any credible post-accident condition or as an alternative, access to other areas of the facility as necessary to shut down and maintain safe control of the facility without excessive radiation exposures of personnel (GDC 11).

The plant is equipped with a Control Room, which contains those controls and instrumentation necessary for safe operation of the plant, including the reactor and the turbine-generator, under normal and accident conditions.

Sufficient design features (shielding, distances, containment integrity and filtration systems) are provided to assure that Control Room personnel shall not be subjected to doses under postulated accident conditions during occupancy of the Control Room which would exceed 5 rem TEDE (total effective dose equivalent) for the 30 days following the accident. In response to Item III.D.3.4 of NUREG-0737, a review of post-accident Control Room habitability was performed. The NRC has determined that the Control Room habitability systems are acceptable and will provide a safe, habitable environment within the Control Room under design basis accident radiation and toxic gas conditions, including LOCAs (see NRC SER in Reference 1). The analysis has been revised to show that the doses remain below the appropriate limit based on the 10 CFR 50.67 guidelines for implementation of alternate source term (Reference 2). The results are presented in Chapter 14.

The Control Room Ventilation System provides a large percentage of recirculated air. Process Monitor Channel R-23 monitors Control Room ventilation air for radiation. If a high radiation condition exists, the monitor initiates closure of the outside air intake. In addition Area Monitor Channel R-1 monitors Control Room air for radiation.

7.7.2 Load Control From the Control Room

Normal load control is accomplished by the licensed operators using the turbine electro-hydraulic control system.

Normal turbine load changes are well within the range of the design capability of the Reactor Control System. As previously stated, the RCS is designed to restrain reactor parameters within the envelope required for reactor protection.

The Kewaunee Plant can accept a loss of 50 percent load without reactor or turbine trip.

The reactor is controlled by a coordinated combination of chemical shim and mechanical control rods. The control system allows the plant to accept step-load changes of 10 percent and ramp-load changes of 5 percent per minute over the load range of 15 to 95 percent power under nominal operating conditions (see Section 7.3.1).

7.7.3 Vertical Panels and Consoles

Complete supervision of both the reactor and turbine-generator is accomplished from a single Control Room. A typical layout of vertical panels and consoles for the Control Room is shown in Figure 7.7-1.

In general, the main control console, rack, and panel layout incorporates the arrangement of controls and information instrumentation for the safe operation of both the NSSS and conventional plant equipment in such a manner as to effectively reduce the amount of area needed to be kept under surveillance, and to provide quick access to controls. Control stations are packaged in a modular concept and are grouped according to function to minimize the possibility of operator error. Control stations with both automatic and manual positions are provided with smooth transfer of function.

In general, instrumentation, recorders and annunciator panels are incorporated in the vertical panel of the Main Control Board to keep the operator informed on process flows, pressure, temperatures, etc., as well as alarms for out-of-limit points requiring operator action. Infrequently used switches are also located on the vertical panels. The console section contains frequently used control devices (switches and control stations) and related indicating lights and indicators.

Referring to Figure 7.7-1, the mechanical vertical panel “B” contains the major part of the Nuclear Instrumentation System. This includes four Nuclear Instrumentation System racks containing amplifiers, signal conditioners, trip units, power supplies, etc. The Nuclear Instrumentation System indicators, recorders and status lights are located to the right of the racks. This panel also contains the Analog RCCA Position Indicators.

Mechanical control console “B”, which is located directly in front of the “B” vertical panel, contains the Instrumentation and Control devices for the Rod Control System and the Chemical and Volume Control System (CVCS). The right-hand portion of the console contains the Rod Control System and the NIS indicators and permissive pushbuttons. The left-hand side of the console contains the CVCS process instrument indicators, controllers, and selected motor and valve controls and indicating lamps. A mimic bus has also been provided.

The Instrumentation and Control devices for the Safety Injection, Auxiliary Coolant, and RCS are located on mechanical control console “C”. The RCS devices are located on the right-hand portion of the console, which is adjacent to the Chemical and Volume Control System devices located on mechanical console “B”. The Auxiliary Coolant System Instrumentation and

Control devices are located on the center portion of mechanical console “C” and the SI System instrumentation and control devices are located on the left-hand portion of the console. The equipment on this console includes indicators, controllers, recorders, and the necessary motor and valve controls and indicating lamps. A mimic bus has been provided to enhance the operator’s ability to rapidly evaluate the status of the SI and Auxiliary Coolant Systems. The in-core Instrument and Radiation Monitoring System panels are located in Mechanical Vertical Panel “C.”

The mechanical vertical panel “A” can be operationally divided into five sections, they are:

- Nuclear Steam Supply Systems,
- Main Steam System,
- heating and ventilating,
- miscellaneous balance-of-plant systems, and
- Turbine System.

This panel contains recorders, indicators, status lights, and infrequently used control switches.

The mechanical control console “A” which is located in front of mechanical vertical panel “A,” can operationally be divided into three sections, they are:

- Steam Generator and Feedwater System,
- Condenser and Heater Drain System, and
- Turbine System.

This console contains process indicators, controllers, selected status lights, and control switches for the various systems.

The electrical vertical panel “A” may be used to monitor and control the 345 kV, 138 kV and 13.8 kV substation breakers.

The electrical control console “A” is used to monitor and control the 345 kV, 4 kV, and 480V plant distribution system. The console also contain the controls for the two diesel generators. A mimic bus has been provided for both the vertical panel and the console. The devices supplied include indicating meters, lights, recorders, controllers, and control switches.

At the Kewaunee Plant, the operator controls the 345 kV generator breakers, 138 kV circuit breakers, and the 13.8 kV circuit breaker for the high-voltage auxiliary transformers in the

switchyard. All line and bus section breakers are controlled via the system operating office by supervisory control.

7.7.4 Additional Control Stations

Local control panels are provided for certain systems and components, which are used on an intermittent basis. Such systems are the Waste Disposal System, Sampling System, Boron Recycle System (part of CVCS), heating boilers, and the Turbine-Generator Hydrogen Cooling System. In these cases, however, appropriate alarms are located in the Control Room and are activated to alert the operator of equipment malfunction or approach to unsafe conditions.

The waste disposal and boron recycle control panels are located in the Auxiliary Building. These boards permit control and monitoring of the processing of wastes in the general area where equipment is located. Alarm signals from these system components annunciate on this board. Actuation of any alarm on this panel actuates a general alarm on the main control board. In this manner, general surveillance over these systems is maintained in the Control Room.

7.7.5 Fire Prevention Design

The KPS Fire Plan defines and guides the implementation of KPS fire protection practices in order to ensure adequate preventive, corrective and mitigative measures. The plan was prepared in response to and in accordance with the guidance provided in NRC Generic Letter 86-10. Refer to the KPS Fire Plan for design requirements.

7.7.6 Emergency Shutdown Control

Provisions have been made so that the plant can be shutdown and maintained in a safe condition by means of controls located outside the Control Room. During such a period, the reactor will be tripped and the plant maintained in the hot shutdown condition. If the period extends for a long time, the RCS can be borated to maintain shutdown as xenon decays. Local controls are located such that the stations to be manned are readily accessible to the plant operating crew for the times required. The plant intercom system provides communication so that the operation can be coordinated.

The functions for which local control provisions have been made are listed below, along with the type of control and its location in the plant. Transfer to these local controls is annunciated in the Control Room.

Basically all control is manual if outside the Control Room. It is expected that all automatic systems will continue functioning until local manual control is established.

However, the reactor can be tripped manually by equipment outside the Control Room if necessary, either by opening the reactor trip and/or power supply breakers or by actuating the manual turbine trip on the turbine. The necessary indicators and manual controls for the hot shutdown capability are provided outside the Control Room. The controls include the necessary

speed and valve controls and local and remote stop/start push button motor controls with local selector switch for local operations. These include controls for the main feed and auxiliary feedwater systems and atmospheric relief and steam dump valves for maintaining the steam generator water level.

7.7.6.1 Equipment Control Outside Control Room

If the Control Room should be evacuated suddenly without any action by the operators, the reactor can be tripped by either of the following:

1. Open reactor trip or rod power supply breakers.
2. Actuate the manual turbine trip on the turbine (above P7).

Following evacuation of the Control Room, the following systems and equipment are provided to maintain the plant in a safe shutdown condition from outside the Control Room:

- Decay heat removal
- Reactivity control, i.e., boron injection to compensate for fission-product decay
- Pressurizer pressure and level control
- Electrical System, as required to supply the above systems
- Other equipment, as described herein

7.7.6.1.1 Residual Heat Removal

Following a normal plant shutdown, automatic steam dump control maintains the reactor coolant temperature at its no-load value. Where necessary, redundancy and full protection is built into the system to ensure the continued operation of the steam generators. If the automatic steam dump control system is not independently available, a power-operated relief valve on each steam generator maintains the steam pressure. These relief valves are further backed up by safety valves on each steam generator. Numerous calculations, verified by start-up tests have shown that with the steam generator safety valves alone, the RCS maintains itself close to the nominal no-load condition. For RHR, it is necessary only to maintain the control on one steam generator.

7.7.6.1.2 Reactivity Control

Following plant shutdown to the hot shutdown condition, boric acid is added to the RCS to maintain sub-criticality. For boron addition, the Chemical and Volume Control System is used. Boration requires the use of:

1. Charging pumps and volume control tank with associated piping.
2. Boric acid transfer pumps with tanks and associated piping.

It should be noted that with the reactor held at hot shutdown conditions, boration of the plant is not required immediately after shutdown. The xenon transient does not decay to the

equilibrium level until some ten to fifteen hours after shutdown, and a further period would elapse before the 1 percent reactivity shutdown margin provided by the full-length control rods would be cancelled. This delay would provide ample time for emergency measures.

7.7.6.1.3 Pressurizer Pressure and Level Control

Following a reactor trip, the reactor coolant temperature will automatically reduce to the no-load temperature condition as dictated by the steam generator temperature conditions. This reduction in the reactor coolant water temperature reduces the reactor volume, and if continued pressure control is to be maintained, reactor coolant makeup is required.

The pressurizer level is controlled in normal circumstances by the CVCS. The facility for boration is provided as described above; it is necessary only to supply water for makeup. Water may be readily obtained from normal sources such as the reactor makeup storage tanks or RWST.

7.7.6.1.4 Electrical Systems

Off-site or on-site emergency power will be available to supply the above systems and equipment for the hot shutdown condition.

7.7.6.1.5 Startup of Other Equipment

Although not directly related to plant safety, the air temperature inside containment should be kept below 120°F. For this reason the containment fan coil units and service water will continue in operation.

7.7.6.2 Indication and Controls Provided Outside the Control Room

The specific indication and controls provided outside the Control Room for the above capability are summarized as follows:

- Indication

  a. Level indication for the individual steam generators is located on the dedicated shutdown panel;

  b. Pressure indication for the individual steam generators is located on the dedicated shutdown panel;

  c. Pressurizer level and pressure indicators are located on the dedicated shutdown panel;

  d. Level indication for the RWST is located on the dedicated shutdown panel;

  e. Temperature indication for reactor coolant system cold leg and hot leg for Loop A is located on the dedicated shutdown panel.

- Controls

  Start/stop motor controls along with a selector switch are provided for each of the motors listed below. Both of these controls are located on the dedicated shutdown panel. The selector switch transfers control of the equipment from the Control Room to the dedicated shutdown panel. Placing the selector switch in the local position provides an annunciator alarm in the Control Room and will turn out the following motor control indicating lights in the Control Room:

  a. AFW Pump 1A

  b. Charging Pump 1C

Alternate motor control location is not required for the items listed below. These items automatically restart on a blackout once the diesel generators are operating.

a. Component cooling water pumps

b. Instrument Air Compressors 1B and 1C

c. Service Water Pumps

d. Containment fan coil units

- Speed Control

  a. Speed control is provided locally for the turbine driven auxiliary feedwater pump;

  b. Speed control for two of the charging pumps is provided locally;

  c. Speed control for one of the charging pumps is located on the dedicated shutdown panel.

- Valve Control

  a. Main feedwater control valves.

  b. The control for the 1A AFW pump control valve is located on the dedicated shutdown panel.

  c. The control for the Steam Generator 1A power-operated relief valve is located on the dedicated shutdown panel (local manual control is also provided).

  d. Steam Dump (Local Manual Control).

  e. All other valves requiring operation during hot standby for the dedicated system can be operated from the dedicated shutdown panel.

  f. Letdown orifice isolation valves (Controls mounted on the dedicated shutdown panel. Selector switch and position lamp are also provided.).

g. The control for the charging line flow control valve is located on the dedicated shutdown panel.

- Pressurizer Heater Control

  Pressure Heater Backup Group 1A normal supply breaker with a selector switch and indicating lamp is also located on the dedicated shutdown panel.

- Lighting

  Emergency lighting is provided in all operating areas as defined by the foregoing.

- Communications

  The communication network provides communications between the area of the auxiliary feedwater pumps and the charging pumps, boric acid transfer pumps, diesel generators, and the outside exchange without requiring use of the Control Room.

7.7 References

1. NRC Safety Evaluation Report, S. A. Varga (NRC) to C. W. Giesler (WPS), Letter No. K-83-141, July 7, 1983
2. Lamb, John, (NRC) to Tom Coutu (NMC), transmitting the NRC SER for Amendment No. 166 to the Operating License, approving Implementation of Alternate Source Term, Letter No. K-03-040, March 17, 2003

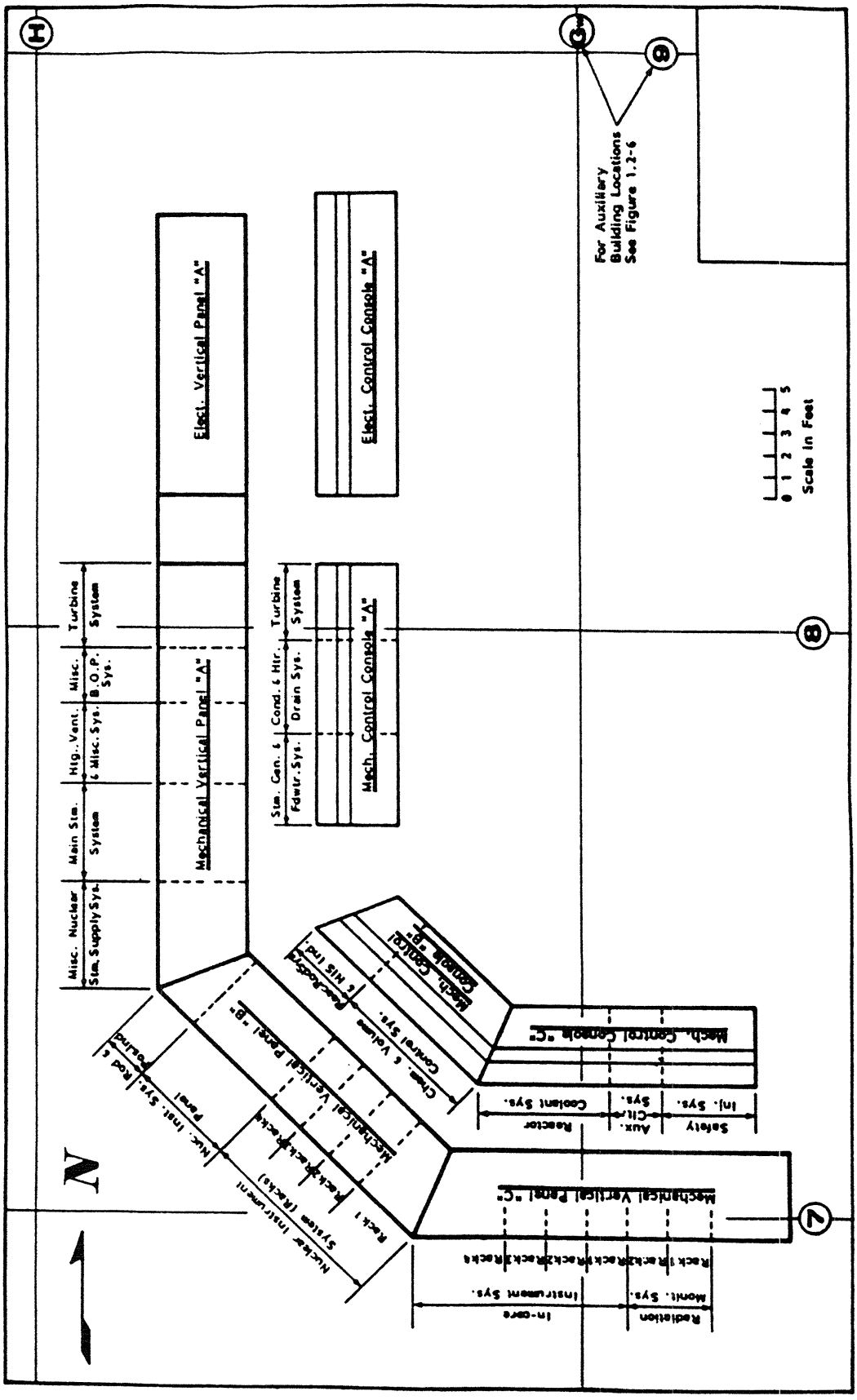


Figure 7.7-1 Plan-Vertical Panels and Consoles

Intentionally Blank