CHAPTER 7 TABLE OF CONTENTS

7.0 INSTRUMENTATION AND CONTROL

7.1 INTRODUCTION

Instrumentation is provided for automatic protection of each unit's reactor during accident conditions, in the form of the reactor protection system (for reactor trip) and the engineered safety features actuation system. In addition, instrumentation is provided for automatic and/or manual control of the nuclear (primary) and turbine-generator (secondary) portions of the plant during normal and off-normal operating conditions, and for monitoring essential plant systems operation during post-accident conditions.

Operation of both units is supervised from a common control room. Because unit-specific instrumentation is basically identical between units, this section typically describes the instrumentation and control systems for a single unit. Where applicable, instrumentation and controls that are shared between both units are also identified.

7.1.1 IDENTIFICATION OF SAFETY-RELATED INSTRUMENTATION SYSTEMS

Safety-related instrumentation systems include:
Reactor Protection System
Engineered Safety Features Actuation System
Nuclear Instrumentation System
Post-Accident Monitoring Instrumentation (Reg. Guide 1.97 Type A Variables)

The design of reactor protection, engineered safety features actuation, and nuclear instrumentation systems is similar to the R.E. Ginna plant.

7.1.2 GENERAL DESIGN CRITERIA

General design criteria (GDCs) that apply to instrumentation and control systems are discussed below.

Reactor Core Design (GDC 6)

> The reactor core with its related controls and protection systems shall be designed to function throughout its design lifetime without exceeding acceptable fuel damage limits which have been stipulated and justified. The core and related auxiliary system designs shall provide this integrity under all expected conditions of normal operation with appropriate margins for uncertainties and for specified transient situations which can be anticipated.

DISCUSSION

The reactor control and protection systems are designed to function throughout their design lifetime to prevent exceeding acceptable fuel damage limits, and to actuate a reactor trip for any anticipated combination of plant conditions, when necessary, to ensure a departure from nucleate boiling (DNB) ratio equal to or greater than the limits specified for STD, OFA, upgraded OFA, and 422V+ fuel.

Suppression of Power Oscillations (GDC 7)

> The design of the reactor core with its related controls and protection systems shall ensure that power oscillations, the magnitude of which could cause damage in excess of acceptable fuel damage limits, are not possible or can be readily suppressed.

DISCUSSION

Ex-core instrumentation is provided to obtain necessary information concerning axial neutron flux distributions. This instrumentation is adequate to enable the operator to monitor and control xenon-induced oscillations. In-core instrumentation is used to periodically calibrate and verify the axial flux information provided by the ex-core instrumentation. The analysis, detection, and control of these oscillations is discussed in Reference 2 of Section 3.2.1.

Control Room (GDC 11)

> 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.

DISCUSSION

The plant is equipped with a common control room which contains those controls and instrumentation necessary for operation of each unit's reactor and turbine generator under normal and accident conditions. The control room is continuously occupied under all operating and accident conditions, except for the special case of a control room fire forcing evacuation and alternate shutdown from outside the control room. No other accident is required to be assumed during a control room evacuation due to fire.

Sufficient shielding, distance, and containment integrity are provided to assure that control room personnel shall not be subjected to a dose greater than 5 rem total effective dose equivalent (TEDE) under postulated accident conditions. This dose limit includes control room occupancy, ingress, and egress for the duration of the accident.

The control room ventilation system design normally combines outside makeup air with a large percentage of recirculated air. The radiation monitoring system monitors the control room and the control room air supply and automatically places the ventilation system in operating Mode 5 if a high radiation condition occurs. Refer to Section 9.8 for further discussion of control room ventilation system performance capability.

Instrumentation and Control Systems (GDC 12)

> Instrumentation and controls shall be provided as required to monitor and maintain within prescribed operating ranges essential reactor facility operating variables.

DISCUSSION

Instrumentation and controls are provided to monitor and maintain important reactor parameters (including neutron flux, primary coolant pressure, loop flow rate, coolant temperatures, and control rod positions) within prescribed operating ranges. Other instrumentation and control systems are provided to monitor and maintain, within prescribed operating ranges, the temperatures, pressure, flow, and levels in the reactor coolant system, steam systems, containment, and other auxiliary systems. Process variables which are required on a continuous basis for the startup, power operation, and shutdown of the plant are indicated, recorded, and controlled from the control room, which is a controlled access area. The quantity and types of instrumentation provided are adequate for safe and orderly operation of all systems and processes over the full operating range of the plant.

Fission Process Monitors and Controls (GDC 13)

> 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.

DISCUSSION

Ex-core nuclear instrumentation is used primarily for reactor protection, by monitoring neutron flux and by generating appropriate trip and alarm functions for various phases of reactor operating and shutdown conditions. Nuclear instrumentation also provides a fission process control function and indicates reactor fission process status during startup and power operation. The nuclear instrumentation system supplies information from three separate types of flux detection channels to provide three discrete ranges and protection levels. Each range of instrumentation (source, intermediate, and power) provides the necessary overpower reactor trip protection during operation in that range. The overlap of instrument ranges provides reliable continuous protection from source to intermediate and low-power ranges. As the reactor power increases, the overpower protection level is increased administratively after satisfactory higher range instrumentation operation is obtained. Automatic restoration of the more restrictive trip protection is provided when reducing power. Section 7.6.1 includes additional information on the ex-core nuclear instrumentation system.

Core Protection Systems (GDC 14)

> 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.

DISCUSSION

If the reactor protection system sensors detect conditions which indicate an approach to unsafe operating conditions that require core protection, the system actuates alarms, prevents control rod motion, initiates load runback, and initiates reactor trip by opening the reactor trip breakers.

The basic reactor protection philosophy to prevent departure from nucleate boiling (DNB) is to define an allowable region of power and coolant temperature conditions. This allowable range

is constrained by the primary reactor trip functions, including the overpower ΔT trip, the overtemperature ΔT trip and the nuclear overpower trip. The allowable operating region below these trip settings is designed so that no combination of power, temperature, and pressure could result in a DNB Ratio (DNBR) less than the design basis limit DNBR (approximate value of 1.3) with all reactor coolant pumps in operation. Other reactor trips are provided to back up the primary trips for specific abnormal conditions. A complete list of reactor trips may be found in Table 7.2-1.

Automatic rod stops are provided prior to reaching the nuclear overpower, overpower ΔT, and overtemperature ΔT reactor trip setpoints, to prevent abnormal power conditions which could result from excessive control rod withdrawal.

Engineered Safety Features Protection Systems (GDC 15)

> Protection systems shall be provided for sensing accident situations and initiating the operation of necessary engineered safety features.

DISCUSSION

Instrumentation and controls provided for the engineered safety features actuation system are designed to automatically initiate engineered safety features (ESF) equipment during those accidents which are mitigated by automatic ESF equipment operation. Actuated ESF equipment (depending on the severity of the condition) includes the Safety Injection System, the Containment Air Recirculation Cooling System, containment isolation, and the Containment Spray System, as discussed in Section 6.0.

The engineered safety features actuation system consists of redundant analog channels, each containing sensors for different trip parameters, channel circuitry, and trip bistables. The trip bistable outputs are combined in coincident trip logic in two redundant actuation trains. Sufficient redundancy is provided so that a single failure will not defeat the actuation function. The arrangement of initiating sensors, bistables, and logic are shown in the figures included in the detailed Engineered Safety Features Instrumentation Description given in Section 7.3.

Protection Systems Reliability (GDC 19)

> Protection systems shall be designed for high functional reliability and inservice testability necessary to avoid undue risk to the health and safety of the public.

DISCUSSION

A minimum of two independent protection channels are provided in the reactor protection system and engineered safety features actuation system for each trip variable, with most variables having three or four independent channels. Protection system reliability to avoid unnecessary trips is provided by redundancy within each tripping function and the use of coincidence trip logic. Each protection channel associated with any specific trip variable is provided with an independent source of electrical power and independent circuitry from the sensor through the trip bistable. Therefore, in the event that the loss of a single protection channel occurs, only that particular protection channel is affected, and coincidence logic is not satisfied to initiate a protective action (unless a one-out-of-two coincidence logic is employed).

Most protection channels are designed so that on loss of power, the bistables fail in the tripped condition (the preferred failure direction for most protection channels).

Protection channels are designed with sufficient redundancy for individual channel calibration and testing during power operation without degrading the protection functions. To remove an analog channel from service for test, calibration, or maintenance, all of the associated channel's trip signals to the reactor protection system or engineered safety features actuation system are first placed in the tripped condition. This causes a two-out-of-three coincidence trip logic to become a one-out-of-two coincidence logic on the remaining (untripped) channels. Tripping a channel to be tested will not cause a reactor trip or ESF actuation unless a trip condition already exists in a redundant channel.

Protection Systems Redundancy and Independence (GDC 20)

> 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.

DISCUSSION

A minimum of two independent protection channels are provided in the reactor protection system and engineered safety features actuation system for each trip variable, with most variables having three or four independent channels. The design is such that no single failure within the protection systems or their supporting systems will defeat the overall protective function or violate protection system design criteria. The design includes redundant, independent channels extending from sensors to the trip bistable outputs, which are then combined into coincidence trip logic in two redundant logic trains that extend to the final actuated devices. Sufficient redundancy and coincidence logic is included to reliably accomplish the protective functions if a single failure should occur, while also minimizing unnecessary protective actions due to single failures.

Section 7.2 and Section 7.3 discuss certain protection system backup trips that may not fully meet the single failure criterion. However, failure of a backup trip does not prevent proper protective action of primary trips assumed in the accident analyses, and does not represent a loss of the protective function discussed in GDC 20.

Sensing lines installed between the process piping and the sensors for redundant protection channels are also independent and redundant. However, two exceptions exist where transmitters for redundant channels share common sensing lines (pressurizer pressure and reactor coolant flow). Refer to Section 7.2.1.2.c and Section 7.2.3.3 for justification of shared reactor protection system sensing lines.

When protection system sensors also supply signals for control functions, an isolation amplifier is used to fully isolate the control signal from the protection signal. Therefore, any control circuit failure is prevented from affecting the protection channel. In a few circuits which provide main control board annunciation and stop rod withdrawal, the safety and control

functions are combined from the sensor through dual alarm units. In these circuits, a failure in the control portion of the circuit can cause the safety portion of the circuit to go to its trip position. This may result in initiation of protective action.

Further detail on protection system channel and train redundancy is provided in the descriptions of the respective systems in this chapter. Redundancy of the power supplies to the protection system channels and trains is discussed in Chapter 8.

Protection Against Multiple Disability for Protection Systems (GDC 23)

> The effects of 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.

DISCUSSION

Potentially adverse conditions to which redundant protection system equipment may be exposed include adverse environmental effects, fires, earthquakes, and missile hazards. The design and layout of protection system components precludes loss of the protection function as a result of adverse conditions to which the components may be exposed.

Physical and electrical separation of redundant protection system channels and trains is employed to reduce the probability of an external hazard, such as a fire or missile, impairing the protection function through a common mode failure. Separation of redundant analog channels originates at the process sensors and continues along the field wiring, through containment penetrations, to the analog protection racks. As mentioned previously under GDC 20, some sensors for pressurizer pressure and reactor coolant flow may share common sensing lines, but the consequence of a line failure (rupture) will not prevent a protective action from occurring.

Separation of redundant protection channel/train field wiring is achieved using separate wireways, cable trays, conduit runs, and containment penetrations for redundant channels and trains. Separate, dedicated racks for each channel and train are provided to terminate the field wiring, so that internal wiring within a rack is limited to a single channel or train. Power supplies to redundant channels and trains are provided from separate 120 VAC instrument buses and from separate DC buses, respectively.

Original plant design required separation of main control board power and control wiring that was associated with redundant safety-related train components. Cables for non-vital circuits were not excluded from wireways carrying train A or train B cables. Instrumentation wiring associated with reactor protection or safeguards channels was exempted from separation inside the main control boards because these wires are isolated from their associated safeguards or protection rack by isolation amplifiers or relays. The following instructions were established by Westinghouse during plant construction to effect the cable separation within the main control board in accordance with agreements with the AEC (Reference 1, Reference 2, Reference 3 and Reference 4).

- Wiring requiring separation shall use separate routing of wireways between devices. In no case shall wiring requiring separation be bundled together.

- Devices (switches for example) having connecting wiring requiring separation shall have that wiring separately bundled and routed to obtain physical separation immediately upon leaving the device terminals. Separate routing or wireways to terminal blocks shall be used.
- Wires requiring separation shall terminate on separate terminal blocks for field connections.

Confirmation that physical separation for wiring inside the main control boards is a licensing basis requirement was provided in a Wisconsin Electric letter to the NRC, dated April 16, 1997 (Reference 5). Modifications MR 93-025*A -*H were initiated to improve electrical separation in the main control board and included wrapping cables with a fire retardant material called Siltemp to provide a barrier between redundant trains where adequate physical separation was not practical. *

Section 7.2 and Section 7.3 discuss certain protection system backup trips that may not fully meet wiring separation criteria for redundant trains. However, failure of a backup trip circuit does not prevent proper protective action of primary trips assumed in the accident analyses, and does not represent a loss of the protective function discussed in GDC 23.

Refer to Section 8.0 for a discussion of cable and internal wiring separation criteria and environmental qualification criteria.

Environmental qualification of electrical/electronic equipment is addressed in Section 7.2.3.5.

Protection system components are designed to function under their normal service environments. Under accident conditions, protection system components are either located in a mild environment (such as the control room or cable spreading room) or are located in a potentially harsh accident environment (such as containment). Components in mild environments do not require formal environmental qualification. Protection system components located in potentially harsh environments only require formal environmental qualification if:

1. the component is required to mitigate the accident that creates the harsh environment and the harsh environment degrades the component performance before the protective function occurs, or

2. the component is used for post-accident functions not related to the protection function.

Seismic qualification of protection system components is addressed in Section 7.2.3.4. The seismic design requirement is that for the maximum potential earthquake, the equipment will not lose its capability to perform its protective function; namely, to shut the reactor down and/or maintain the unit in a safe shutdown condition. It is conceivable that protection system equipment may have permanent deformation due to stresses from the maximum potential earthquake; however, the deformation will not impede its ability to perform the protective function.

* Wrapping cables with Siltemp does not create an Appendix R qualified fire barrier.

Demonstration of Functional Operability of Protection Systems (GDC 25)

> 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.

DISCUSSION

During power operation, each reactor protection channel and logic train is capable of being calibrated and tripped independently by simulated signals to verify its operation, without tripping the plant. The testing scheme includes checking through the trip logic to the reactor trip breakers. Thus, the operability of each channel and logic train can be determined conveniently and without ambiguity.

During power operation, each engineered safety features actuation channel and logic train is capable of being calibrated and tripped independently by simulated signals to verify its operation up to the final actuation device. Because ESF equipment actuation would adversely impact plant operation at power, the final ESF actuation devices are not cycled while the reactor is at power. A resistance check of the relay coils is performed at power, but actuation of ESF equipment is performed during refueling shutdowns, rather than at power.

Protection Systems Failure Analysis Design (GDC 26)

> 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.

DISCUSSION

Each reactor protection channel and train is designed on the "de-energize to operate" principle; an open circuit or loss of power causes the respective channel or train to go into its tripped condition (the "preferred failure" direction).

The analog channels for the engineered safety features actuation system, with the exception of containment spray actuation, are designed on the same "de-energize to operate" principle as the reactor protection channels. The high-high containment pressure channels for containment spray actuation are designed as energize-to-operate, to avoid spray operation on inadvertent channel power failures.

Regarding the two ESF actuation trains, the output relays are "energize-to-operate" and require power to actuate ESF equipment. This design prevents inadvertent ESF equipment actuation on power failure of an actuation train (the "preferred failure" direction).

Reactivity Shutdown Capability (GDC 29)

> One of the reactivity control systems shall be capable of making the core subcritical under any anticipated operating condition (including anticipated operational transients) sufficiently fast to prevent exceeding acceptable fuel damage limits. Shutdown margin should assure subcriticality with the most reactive control rod fully withdrawn.

DISCUSSION

The reactor core, together with the reactor control and protection system, is designed so that the minimum allowable DNBR is no less than the design basis limit DNBR and there is no fuel melting during normal operation, including anticipated transients.

The shutdown rod groups are provided to supplement the control groups of rod cluster control assemblies (RCCAs) to make the reactor at least one percent subcritical ($K_{eff} = 0.99$) following a trip from any credible operating condition to the hot zero power condition, assuming the most reactive RCCA remains in the fully withdrawn position.

Sufficient shutdown capability is also provided to maintain the core subcritical, with the most reactive rod assumed to be fully withdrawn, for the most severe anticipated cooldown transient associated with a single active failure, e.g., accidental opening of a steam bypass (condenser steam dump) or relief valve. This is achieved with a combination of control rods and automatic boron addition via the safety injection system.

Reactivity Control Systems Malfunction (GDC 31)

> 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.

DISCUSSION

Continuous rod withdrawal accidents from both subcritical and at-power conditions are analyzed plant transients that rely on an automatic reactor trip for core protection. Automatic reactor trip is completely independent of the normal RCCA control functions, since the reactor trip breakers interrupt the power to the control rod drive mechanisms regardless of existing control signals.

Other General Design Criteria

The following GDCs broadly apply to plant equipment, including instrumentation and controls, and are discussed in other sections, as noted:

GDC 1	Quality Standards	Sections 4.1
GDC 2	Performance Standards	Sections 4.1
GDC 39	Emergency Power	Section 8.1
GDC 40	Missile Protection	Sections 4.1

7.1.3 OTHER CRITERIA

In addition to the General Design Criteria discussed above, the following criteria apply to specific instrumentation:

a. IEEE 279-1968, Proposed IEEE Criteria for Nuclear Power Plant Protection Systems.

The reactor protection system (Subsection 7.2), the engineered safety features actuation system (Subsection 7.3) and portions of the nuclear instrumentation system (Subsection 7.6) are required to meet the design criteria of IEEE 279-1968. The compliance of each system with IEEE 279 is discussed in the individual system subsection.

b. Regulatory Guide 1.97, Rev. 2, Instrumentation to Assess Plant and Environs Conditions during and following an Accident.

Post-accident monitoring instrumentation is required to meet the intent of Regulatory Guide 1.97, Rev. 2. Section 7.6.2 discusses the specific plant variables to which this regulatory guide applies and the type and category of each variable.

7.1.4 REFERENCES

1. Westinghouse Letter to Bechtel Corporation, PBW-B-3145, Point Beach Nuclear Plant Control Board Rerouting, dated February 25, 1970.

2. Westinghouse Engineering Change Notice, ECN-WEP-70083, Main Control Board, Initiated February 10, 1970.

3. Response to AEC Question 7.6, Cable Installation Design Criteria, January 16, 1970.

4. Response to AEC Question 7.3, Isolation of Reactor Protection and Engineered Safety Features Signals to Annunciators and Data Logger/Computer, January 16, 1970.

5. Wisconsin Electric Letter to NRC, Main Control Board Wiring Separation Operability Determination and Restoration Plan, Point Beach Nuclear Plant, Units 1 and 2, dated April 16, 1997.

7.2 REACTOR PROTECTION SYSTEM

The Reactor Protection System (RPS) monitors parameters related to safe operation and automatically trips the reactor to protect the reactor core against fuel rod cladding damage due to Departure from Nucleate Boiling (DNB). It also assists in protecting against Reactor Coolant System (RCS) damage caused by high system pressure by limiting energy input to the system through reactor trip action.

7.2.1 DESIGN BASES

The following PBNP General Design Criteria (GDC) as described in Section 7.1.2 are applicable to the Reactor Protection System:

Criterion 12: Instrumentation and Control Systems
Criterion 13: Fission Process Monitors and Controls
Criterion 14: Core Protection Systems
Criterion 19: Protection Systems Reliability
Criterion 20: Protection Systems Redundancy and Independence
Criterion 23: Protection Against Multiple Disability for Protection Systems
Criterion 25: Demonstration of Function Operability of Protection Systems
Criterion 26: Protection Systems Failure Analysis Design
Criterion 29: Reactivity Shutdown Capability
Criterion 31: Reactivity Control Systems Malfunction

In addition to the above mentioned GDC, the Reactor Protection System is also designed to IEEE 279, "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems" dated August 1968.

7.2.1.1 Conformance to IEEE 279-1968

a. Plant Conditions that Require RPS

The Reactor Protection System is required to protect two of the three physical barriers that guard against the uncontrolled release of radioactivity; (1) fuel clad and (2) reactor coolant system pressure boundary. Chapter 14 describes the accidents that RPS is required to operate under to protect the above mentioned barriers. Note that different accidents may actuate different RPS trips and that not all accidents described in Chapter 14 require the operation of RPS.

b. Plant Variables that Cause Protective Action

The process variables that actuate each RPS trip are identified in Table 7.2-1.

c. Minimum Number of Sensors for Each Variable

The minimum number of sensors assigned to each RPS variable is listed in Technical Specifications.

d. Prudent Operational Limits for Each Variable

The normal operational limits for each RPS variable are defined in the plant operating procedures and Technical Specifications.

e. Margin Between Operational Limits and Onset of Unsafe Conditions

The margin between each RPS variable's operational limit and the analytical limit required for automatic RPS actuation is determined by the RPS setpoints established for the variable in Technical Specifications. (Reference Section 7.2.3.6)

f. Variable Levels that Require Protective Action

The analytical limits established in the accident analyses (Chapter 14) determine the point at which the variables require RPS actuation.

g. Condition for System Performance

The operational conditions (e.g., environmental, seismic, power source, etc.) under which the RPS equipment must function are discussed in Section 7.2.3.4 and Section 7.2.3.5.

h. Performance Requirements of RPS Variables

The range, response time and accuracy requirements of the RPS equipment are chosen to ensure the assumptions of the accident analysis for the variables being monitored are met.

i. Single Failure

No single failure within the reactor protection system or in an associated system, which supports its operation, shall prevent the operation of the reactor protection system.

j. Redundancy and Independence

The reactor protection system is redundant and independent for all primary inputs and functions. Each channel is functionally independent of every other channel and receives power from a separate AC power source. Each train is functionally independent of the redundant train and receives power from a separate DC power source.

k. Manual Actuation

Means are provided for the manual initiation of protective action. Failures in the automatic system will not prevent the manual actuation of protective functions.

l. Channel Bypass or Removal from Operation

The reactor protection system is designed to permit any one channel to be maintained, tested or calibrated during power operation without causing a system trip. During such operation, the active parts of the system continue to meet the single failure criterion, since the channel under test is either tripped or makes use of superimposed test signals, which do not prevent the process signal from actuating the channel.

EXCEPTION: Channels for “one-out-of-two” trip logic are permitted to violate the single failure criterion during channel bypass provided that acceptable reliability of operation can be otherwise demonstrated.

m. Capability for Test and Calibration

The bistable portions of the reactor protection system provide trip signals only after signals from the analog portions of the system reach a preset value. Capability is provided for calibrating and testing the performance of the bistable portion of protection channels and various combinations of the logic network during power operation.

The sensor portion of the protection channel provides an analog signal of the process parameter. The analog portion of a channel can be checked in various ways during power operation, for example:

- varying the monitored parameter,
- introducing and varying a substitute transmitter signal, and
- cross-checking between channels that bear a known relationship to each other and that have readouts available

The design of the system provides for administrative control for the purpose of manually bypassing channels for test and calibration purposes. The design also provides for administrative control of access to all trip settings, module calibration adjustments, test points, and signal injection points.

n. Information Readout

The reactor protection system provides the operator with complete information pertinent to system status and plant safety. All transmitted signals (flow, pressure, temperature, etc.), which can lead to a reactor trip are either indicated and/or recorded for every channel. All neutron flux power range currents (top detector, bottom detector, and algebraic difference and sum of the bottom and top detector currents) are indicated and/or recorded.

Alarms are also provided to alert the operator of deviation from normal operating conditions so that corrective action can be taken prior to reaching a reactor trip setting. In addition, any control rod stop or trip of any reactor trip channel will actuate an alarm.

o. Operating Bypasses

Where operating requirements necessitate automatic or manual bypass (block) of a protection function, the design is such that the bypass is automatically removed whenever the permissive conditions are not met. Devices used to achieve automatic removal of the bypass of a protection function are part of the protection system.

p. Indication of Bypasses

Indication is provided on the main control board if some part of the system has been administratively bypassed or taken out of service.

q. Multiple Trip Settings

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 settings are used. The devices used to prevent improper use of less restrictive trip settings are considered a part of the protective system and are designed

in accordance with the other provisions of the IEEE 279-1968. Multiple trip setpoints are used for monitoring neutron flux during the different modes of operation.

r. Completion of Protective Action

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

s. Protective Actions

The reactor protection system is designed to automatically trip the reactor under the conditions identified in Table 7.2-1.

Interlocking functions of the reactor protection system prevent control rod withdrawal (rod stops) when a specified parameter reaches a preset value, which is less than the value at which a reactor trip is initiated.

For anticipated abnormal conditions, the reactor protection system in conjunction with inherent plant characteristics and the engineered safety features are designed to assure that the limits for energy release to the containment and for radiation exposure are not exceeded.

t. Adverse Environment

The reactor protection system equipment is either located in a mild environment (such as the control room) or a potentially harsh environment (such as containment). The requirements of the equipment are discussed further in Section 7.2.3.5.

7.2.1.2 Exceptions to IEEE 279

a. Backup/Anticipatory Trips

Some of the backup/anticipatory reactor protection system functions that are not assumed in the accident analyses may not fully conform to the IEEE 279 criteria. The specific backup/ anticipatory trips that do not fully conform to IEEE 279 are:

Reactor coolant pump breaker position, Reactor trip on turbine trip (stop valve position and low turbine auto stop oil pressure) and Steam/Feedwater Flow Mismatch Trip.

The exceptions to IEEE 279 include circuits that contain non-safety-related contacts and/or field wiring that may not meet safety-related train separation criteria, and single failure scenarios that may defeat the backup trip functions. Exceptions to the separation criteria are allowed in these cases based on the electrical isolation of the non-conforming circuits such that an electrical fault in the backup trip field wiring will not propagate into and disable the primary trip circuits. Exceptions to single failure criteria in backup trips are allowed because the backup trip functions are not required for plant protection, and their failure will not affect the primary trip functions assumed in the accident analyses.

b. Permissives

Permissive P-9 logic does not fully comply with IEEE 279 due to the fact that the permissive is disabled by non-safety related, non-seismically qualified contacts (high condenser pressure and operating status of circulating water pumps). Exception to IEEE 279 is allowed because the

failure of the P-9 permissive will result in a reactor trip, which is "fail-safe". No failure associated with the P-9 permissive will prevent the RPS from performing its primary trip functions assumed in the accident analyses. Refer to Section 7.2.3.3.

c. Sensing Lines

Some of the sensors used to initiate reactor trips have shared sensing lines. The following two trip parameters share common sensing lines between redundant RPS transmitters:

- Low pressurizer pressure, and
- Low reactor coolant flow

The above trip parameter sensors are allowed to share common sensing lines because no credible failure associated with the sensing lines will prevent the primary trip functions assumed in the accident analyses. Refer to Section 7.2.3.3.

7.2.2 SYSTEM DESIGN

7.2.2.1 Reactor Protection System Description

The RPS 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. The reactor core safety limits are shown in the Core Operating Limits Report (COLR), TRM Section 2.1, for each unit.

Since thermal core power may be represented by the increase in reactor coolant temperature across the core, it is possible to represent the correlation of core inlet temperature and core power in terms of measured plant variables, via reactor coolant temperature difference (ΔT) and the average reactor coolant temperature (T_{avg}). Therefore, the reactor core safety limit curve in TRM Section 2.1 can be included in Figure 7.2-2.

Since the thermal hydraulic properties of compressed water are nonlinear, linearization of Figure 7.2-2 is accomplished by linearizing the pressure level curves (bold solid lines). The linearization establishes pressure level lines in which the DNBR is greater than the safety limit value, thus introducing additional conservatism in the control and protection system design. This ensures that adequate margins exist between the maximum nominal steady state operating point (which includes allowance for temperature, calorimetric, and pressure errors) and the required reactor trip points to avoid a spurious plant trip during design transients.

A simplified block diagram illustrating the reactor protection system is shown in Figure 7.2-3. The reactor protection system consists of four instrument channels that monitor up to four various plant parameters, depending on the coincidence logic required for the specific trip. Each protection channel terminates at a channel trip bistable in the analog protection racks. Each channel trip bistable controls two independent and redundant logic relays associated with the two independent and redundant trains ("A" and "B"). The logic relays for each train are combined in a coincidence logic network (e.g., two-out-of-four). The coincidence logic networks terminate at parallel reactor trip relays as shown in Figure 7.2-6. The logic and reactor trip relays are located in the Train "A" and "B" logic racks.

Although a single reactor trip relay would be sufficient to trip the reactor, parallel reactor trip relays were installed for power generation reliability. The use of parallel relays prevents an unnecessary reactor trip should a single reactor trip relay fail.

Where redundant protective channels are combined to provide non-protective functions, the required signals are derived through isolation amplifiers. These devices are designed so that open or short circuit conditions, as well as the application of 120 VAC or 125 VDC, to the isolated side of the circuit will have no adverse effect on the input or protection side of the circuit. Therefore, failures on the non-protective side of the system will not affect the individual protection channels.

Two independent and redundant reactor trip breakers in series provide power to the control rod drive mechanisms. In addition, two independent and redundant bypass breakers are provided in parallel with the reactor trip breakers to allow for continued reactor operation during testing of the reactor trip breakers.

When the required number of channels (e.g., two-out-of-four) indicate that a plant parameter is outside its acceptable operating limit, their associated channel bistables are tripped. The tripping of the channel bistables result in the tripping of their associated coincidence logic relays for each train, which in turn results in de-energizing the reactor trip relays. De-energizing the reactor trip relays causes the associated train trip breaker to open by de-energizing its undervoltage trip coil and by energizing its shunt trip coil through an interposing relay. De-energizing the reactor trip relays also causes the opposite train bypass breaker to open by de-energizing its undervoltage trip coil.

The shunt trip attachment, which provides a diverse method from the undervoltage coil for tripping the reactor trip breakers, was installed in response to Generic Letter 83-28.

Manual reactor trip switches are also installed between the train logic and the reactor trip breakers, to allow the operator to initiate a reactor trip independent from an automatic reactor trip. When the reactor trip breakers are tripped, the power to the control rod drive mechanisms is interrupted, which allows the control rods to insert into the core by gravity. A simplified diagram is shown in Figure 7.2-4.

7.2.2.2 Protective Actions

Rapid reactivity shutdown is provided by the insertion of the rod control cluster assemblies (RCCAs) by gravity. Reactor Trip Breakers RTA and RTB are duplicate series-connected circuit breakers that provide the power to the control rod drive mechanisms. The control rod drive mechanism (CRDM) must be energized to keep the associated RCCAs withdrawn from the core. Automatic reactor trip occurs upon the loss of power to the RCCAs. The reactor trip breakers are opened by either their undervoltage or shunt trip coils. Any one of several trip signals will simultaneously de-energize the undervoltage coil and energize the shunt trip coil.

The components providing power to the circuit breakers' undervoltage and shunt trip attachment are designed to open the reactor trip breakers on a reactor trip signal. In addition, upon power loss, the undervoltage trip coils will cause the breakers to trip. The system is designed so that once a reactor trip is initiated, it cannot be bypassed and it goes to completion. Return to normal operation requires operator action to reset the reactor trip breakers and withdraw the control rods.

Certain reactor trip channels are automatically blocked below a certain power level, and some are manually blocked above a certain power level where they are not required for safety. Nuclear

source range, intermediate range and power range (low setting) trips are specifically provided for protection at low power or subcritical operation; for higher power operations, they are blocked by manual action. The design provides for the automatic removal of the automatic and manual blocks whenever the permissive conditions are no longer met.

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

Interlocks are also provided to avoid a reactor trip by preventing control rod withdrawal (rod stop) when a specified parameter reaches a value which is less than the limit at which a reactor trip is initiated. These parameters are discussed in Section 7.7.1.

All transmitted signals (e.g., flow, pressure, temperature, etc.) which can result in a reactor trip are indicated and/or recorded for every channel. In addition, alarms are also used to alert the operator of a plant parameter that has deviated from its normal operating band, so that corrective action can be taken prior to reaching the reactor trip limit. In addition, the actuation of any control rod stop or the trip of any reactor protection channel will actuate an alarm.

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., P-7), are listed in Table 7.2-2.

a. Manual Trip

The manual reactor trip pushbuttons are independent of the automatic trip circuitry, and are not subject to failures which make the automatic circuitry inoperable. Any of four manual trip pushbuttons per unit (eight total) located in the control room can initiate a manual reactor trip.

b. High Nuclear Flux (Power Range) Trips

The purpose of these trips is to protect against reactivity excursions during subcritical to low power operation (low setting) and power operation (high setting) to prevent DNB. The reactor is tripped when two-out-of-four power range channels are above the trip setpoint. The low setting can be manually blocked when two-out-of-four power range channels are above the P-10 block setpoint of approximately 10% power. When three-out-of-four channels are below the P-10 unblock setpoint, the trip is automatically reinstated. This ensures that the more restrictive setting is used when required. The high setting is always active.

c. High Nuclear Flux (Intermediate Range) Trip

The purpose of this trip is to protect against reactivity excursions during subcritical to low power operation to prevent DNB. The reactor is tripped when one-out-of-two intermediate range channels are 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 P-10 block setpoint of approximately 10% power. When three-out-of-four channels are below the P-10 unblock setpoint, the trip is automatically reinstated. The intermediate range channels (including detectors) are separate from the power range channels.

d. High Nuclear Flux (Source Range) Trip

The purpose of this trip is to protect against reactivity excursions during reactor startup from subcritical conditions proceeding into the power range. The reactor is tripped when one-out-of-two source range channels are above the trip setpoint. This trip, which provides protection during reactor startup, can be manually blocked when one-out-of-two intermediate range channels are above the P-6 permissive setpoint. When both (two-out-of-two) intermediate range channels are below the P-6 permissive setpoint, the trip is automatically reinstated. This trip is also automatically blocked when two-out-of-four high power range signals are above the P-10 block setpoint of approximately 10% power.

The source range trip setpoint is between the P-6 permissive setpoint (P-6 allows the manual de-energization of the source range high voltage power supply) and the maximum source range power level detection limit.

e. Overtemperature ΔT Trip

The purpose of this "calculated" trip is to protect the core against DNB. The reactor is tripped when two-out-of-four signals, with two sets of temperature measurements per loop, are above the trip setpoint. Two setpoints for this reactor trip are continuously calculated for each loop by solving the following equation (simplified version):

$$\Delta T \text{ setpoint} = K_1 - K_2 T_{avg} + K_3 P - f(\Delta I)$$

Where:

T_{avg}	=	Average reactor coolant temperature (°F), four independent measurements (lead-lag compensated)
P	=	Pressurizer pressure, four independent measurements (psia)
K_1, K_2, K_3	=	Setpoint constants derived from Technical Specifications
$f(\Delta I)$	=	A function of flux difference between upper and lower detectors of the power range ion chambers, four independent measurements.

Each of the four power range ion chamber units separately feeds one overtemperature ΔT trip channel. Thus, a single failure neither defeats the trip function nor causes a spurious trip. Resultant changes in f(ΔI) can only lead to a decrease in trip setpoint.

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

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

where

$\Delta T_{\text{rod stop}}$	=	$\Delta T_{\text{setpoint}} - B_P$
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. This gives the operator the opportunity to adjust the rods and reshape the flux before a reactor trip occurs.

f. Overpower ΔT Trip

The purpose of this "calculated" trip is to protect against excessive power level (fuel rod rating protection). The reactor is tripped when two-out-of-four signals, with two sets of temperature measurements per loop, are above the trip setpoint.

The setpoint for this reactor trip is continuously calculated for each channel by solving the following equation (simplified version):

$$\Delta T_{setpoint} = K_4 - f(T_{avg})$$

where:

K_4 = A setpoint constant derived from Technical Specifications

$f(T_{avg})$ = Function based on the effect of density and specific heat of water as a function of average temperature.

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

g. Low Pressurizer Pressure Trip

The purpose of this trip is to protect against excessive boiling in the core and limit the range of required protection from the overpower and overtemperature delta T trips. Above either P-7 permissive setpoint of approximately 10% reactor power or approximately 10% turbine power, the reactor is tripped when two-out-of-four low pressurizer pressure signals are below the setpont. This trip is automatically blocked by the P-7 permissive, when three-out-of-four power range channels and both turbine first stage pressure channels are below their respective P-7 permissive setpoints. When two-out-of-four power range channels or one-out-of-two turbine first stage pressure channels are above their respective P-7 setpoints, the reactor trip is automatically reinstated.

h. High Pressurizer Pressure Trip

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

i. High Pressurizer Water Level Trip

The trip is a backup to the high pressurizer pressure trip. Above either P-7 permissive setpoint of approximately 10% reactor power or approximately 10% turbine power, the reactor is tripped when two-out-of three high pressurizer water level signals are above the setpoint. This trip is automatically blocked by the P-7 permissive, when three-out-of-four power range channels and both turbine first stage pressure channels are below their respective P-7 permissive setpoints. When two-out-of-four power range channels or one-out-of-two turbine first stage pressure channels are above their respective P-7 setpoints, the reactor trip is automatically reinstated.

j. Low Reactor Coolant Flow Trip

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

1. Measured Low Coolant Flow in the Reactor Coolant Piping.

   Above the P-8 permissive setpoint of approximately 35% reactor power, the reactor is tripped when two-out-of-three flow signals for either reactor coolant loop are below their low flow setpoint. This trip is automatically blocked when three-out-of-four power range channels are below the P-8 permissive setpoint. When two-out-of-four power range channels are above the P-8 permissive setpoint, the reactor trip is automatically reinstated.

   Above either P-7 permissive setpoint of approximately 10% reactor power or approximately 10% turbine power, the reactor is tripped when two-out-of-three flow signals for both reactor coolant loops are below their low flow setpoint. This trip is automatically blocked by the P-7 permissive, when three-out-of-four power range channels and both turbine first stage pressure channels are below their respective P-7 permissive setpoints. When two-out-of-four power range channels or one-out-of-two turbine first stage pressure channels are above their respective P-7 setpoints, the reactor trip is automatically reinstated.

   The elbow tap configuration used for reactor coolant loop flow measurement is discussed in Section 4.2.

2. Monitored Electrical (Voltage) Supply and Breaker Position to the Reactor Coolant Pumps.

   Above either P-7 permissive setpoint of approximately 10% reactor power or approximately 10% turbine power, the reactor is tripped when one-out-of-two undervoltage relays on both 4160 volt buses (A01 and A02) are below their setpoint. This trip is automatically blocked by the P-7 permissive, when three-out-of-four power range channels and both turbine first stage pressure channels are below their respective P-7 permissive setpoints. When two-out-of-four power range channels or one-out-of-two turbine first stage pressure channels are above their respective P-7 setpoints, the reactor trip is automatically reinstated.

   Above the P-8 permissive setpoint of approximately 35% power, the reactor is tripped when either reactor coolant pump breaker is open. This trip is automatically blocked when three-out-of-four power range channels are below the P-8 permissive setpoint. When two-out-of-four power range channels increase above the above the P-8 permissive setpoint, the reactor trip is automatically reinstated.

   Above either P-7 permissive setpoint of approximately 10% reactor power or approximately 10% turbine power, the reactor is tripped when both reactor coolant pump breakers are open. This trip is automatically blocked by the P-7 permissive, when three-out-of-four power range channels and both turbine first stage pressure channels are below their respective P-7 permissive setpoints. When two-out-of-four power range channels or one-out-of-two turbine first stage pressure channels are above their respective P-7 setpoints, the reactor trip is automatically reinstated.

A reactor coolant pump breaker is tripped (opened) when two-out-of-two undervoltage or one-out-of-one fault relays on the breaker's associated 4160 volt bus (A01 or A02) are below the trip setpoint. Both reactor coolant pump breakers are tripped when one-out-of-two underfrequency relays on both 4160 volt buses (A01 and A02) are below the trip setpoint.

k. Safety Injection System Actuation Trip

The reactor trip occurs when the safety injection system is actuated. The means of actuating safety injection is described in Section 7.3. Either Train "A" or "B" of safety injection will actuate a reactor trip signal in both Trains "A" and "B" of reactor protection.

l. Turbine Generator Trip

The reactor is tripped when two-out-of-three low pressure signals that monitor the turbine autostop oil pressure are below the setpoint or when two-out-of-two turbine stop valves close, which would indicate that the turbine has tripped. This trip is automatically blocked by the P-9 permissive when three-out-of-four power range detectors are below approximately 50% power, one-out-of-two circulating pumps are running, condenser vacuum exists and full power Tavg is $\geq$572°F. The trip is automatically reinstated when two-out-of-four power range detectors are above approximately 50% power or two-out-of-two circulating pumps are not running or condenser vacuum does not exist. When full power Tavg is <572°F the reactor trip is blocked and reinstated as described above except the P-9 power range detector setpoint is set at approximately 35% power.

This trip is also automatically blocked by the P-7 permissive, when three-out-of-four power range channels and both turbine first stage pressure channels are below their respective P-7 permissive setpoints. When two-out-of-four power range channels or one-out-of-two turbine first stage pressure channels are above their respective P-7 setpoints of approximately 10% reactor power or 10% turbine power, the reactor trip is automatically reinstated.

m. Steam/Feedwater Flow Mismatch Trip

The purpose of this trip is to protect the reactor from a sudden loss of its heat sink. The reactor is tripped when one-out-of-two circuits monitoring steam/feedwater flow for each steam generator indicate a flow mismatch and the corresponding loop low level steam generator signals are below the trip setpoint.

n. Low-Low Steam Generator Water Level Trip

The purpose of this trip is to protect the steam generators and to protect the reactor from a loss of its heat sink in the case of a sustained steam/feedwater flow mismatch of insufficient magnitude to cause a flow mismatch reactor trip. The reactor is tripped when two-out-of-three low-low steam generator water level signals in either steam generator are below the trip setpoint.

7.2.2.3 System Safety Features

a. Isolation of Redundant Protection Channels and Trains

The reactor protection system is designed to achieve isolation between redundant protection channels and trains. The channel design applies to the analog portions through the channel trip bistable and the train design applies to the logic portions as illustrated by Figure 7.2-4. Although the illustration is for a four channel coincidence, the design is also applicable to two and three channel coincidence logics.

The reactor protection system is comprised of identifiable channels which are physically, electrically and functionally separated and isolated from one another. Each channel is energized from a separate AC power feed. Isolation of redundant analog channels originates at the process sensors and continues along the field wiring and through containment penetrations to the analog protection racks. Isolation of field wiring is achieved using separate wireways, cable trays, conduit runs, and containment penetrations for each redundant channel. Analog equipment is isolated by locating redundant components in different protection racks.

The transition from channel identity to train identity occurs at the logic relay coil/relay contact interface. As such, there is both electrical and physical separation between the channel and the train portions of the protection system. The “coil side” of each logic relay is associated with the channel logic, and the “contact side” of each logic relay is associated with the train logic. The channel trip bistables are mounted in the analog protection racks and are the final operational component in an analog protection channel. Each bistable drives two logic relays, one for Train “A” and one for Train “B.”

Train separation is achieved by providing separate racks. Physical separation is provided between these racks. Each train is energized from a separate DC power feed. The contacts from the Train “A” relays are interconnected to form the required actuation logic for one reactor trip breaker.

The above configuration is duplicated for the other reactor trip breaker using the contacts from the Train “B” relays. Therefore, the two redundant reactor trip trains are physically separated and electrically isolated from one another.

b. Loss of Power

The four RPS channels are powered from four separate and independent 120 VAC instrument buses, which are battery backed. The logic racks for the two RPS trains are powered from separate and independent 125 VDC sources. See Chapter 8 for a further discussion on 120 VAC and 125 VDC buses.

Availability of power to the reactor protection system channels and trains is continuously indicated. Loss of AC power to an individual RPS channel will cause the channel’s bistables to trip, causing the affected channel to trip. The tripping of a channel is annunciated in the Control Room. All bistables are normally energized and de-energize to actuate. Therefore, the loss of power results in the channel going to its “fail-safe” state. Since the reactor protection system requires the tripping of at least two coincident channels, the loss of power to one reactor protection channel will not result in a reactor trip. However, the loss of DC power to an individual RPS train will result in the tripping of the reactor trip breakers, which will result in a reactor trip.

c. Reactor Trip Signal Testing

The train logic portion of the reactor protection system initiates a reactor trip only after signals from the analog channel portion of the system reach a preset value. Capability is provided for calibrating and testing the performance of the channel trip bistables, and various coincidence combinations of the train logic during reactor operation.

1. Analog Channel Testing

The basic elements comprising an analog protection channel are shown in Figure 7.2-5, and consist of a transmitter, power supply, bistable, bistable trip switch and proving lamp, test signal injection switch, test signal injection jack and test point.

Each 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 the test panel. Opening the cover or placing the test-operate switch in the "TEST" position will initiate an alarm. These alarms are arranged on a rack basis to preclude entry to more than one redundant protection rack (or channel) at any time. The test panel cover is designed such that it cannot be closed (and the alarm cleared) unless the test signal plugs (described below) are removed. Closing the test panel cover will mechanically return the test switches to the "OPERATE" position.

During power operation, administrative procedures require that the affected channel is placed in its tripped state before that channel is taken out of service for repair or testing, so that the minimum degree of redundancy is met for its intended function. This places a proving lamp across the bistable output so that the bistable trip point can be checked during channel calibration. The bistable trip switches must be manually reset after completion of a test. Closing the test panel cover will not restore the bistable trip switches to the untripped mode. However, the annunciator on the main control board cannot be reset until these switches are returned to the untripped mode.

Provisions have been implemented for the insertion of test signals in each analog loop. Channel calibration consists of inserting a test signal from an external calibration signal source into the test signal injection jack. Where applicable, the channel power supply will serve as a power source for the calibration source and permit verifying the output load capacity of the power supply. Test points are located in the analog channel and provide an independent means of measuring the calibration signal level. Transmitters and sensors are checked against each other and/or precision test equipment during normal operation.

In the source and intermediate ranges where the trip logic is one-out-of-two for each range, bypasses are provided for testing and the trip logic reverts to one-out-of-one, which is allowed by Section 4.11 of IEEE 279-1968.

Nuclear instrument power range channels are tested by superimposing a test signal on the normal sensor signal so that the reactor trip function is not bypassed. Based upon the two-out-of-four logic, this will not trip the reactor; however, a reactor trip will occur if required.

2. Logic Testing

The general design features of the logic system are described below. Each analog channel trip bistable drives two logic relays (one for Train "A" and one for Train "B"). The typical two-out-of-three logic network (e.g., high pressurizer level) is represented by contacts "A" and "B", whereas the typical two-out-of-four logic network (e.g., low pressurizer pressure) is represented by contacts "C" and "D" in Figure 7.2-6.

The parallel reactor trip relays are represented by "E" and "F" for Train "A", and "G" and "H" for Train "B". The reactor trip relays are de-energized when the required coincidence logic (e.g., two-out-of-three) is met, which results in the de-energization of the undervoltage coil and energization of the shunt trip attachment.

A series configuration is used for the reactor trip breakers so that no single failure will prevent the interruption of power to the control rod drive mechanisms. This approach is consistent with a de-energize-to-trip preferred failure mode. Each reactor trip breaker is tripped by removing power to its undervoltage trip coil as well as energizing its shunt trip coil.

The train logic testing includes exercising the reactor trip breakers to demonstrate their operability. Bypass breakers are provided to prevent an inadvertent reactor trip when the reactor trip breaker being tested is tripped; however, a valid reactor trip will still occur, if required, by tripping the reactor trip breaker not under test. During normal operation, the bypass breakers are open. Administrative control is used to minimize the amount of time these breakers are closed, and to prevent the simultaneous closure of both bypass breakers. Indication of a closed bypass breaker is provided locally, on the test panel, and on the main control board. Also, if both bypass breakers are simultaneously racked in, with one being used for the bypass function, a reactor trip will result.

As shown in Figure 7.2-6, the trip signal from the channel network for Train "A" is designed to trip (open) Reactor Trip Breaker RTA as well as the Bypass Breaker BYB. The Train "B" logic applies to the RTB and BYA. Therefore, if a valid trip signal occurs while BYA is closed to bypass RTA during testing, RTB and BYA will be tripped by the coincidence logic for Train "B", which would result in the removal of power to the control rod mechanisms and a reactor trip. In addition, RTA would either have been tripped manually as part of the test or would be tripped through its associated coincidence logic.

An auxiliary relay is located in parallel with the undervoltage coil and shunt trip attachment of each reactor trip breaker. This relay is connected to the events recorder. In addition, lights are provided to indicate the status of the individual logic relays.

The following procedure illustrates the method used for testing RTA and its associated logic network.

1. With the bypass breaker (BYA) in the test position, locally close the BYA breaker. Trip BYA from the logic test panel to verify operation.

2. Rack in and close BYA.

3. Perform a verification of the shunt trip block mechanism. Then, with the shunt trip block actuated, do an independent test of the undervoltage trip mechanism.

   De-energize the logic relays (A1, A2, A3) for one logic combination (1 and 2, 1 and 3, or 2 and 3) and verify that the logic network de-energizes the undervoltage coil on RTA. The first combination tested will physically trip the breaker.

   Reclose the breaker and with the shunt trip block signal cleared, perform an independent check of the shunt trip coil by actuating the shunt trip pushbutton. This also physically trips the breaker. These two tests verify that the reactor trip breaker will be tripped either by the undervoltage or the shunt trip coils.

   The other two logic combinations are then tested to verify that the logic network de-energizes the undervoltage coil and would energize the shunt trip coil. Since the events recorder or white test light monitors the signal applied to the undervoltage coil, signal verification can be determined from the events recorder or the white test light.

4. Repeat step 3 for every logic combination associated with the logic network for the undervoltage coil test; however, the reactor trip breaker is not tested again.

5. Reset RTA. Trip and rack out BYA.

   In order to minimize the possibility of operational errors (such as tripping the reactor inadvertently or only partially checking all logic combinations), each train 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 7.2-7. The test switches used to de-energize the trip bistable relays operate through interposing relays as shown on Figure 7.2-5. 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 isolation of redundant protection channels are maintained by the inclusion of the interposing relay which is actuated by the logic test switches.

7.2.2.4 Conformance With Generic Letter 83-28

The following design features and maintenance requirements for the reactor trip and bypass breakers were credited or required for compliance with Generic Letter 83-28, Required Actions Based on Generic Implications of Salem ATWS Events.

Design (Reference 1)

- Implementation of automatic actuation of the shunt trip attachment on each reactor trip breaker when a reactor trip signal is generated by the associated train.

- The circuitry used to implement the shunt trip function is Class 1E (safety related) and the design of the circuits is consistent with the Westinghouse Owners Group (WOG) generic design.

- The WOG generic seismic, environmental and life cycle testing of the shunt trip components is applicable to Point Beach. This includes seismic qualification of the shunt trip components in accordance with the provisions of Regulatory Guide 1.100, Revision 1, which endorses IEEE Standard 344.

- Components of the shunt trip circuitry have the ability to perform their intended function up to a voltage of approximately 140 V DC. The voltage source for the undervoltage and shunt trip coils is from station batteries and the battery voltage is maintained less than 135 VDC.
- Field cables for redundant trains of the circuits used to manually initiate the shunt trip attachments are routed in separate raceways between the reactor trip switchgear and the main control board. In the main control board six inches of free air space or an intervening barrier is provided between redundant circuits which provide for manual initiation of the shunt trip attachments of the redundant trip breakers.
- Redundancy of the reactor trip breakers is maintained by using separate Class 1E 125 V DC power sources for the Train A and Train B shunt trips. Cables which are associated with both power supply circuits due to their presence in common enclosures or raceways were analyzed and it was determined that Class 1E circuits are not degraded below an acceptable level. This is in accordance with IEEE 384 and, is therefore, acceptable.
- Installation of bypass breaker position indication on the main control board and interlocking all remote bypass breaker indication with breaker cell switches.

Maintenance (Reference 2 and Reference 3)

- Periodic maintenance, inspection, and lubrication of reactor trip and bypass breakers and associated switchgear is based on the manufacturer's recommendations which include performing maintenance on a refueling outage interval.
- Trip force and breaker response time for UV trip of reactor trip and bypass breakers are recorded and compared to the maximum acceptable values of 31 ounces and 10 cycles respectively. Corrective action is taken if the recorded values are significantly in excess of those normally experienced.
- The UV trip attachment dropout voltage for the reactor trip and bypass breakers is trended as per the manufacturer's recommendations contained in the component instruction manual.
- Reactor trip breaker and bypass breaker insulation is inspected for cracks or other signs of deterioration.

Generic Letter 83-28 requirements for reactor trip and bypass breaker testing are included in Technical Specification 3.3.1, Reactor Protection System (RPS) Instrumentation, except that testing of the bypass breaker shunt trip attachment was removed during the conversion to Improved Technical Specifications.

7.2.3 SYSTEM EVALUATION

The design on the reactor protection system meets that applicable protection system General Design Criteria and IEEE 279-1968 criteria, except where exceptions have been identified in Section 7.2.3.3. The following sections describe specific areas related to these criteria.

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 affecting the DNB ratio are:

Thermal power
Coolant flow
Coolant temperature
Coolant pressure
Core power distribution (hot channel factors)

Figure 7.2-2 illustrates the actual core limits for different pressure ranges, where the DNBR for the hottest fuel rod is the DNB limit. The figure also shows the computed overpower and overtemperature ΔT reactor trips as a function of ΔT, T_{avg} and pressure. Figure 7.2-8 depicts the typical T_{avg}/ΔT control and protection system for each reactor coolant loop.

Variations in both flow and power are monitored by the overpower and overtemperature ΔT trips, because a decrease in flow has the same effect on the measured loop ΔT signal as an increase in power. It is the characteristic of the DNB limits that a reduction in flow of 10% would require a reduction in power of about 5% to maintain the same DNBR, all other variables remaining constant. Therefore, the allowed ΔT increases somewhat at a reduced flow. The trip setpoints are therefore conservatively based on maximum flow. A reduction in flow increases the margin between the trip point and the actual core limit. Periodic measurements using the incore instrumentation system are used to verify that the actual core power distribution is within design limits.

High pressurizer pressure and low pressurizer pressure trips are fixed to limit the pressure range over which core protection depends on the overpower and overtemperature ΔT trips.

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

The reactor protection system actuates a reactor trip on “calculated” overpower ΔT and overtemperature ΔT setpoint based on the hottest fuel rod approaching the DNBR limit. Because of the statistical nature of the DNB correlation and the statistical makeup of a portion of the hot channel factors, there exists a finite probability that a few rods could experience DNB based on the identified hottest fuel rod.

For the anticipated abnormal conditions, it is highly unlikely that the exact combination of conditions (reactor coolant pressure, temperature and core power, instrumentation inaccuracies, etc.) that cause a DNBR equal to the limit will be approached before the reactor trips. The simultaneous loss of power to all of the reactor coolant pumps is the accident condition most likely to approach the DNBR limit for the calculated hottest fuel rod. In any event, the DNBR at the hottest fuel rod is near the limit for only a few seconds.

The hottest fuel rods are not adjacent to one another. They are located near the RCCA guide thimbles. Fuel rods located in the immediate vicinity of the hottest fuel rod have a DNBR higher than that rod.

The ΔT trip functions are based on the differences between measured hot leg and cold leg temperatures. These differences are approximately proportional to core power. Nonlinearities between ΔT and core power due to variations in specific heat are conservatively accounted for.

The overtemperature ΔT trip functions are provided with a neutron flux feedback to reflect a measure of axial power distribution. This assists in preventing an adverse axial distribution which could lead to exceeding the allowable core conditions.

In the event that the difference between the upper and lower power range ion chamber signals exceeds the desired range, automatic feedback signals are provided to reduce the overtemperature trip setpoints, block rod withdrawal and reduce the load to maintain appropriate operating margins for these trip setpoints.

7.2.3.2 Specific Control and Protection Interactions

Some of the control functions derive their signals from the reactor protection system through isolation devices. The isolation devices prevent any failure in the control system from propagating back into the protection system; therefore, no control system failure will adversely affect the protection system.

Certain failures in the protection system could conceivably prevent a particular protection channel from functioning. In addition, the failure could also cause spurious control actions that might require protective action to prevent the resultant spurious control action from exceeding design limits. IEEE 279-1968 Section 4.7 requires analysis for control/protection interactions when protection system variables also provide control signals. The analysis requires that a failure in the protection system that can cause spurious control actions be analyzed in conjunction with a second failure assumed in the protection system. RPS variables that supply control signals were evaluated in WCAP-7306.

a. Power Range Nuclear Flux

Four power range neutron flux channels are provided for overpower protection. Isolated outputs from all four channels are averaged to provide for automatic control rod regulation of power. If any channel fails in such a way as to produce a low output, that channel is incapable of proper overpower protection and may cause a rod withdrawal resulting in overpower. If a second failure is taken for a redundant channel failing to trip on high reactor power, the remaining two-out-of-four overpower trip channels satisfy IEEE 279 Section 4.7 and will ensure an overpower trip, if needed.

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

b. Coolant Temperature

Two hot leg and two cold leg temperature measurements are made for each reactor coolant loop to provide reactor protection. In addition, the use of isolation amplifiers located in the temperature protection channel allow the temperature signals to also be used for reactor control. The temperature measurements, T_{avg} and ΔT, for each loop are used for the overpower and overtemperature ΔT reactor protection, with two channels per loop. The reactor control system uses the highest of the four isolated temperature measurements signal.

In addition, alarms are actuated in the reactor control system if any temperature channel deviates significantly from the others. Automatic rod withdrawal blocks also occur if any one of four nuclear power channels indicates an overpower condition, or if any two-out-of-four temperature channels indicates an overtemperature condition. Two-out-of-four coincidence logic is used to ensure that an overtemperature trip will occur, 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 rate of reactivity insertion.

The hot and cold leg resistance temperature detectors (RTDs) are installed in the 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 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.

Three sampling probes are installed in a cross-sectional plane of each hot leg at approximately 120° intervals. Each sampling probe, which extends several inches into the hot leg coolant stream, contains five inlet orifices distributed along its length. Therefore, a total of fifteen locations in the hot leg stream are sampled to provide a representative reactor coolant temperature. The 2 inch diameter pipe leading to the manifold containing the 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 the 2 inch pipe connecting the probes to the manifold.

The cold leg primary coolant flow is well mixed by the reactor coolant pumps. Therefore, the cold leg sample is taken directly from a 2 inch pipe tap on 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 at high power levels near 100% power. All ΔT setpoints are in terms of the full power ΔT, and thus, accurate ΔT measurements are not required. Linearity of ΔT with power was verified during startup tests.

Reactor protection logic that uses reactor coolant loop temperatures consists of a two-out-of-four trip logic that consists of 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 measurements from detector channels which are separate from those used for reactor protection. Since reactor control is based on the highest average temperature from the two loops, the control rods are always moved based upon the most conservative temperature measurement with respect to DNB margin. A spurious low average

temperature (T_{avg}) signal from any temperature control channel will not result in any control action. A spurious high average temperature signal will cause control rod insertion, which results in reduced reactor power. Two-out-of-four trip logic is used to ensure that an overtemperature trip occurs, if needed, even with an independent failure in another channel; therefore, the reactor coolant temperature measurements meet the requirements of IEEE 279-1968 Section 4.7.

A common low flow alarm with an individual status light for each reactor coolant bypass loop is provided on the main control board. The alarm and status lights provide the operator with immediate indication of a low flow condition in the bypass loops associated with either reactor coolant 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 is monitored:

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

The time delays associated with the temperature measurements used for reactor protection include RTD bypass loop fluid transport delay effect, bypass loop piping thermal capacity, RTD time response, and trip circuit channel electronics delay. The total time delay is measured from the time the temperature difference in the coolant loops exceeds the trip setpoint until the rods are free to fall.

Functional demonstration testing of the RTDs installed in the bypass lines in the Point Beach Nuclear Plant were conducted. The tests included both the incore thermocouple/RTD intercalibrations and load swing tests. Flow through the manifolds was checked and balanced. Consistency of the readings from the RTDs in the loops as well as reproducibility of the readings during power operation were checked. The load swing test demonstrated the response times were higher than the 2.3 seconds used in the accident analysis, which could have resulted in a reduction in DNBR to less than the 1.3 minimum ratio allowed by the accident analyses during a rod withdrawal accident at full power operation.

As a result of the testing, the lead time values used to calculate the overtemperature ΔT and overpower ΔT setpoints were increased to compensate for the slower than expected response times of the RTD bypass loops. The overtemperature and overpower ΔT instrumentation were adjusted for the more conservative settings prior to full power operation. This ensures that the reactor protection instrumentation will maintain the plant within the limits described in the accident analysis, Section 14.1. The values for the overtemperature ΔT and overpower ΔT setpoints are listed in the Technical Specifications.

c. Pressurizer Pressure

Four pressure channels are used for low pressure protection and as part of overtemperature protection. Three of the four pressure channels are used for high pressure protection. Isolated output signals from these channels also are used to control pressurizer spray, power-operated relief valves, and pressurizer heaters. (See Figure 7.2-10)

1. Low Pressure

   A spurious high pressure signal can cause low pressure by actuating the spray valves. Low pressure caused by spurious opening of a PORV is prevented by a two-out-of-two high pressure actuation logic. If a second failure is taken for a redundant pressure channel failing to trip on de-pressurization caused by the inadvertent spray valve actuation, the remaining two-out-of-four low pressure channels satisfy IEEE 279 Section 4.7 and ensures a reactor trip, if needed.

2. High Pressure

   The pressurizer heaters are incapable of overpressurizing the reactor coolant system. Maximum steam generation rate with heaters is about 8,200 lbs/hr, compared with a total relieving capacity of 576,000 lbs/hr for the two safety valves and a total relieving capacity of 358,000 lbs/hr for the two pressurizer power-operated relief valves. Therefore, overpressure protection is not required for a pressure control failure that could cause the heaters to energize. Two-out-of-three high pressure trip logic is therefore 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 pressure alarms are available which provide ample time for operator action.

d. Pressurizer Level

   Three pressurizer level channels are used for high level reactor protection. Isolated output signals from these channels are used for volume control, increasing or decreasing water level. A level control failure could fill or empty the pressurizer at a slow rate (on the order of half an hour or more). (See Figure 7.2-11)

1. High Level

   A reactor trip on pressurizer high level is provided to prevent rapid thermal expansions of reactor coolant fluid from filling the pressurizer. The rapid change from high rates of steam relief to water relief can be damaging to the safety valves, the relief piping and pressure relief tank. A level control failure cannot actuate the safety valves because the high pressure reactor trip setpoint is below the safety valve setpoint. With the slow rate of charging available, the pressure overshoot before the high pressure reactor trip is much smaller than the difference between high pressure reactor trip and safety valve set pressure. Therefore, a control failure does not require protection system action.

   In addition, alarms are available and ample time exists for operator action.

2. Low Level

   For control failures which tend to empty the pressurizer, low level alarms provide ample time for operator action.

e. Steam Generator Water Level and Feedwater Flow

The basic function of the reactor protection trips 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 (See Figure 7.2-12). Should a complete loss of feedwater occur with no reactor protection action, the steam generators would boil dry and cause an overtemperature/overpressure excursion of the reactor coolant.

Reactor trips on temperature, pressure, and pressurizer water level will trip the plant before there is any damage to the core or reactor coolant system. However, the residual heat remaining after a trip would cause thermal expansion and discharge of the reactor coolant to containment through the pressurizer relief valves and pressurizer relief tank.

Redundant auxiliary feedwater pumps are provided to prevent the loss of steam generator inventory. Reactor trips act before the steam generators are dry, to reduce the required capacity and starting time requirements for the auxiliary feedwater pumps and minimize the thermal transient on the reactor coolant system and steam generators. Independent trip circuits are provided for each steam generator for the following reasons:

- Should severe mechanical damage (e.g., feedwater line break, etc.) occur to the feedwater line to one steam generator, it is difficult to ensure the functional integrity of the level and flow instrumentation for that steam generator.
- 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 would affect only one steam generator and would not impair the capability of the main feedwater system under either manual control or automatic control. The control and protection interactions associated with the steam generator and feedwater flow are as follows:

1. 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, ensures a reactor trip, if needed.

2. Steam Flow

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

3. Steam Generator Level

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

- 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.
- 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 a reactor trip on two-out-of-three low-low level is acceptable.

Refer to Section 7.3.3 for a further discussion on control/protection interaction for the feedwater isolation function.

7.2.3.3 Specific Exceptions to IEEE 279-1968

a. Low Pressurizer Pressure Protection

Two of the four low pressurizer pressure transmitters share a common sensing line. There are two failure mechanisms that may be expected with a instrument sensing line:

- Broken line, and
- Blocked line

A broken sensing line would result in a reactor trip due to the two-out-of-four transmitters providing a low pressurizer pressure signal. Therefore, the failure of the sensing line would result in a reactor trip, and would not prevent the reactor protection system from meeting the assumptions in the accident analysis.

A blocked sensing line could result from a closed isolation valve. If the blocked line occurred on the shared sensing line, this could prevent the low pressurizer pressure trip from actuating when considered with a single active failure of another pressurizer pressure transmitter channel failing high. However, administrative procedures exist to ensure that the transmitter's valves are returned to correct position after calibration or maintenance. In addition, the failure of the transmitters to track the remaining redundant instrumentation during plant startup or operation would be identified. Therefore, the closure of an isolation valve is not considered a credible failure mechanism associated with the shared sensing line.

Based on the design of the protection system, its inability to withstand a pinched sensing line concurrent with a single active failure demonstrates that pinching of sensing lines due to accident effects was not considered as part of the original design for Point Beach; therefore, the pinching of the shared sensing line is not considered a credible failure mechanism.

Thus, no credible failure of the shared sensing line associated with the low pressurizer pressure trip will prevent the reactor protection system from tripping the reactor.

b. Coolant Flow

1. Measured Low Coolant Flow in Reactor Coolant Piping

   Three flow channels are used for the low reactor coolant flow reactor protection. The reactor coolant flow is determined by transmitters that measure the differential pressure (ΔP) associated with the elbow flow taps described in Section 4.2. The flow transmitters share a common high pressure sensing line, while the low pressure sensing lines are independent for each transmitter. There are two failure mechanisms that may be expected with an instrument sensing line:

- Broken line, and
- Blocked line

A broken high pressure sensing line would result in a reactor trip due to the three flow transmitters providing a low flow signal. Therefore, the failure of the sensing line would result in a reactor trip, and would not prevent the reactor protection system from meeting the assumptions in the accident analysis.

A blocked high pressure sensing line could result from a closed isolation valve. This could result in degraded performance of the low reactor coolant flow pressure trip. However, administrative procedures exist to ensure that the transmitter's valves are returned to the correct position after calibration or maintenance. In addition, the failure of the flow transmitters on one loop to track the flow instrumentation on the other loop during plant startup would be identified. Therefore, a blocked high pressure sensing line is not considered a credible failure mode associated with the shared sensing line.

Based on the design of the protection system, its inability to withstand a pinched sensing line concurrent with a single active failure demonstrates that pinching of sensing lines due to accident effects was not considered as part of the original design for Point Beach; therefore, the pinching of the shared sensing line is not considered a credible failure mechanism.

Thus, no credible failure of the shared sensing line associated with the low reactor coolant flow trip will prevent the reactor protection system from tripping the reactor.

2. Monitored Breaker Position to the Reactor Coolant Pumps

The reactor is tripped when either one-out-of-two reactor coolant pump breakers are open (tripped) above approximately 50% power and when two-out-of-two reactor coolant pump breakers are open below approximately 50% power. Some of the components in the reactor coolant pump breaker trip circuit are non-safety related, non-seismically qualified. In addition, the trip below approximately 50% power requires a two-out-of-two trip logic, which is not single failure proof.

The reactor trip on reactor coolant pump breaker position is considered an anticipatory (backup) trip for a complete loss of flow event and no credit is taken for the trip in the accident analysis. No failure associated with reactor coolant pump breakers will prevent the reactor protection system from tripping the reactor, although the failure could initiate a reactor trip via one or both reactor trip trains.

c. Turbine Trip

The reactor is tripped when either two-out-of-two turbine stop valves close or when two-out-of-three pressure switches indicate low turbine auto stop oil pressure. The position indication and oil pressure indication are initiated by non-safety related, non-seismic instrumentation whose circuits are not physically separated in accordance with IEEE 279. In addition, the circulating water pump operating status and the condenser vacuum status inputs to the P-9 permissive, which blocks the reactor trip on turbine trip as discussed in Section 7.2.2.2.l, are non-safety related, non-seismically qualified. Also, the stop valve position trip and the automatic removal of the P-9 permissive on loss of circulating water pumps relies on two-out-of-two logic, which is not single failure proof.

The reactor trip on turbine trip is considered an anticipatory trip and no credit is taken for this trip in any of the accident analyses. These trips consist of contacts connected to the train logic relays. No failure associated with the instrumentation, shared circuit routing or trip logic will prevent the reactor protection system from tripping the reactor, although the failures could initiate a reactor trip via one or both reactor trip trains. In addition, since these circuits do not provide input to the analog channel logic, no failure associated with these trips will adversely affect any primary reactor trip channel.

The failure of the inputs could prevent the P-9 permissive from energizing below its setpoint, which could result in a reactor trip. No failure associated with the P-9 permissive will prevent the reactor protection system from functioning. Therefore, the failure of the permissive is "fail-safe."

d. Steam/Feedwater Flow Mismatch Trip

The feedwater flow transmitters for Unit 1 and Unit 2 FT-466, FT-467, FT-476, and FT-477 are Seismic Class 3. These transmitters provide input to the reactor protective scheme to provide a reactor trip upon Steam Flow/Feed Flow mismatch coincident with a Low Steam Generator Water Level. Since the feed flow transmitters are not seismically qualified, they may not perform their functions during and after a seismic event as depicted in FSAR Section 7.2.3.4.

The reactor trip on Steam/Feedwater Flow Mismatch coincident with a Steam Generator Water Level Low condition is considered an anticipatory backup trip for a Loss of Normal Feedwater Event and is described as such in FSAR Section 7.2.3.2e and no credit is taken for the trip in the accident analysis. No failure associated with the feedwater flow transmitters will prevent other portions of the reactor protection system from tripping the reactor.

7.2.3.4 Seismic Qualification of Protection System Equipment

NOTE: The following describes the original method used to seismically evaluate reactor protection system equipment. Additional verification of the seismic adequacy of plant mechanical and electrical equipment was performed as discussed in Section A.5.6, "Verification of Seismic Adequacy of Equipment per Generic Letter 87-02."

Documentation of the seismic test program for protection system components is contained in Westinghouse WCAP-7397-L, "Topical Report Seismic Testing of Electrical and Control Equipment" dated January 1970, which summarizes the results as follows:

In a nuclear power plant, electrical and control equipment which initiates reactor trips, actuates safeguards systems, and/or monitors radioactive releases from the plant must be capable of performing their functions during and after an earthquake that has occurred at the plant site. To demonstrate the ability of this equipment to perform under earthquake conditions, selected types of this essential equipment representative of all protection and safeguards circuits and equipment were subjected to vibration tests which simulated the seismic conditions for the "low seismic" class of plants. During the tests, equipment operation was monitored to prove proper performance of function. The results show that there were no electrical malfunctions. Based on these results, it is concluded that the equipment will perform their design functions during, as well as following, a "low seismic" earthquake.

To apply WCAP-7397-L to the Point Beach design, the locations of the protection systems equipment were identified. Dynamic analysis of the buildings for the plant design basis

earthquake shows that the horizontal and vertical accelerations of the buildings floors where the equipment is located are within the specific low seismic test envelope given in WCAP-7397-L, Figure B-2.

The protection or safeguard instrumentation systems are qualified to withstand a seismic event as follows:

A protection or safeguard signal is initiated by an instrument or transmitter, which has been demonstrated to withstand the seismic forces as identified in Section 4.8 of WCAP-7397-L.

The signal is carried by circuits installed in conduit and cable trays, which have been designed to withstand seismic forces. Appropriate supports have been added to typical configurations to withstand the accelerations determined for the building and elevation through which the circuit is routed.

The signal continues to the process control racks, which have been demonstrated to withstand the seismic forces as identified in Section 4.2 of WCAP-7397-L.

Then the signal proceeds to the actuation racks, which have been demonstrated to withstand the seismic forces as identified in Section 4.3 of WCAP-7397-L.

The actuation signal proceeds through a switch on the main control board to the appropriate switchgear (refer to Section 8.0 for switchgear discussion). The main control boards were specified to "be designed such that the maximum stresses, including simultaneous seismic accelerations of 5.2g in the horizontal and vertical directions, shall not dislodge or cause relative movement between components such as to impair the functional integrity of circuits or equipment." This acceleration exceeds that calculation as input to the boards from the floor of the main control room. In shipment, boards of this manufacturer and construction have recorded shocks of 8-10g and, when wired, the switches have operated without repair.

7.2.3.5 Environmental Qualification of Reactor Protection System Equipment

The reactor protection equipment that is located in a mild environment (e.g., an environment that would, at no time, be more severe that the normal service environment, such as the control room or cable spreading room) is not required to be environmentally qualified in accordance with 10 CFR 50.49. However, the design for normal service conditions and the PBNP quality assurance, maintenance, and surveillance programs ensure that the equipment is capable of performing its safety function on demand throughout its installed life.

The reactor protection equipment that is located in a potentially harsh environment, such as sensors inside containment, has to be environmentally qualified in accordance with 10 CFR 50.49 for reactor trip protection only if:

1. The equipment is the primary reactor trip assumed in the accident analysis for the accident that creates the harsh environment, and
2. The harsh environment degrades the equipment performance prior to initiating the reactor trip.

Therefore, if the equipment can be shown to not meet the above two requirements, the equipment does not need to be qualified from a reactor protection system standpoint. However, if the equipment is not required to be environmentally qualified for a reactor protection function, it may require qualification if it is used to provide post-accident monitoring.

a. Normal Operating Environment

A normal operating environment of ≤75°F is maintained in the control room. Protection equipment inside the control room is designed to operate within design tolerance over this temperature range and will perform its protection function in an ambient temperature of 110°F (e.g., there will be no loss of function in an ambient temperature of 110°F).

The operating environment for equipment within containment is normally controlled to less than 105°F. The reactor protection system instrumentation within containment is designed for continuous operation. The temperature of the out-of-core neutron detectors is maintained at or below 135°F by the reactor cavity air cooling system. The detectors are designed for continuous operation of 135°F and will withstand operation at 175°F for short durations.

Typical test data (or reasonable engineering extrapolation based on test data) is used to verify that protection system's equipment meet, on a continuing basis, the functional requirements under the anticipated normal ambient conditions.

Table 7.2-3 provides information about the process instrumentation used to provide signals to the reactor protection system.

7.2.3.6 Methodology for Determination of RPS/ESFAS Setpoint Values (Reference 5)

The methodology for determining RPS/ESFAS protection system setpoints follows the guidance of PBNP Design Guide DG-I01, Instrument Setpoint Methodology. Applying the methodology, setpoint calculations are prepared to: 1) identify an analytical limit (AL) or process limit (PL) for the setpoint, 2) quantify the Total Loop Error (TLE) for the setpoint instrument string, 3) determine the Limiting Trip Setpoint (LTSP) and Allowable Value (AV), 4) select the Nominal Trip Setpoint (NTSP), and 5) determine as-left and as-found tolerances for the NTSP.

The calculated values are determined such that there is a 95% probability and 95% confidence level that the instrument channel will trip prior to the process variable exceeding the established AL or PL.

a. Setpoint Determination

Analytical Limits are the process limits at which protective actions are assumed to occur in plant accident analyses. The setpoint must be chosen such that protective action occurs at or prior to reaching the Analytical Limit, to assure that any associated analysis Safety Limit is protected. For backup, anticipatory, interlock or permissive functions that lack an AL, a process limit or nominal setpoint value may be used instead.

Total Loop Error is the combination of random (±) and non-random (bias) errors for the instrument string that provides the process signal to the trip bistable. Random errors are combined using the square root sum of squares (SRSS) method and bias terms are included algebraically to arrive at the TLE.

The Limiting Trip Setpoint is calculated by subtracting TLE from the Analytical Limit (or PL), for variables that increase toward the limit. For variables that decrease toward the limit, the TLE is added to the Analytical Limit or PL. The LTSP represents the limiting value that the field setpoint can have and still protect the AL or PL, assuming worst case 95/95 instrument uncertainty. The LTSP results may be rounded in a conservative direction to arrive at the Allowable Values that are published in the RPS/ESFAS Technical Specifications.

For trip and actuation functions (excluding interlocks and permissives), the NTSP (the actual field setpoint in calibration procedures) is chosen to be conservative to the LTSP and the AV. For interlocks and permissives, the NTSP is a nominal value assumed in the analysis. The NTSP values are published in the RPS/ESFAS Technical Specifications.

b. As-Left and As-Found Tolerances

As-left and as-found tolerances permitted during instrument calibration are symmetric values applied on each side of the NTSP. The NTSP is identified in the calibration procedures as the "ideal" setpoint value.

The methodology used to determine as-left and as-found tolerances in calibration procedures that accomplish RPS and ESFAS channel surveillance testing is described below. This methodology must be specified in FSAR Section 7.2 per notes in RPS and ESFAS Technical Specification Tables 3.3.1-1 and 3.3.2-1 issued for implementation of automatic AFW Pump suction transfer and power uprate to 1800 MWt.

1. As-Left Tolerances

   As-left setting tolerances are applied to calibration settings for RPS/ESFAS components such as bistables, signal conditioning modules, and sensors that perform protective functions. A component's as-left tolerance is determined in an associated uncertainty/ setpoint calculation for the plant variable measured by the channel. The as-left tolerance is typically based on the reference accuracy of the component being calibrated. In some cases, the as-left tolerance may be a historically-chosen value based on limitations in adjusting the module and instrument performance. In those cases where the as-left tolerance is a historically-chosen value, the calculation provides a basis for using the historical value as the source for the setting tolerance, rather than using the component's reference accuracy.

   If a single component (e.g., a bistable) is calibrated alone, the as left tolerance is typically the reference accuracy for the module. When a group of components are calibrated together (in a string calibration), the as-left tolerance is the square-root-sum-of-the-squares (SRSS) combination of the individual setting tolerances of components in the calibration string.

2. As-Found Tolerances

   As-found setting tolerances (AF) are determined by calculation and are used during calibration to evaluate if a setting or output of a component or string of components is either behaving normally or has drifted excessively over the preceding calibration interval. The as-found tolerance accounts for the as-left tolerance plus the maximum 2σ drift expected to occur over the calibration interval when the component is behaving normally. As such, the AF is slightly larger than the as-left tolerance, and is also symmetric around the ideal setting or NTSP. As-found tolerances are determined as follows:

- If the expected component drift over the calibration interval is derived statistically from as-left/as-found data, the acceptable as-found tolerance can be calculated as the SRSS of the as-left setting tolerance (Rv) and the 2σ rack drift (Rd), as follows:

$$AF = \pm [Rv^2 + Rd^2]^{1/2}$$

- If the rack drift is not derived from actual as-left/as-found data, the acceptable as-found tolerance can be calculated as the SRSS of the as-left setting tolerance (Rv), predicted 2σ rack drift (Rd), and M&TE uncertainty (Rm), as follows:

$$AF = \pm [Rv^2 + Rd^2 + Rm^2]^{1/2}$$

By incorporating a 2σ drift value into the AF term, AF is a reasonable limit for evaluating that an individual module or a string of modules is behaving normally over the calibration interval. If the AF limit is exceeded when the as-found setting is measured, the excessive drift may be within 95/95 statistical probability, or the drift may indicate that the equipment is behaving erratically. An evaluation of an out-of-tolerance condition may include a review of calibration history and the drift magnitude as compared to predicted drift, to assess if the component is behaving within expected limits or is degrading such that repair or replacement may be necessary.

7.2.4 REFERENCES

1. NRC SE, "Wisconsin Electric Power Company, Point Beach Nuclear Plant Units 1 & 2, Generic Letter 83-28, Item 4.3, Reactor Trip Breaker Automatic Shunt Trip," dated September 26, 1984.

2. NRC SE, "Wisconsin Electric Power Company, Point Beach Nuclear Plant Units 1 and 2, Reactor Trip System Reliability, Items 4.2.1 and 4.2.2 of Generic Letter 83-28," dated May 16, 1985.

3. Commitment Change Evaluation CCE 98-001, dated September 24, 1998, for increase in preventive maintenance interval for reactor trip and bypass breakers.

4. NRC SE, Point Beach Nuclear Plant Units 1 and 2, "Issuance of License Amendments Regarding Extended Power Uprate," dated May 3, 2011.

5. NRC SE, Point Beach Nuclear Plant Units 1 and 2, "Issuance of License Amendments Regarding Revision of Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS) Setpoints," dated March 25, 2011.

Table 7.2-1 LIST OF REACTOR TRIPS

	REACTOR TRIP	COINCIDENCE CIRCUITRY AND INTERLOCKS	COMMENTS
1.	Manual	1/2, no interlocks.	
2a.	Power Range Nuclear Flux, High	2/4, no interlocks.	
2b.	Power Range Nuclear Flux, Low	2/4, manual block permitted by P-10.	Automatic unblock of low setting by P-10.
3.	Overtemperature ΔT	2/4, no interlocks.	
4.	Overpower ΔT	2/4, no interlocks.	
5.	Low Pressurizer Pressure	2/4, interlocked with P-7.	
6.	High Pressurizer Pressure	2/3, no interlocks.	
7.	High Pressurizer Water Level	2/3, interlocked with P-7.	
8a.	Low Reactor Coolant flow	2/3, per loop interlocked with P-8 or 2/3 both loops interlocked with P-7.	Both loops blocked below P-7. Single loop blocked below P-8.
8b.	RCP breakers only	1/1 per loop, interlocked with P-8 or 1/1 both loops interlocked with P-7.	
8b1.	RCP breaker trip, underfrequency	1/2 per bus on both buses, no interlocks.	Trips both RCPs.
8b2.	RCP breaker trip, undervoltage	2/2 per bus, no interlocks, approximately 5 second time delay.	Trips RCP on affected bus only.
8b3.	RCP breaker trip, A01 or A02 bus fault	1/1 per bus, no interlocks.	Trips RCP on affected bus only.
8c.	Undervoltage on A01 or A02	1/2 per bus interlocked with P-7.	
9.	Safety Injection Signal (Actuation)	1/2 manual, 2/3 low pressurizer, 2/3 high containment pressure, or 2/3 low steam line pressure (either loop).	Low pressurizer pressure and low steam line pressure SI signals may be manually blocked with RCS pressure below SI block setpoint, automatically unblocked above the setpoint.
10.	Turbine-Generator Trip	2/3 low auto stop oil pressure or 2/2 stop valve closure indication both interlocked with P-7 and P-9.	
11.	Steam/Feedwater Flow Mismatch	1/2, steam/feedwater flow mismatch (steam flow > feed flow) in coincidence with 1/2, low steam generator water level, per loop.	
12.	Low-Low Steam Generator Water Level	2/3, per loop.	
13.	Intermediate Range Nuclear Flux	1/2, manual block permitted by P-10.	Automatic unblock by P-10.
14.	Source Range Nuclear Flux	1/2, manual block permitted by P-6, interlocked with P-10.	Automatic unblock by P-10.

Table 7.2-2 INTERLOCK CIRCUITS

Interlock Number	Function	Required Input
P-1	Prevent rod withdrawal on overpower	1/4 high neutron flux (power range); or 1/2 high neutron flux (intermediate range); or 2/4 overtemperature ΔT; or 2/4 overpower ΔT.
P-2	Auto-rod withdrawal stop at low powers	Low MWe (15% power) load signal (turbine pressure)
P-5	Steam dump interlocks	Rapid decrease of MWe load signal (turbine pressure)
P-6	Manual block of source range trip	1/2 high intermediate range flux allows manual block, 2/2 low intermediate range defeats block
P-7	Block various trips at low power	3/4 low-low neutron flux (power range) and 2/2 low MWe load signal (turbine pressure)
P-8	Block single primary loop loss of low trip	3/4 low neutron flux (power range)
P-9	Block reactor trip following turbine trip	3/4 low neutron flux (power range) and low condenser pressure (2/2) and circulating water pump (1/2)
P-10	Manual block of power range trip (low setpoint); manual block of intermediate range trip; and automatic block of source range trip	2/4 high neutron flux allows manual block, 3/4 low neutron flux (power range) defeats manual block.

Table 7.2-3 RPS/ESFAS PRIMARY AND SECONDARY INSTRUMENTATION

Parameter	Transmitter/Sensor	Readout*	Power	Prot/Safeguards Use	Taps
Reactor Coolant temperature	4 RTD's/loop plus spares	C.B. Meter	Ext.	ΔT trips, T_{ave} Interlock	1 each
Pressurizer Pressure	4 transmitters	C.B. Meter	Ext.	Hi/low pressure trips, SIS(3)	3 (shared with level); one common for two transmitters
Pressurizer Level	3 DP transmitters	C.B. Meter	Ext.	Hi level trip	One pair each (shared with pressure)
Steam Flow	2 DP transmitters/loop	C.B. Meters	Ext.	Mismatch trip, steamline isolation	1 pair each
Feedwater Flow	2 DP transmitters/loop	C.B. Meter	Ext.	Mismatch trip	1 pair each
Steam Pressure	3 transmitters/loop	C.B. Meter	Ext.	SIS	1 each
Steam Generator Level	3 DP transmitters/SG	C.B. Meter	Ext.	Lo level coincidence with mismatch trip , Lo-Lo level trip, AFW actuation	3 pairs each S/G
Reactor Coolant Flow	3 DP transmitters/loop	C.B. Meter	Ext.	Low flow trip	1 common high pressure/loop; 1 each low pressure/loop
Containment Pressure	6 transmitters	C.B. Meter	Ext.	SIS (3); Spray (3+3), steamline isolation (3)	3 shared
Turbine 1st Stage Pressure	2 transmitters	Blind	Ext.	Rod control and PZR level control programs and turbine power permissives	1 each

*C.B. is Control Board

Figure 7.2-1 REACTOR CORE SAFETY LIMITS

See TRM Section 2.1, Core Operating Limits Report (COLR)

Figure 7.2-2 TYPICAL ILLUSTRATION OF HIGH ΔT TRIP (ΔT vs. T_{AVG})

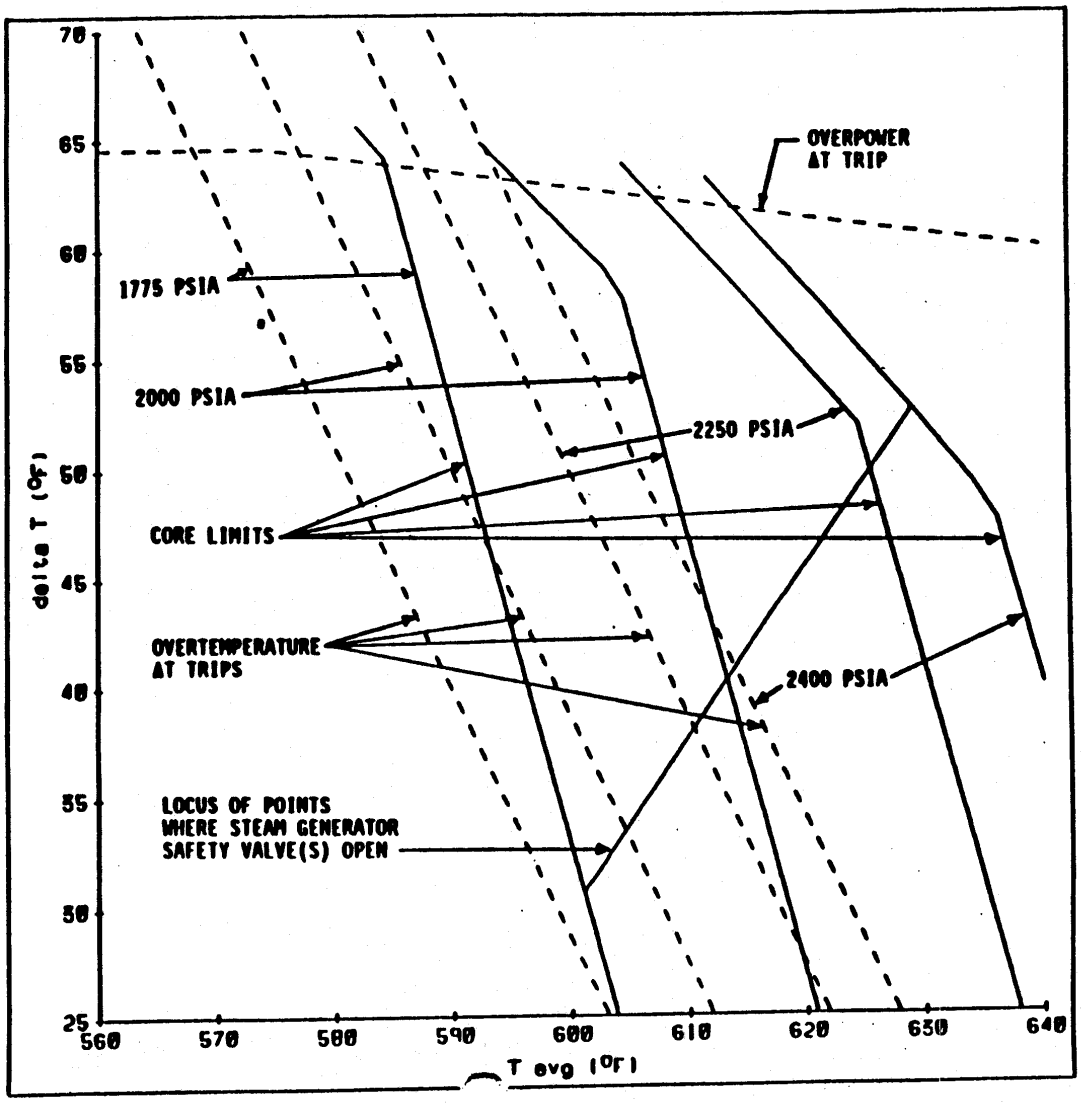


Figure 7.2-3 REACTOR PROTECTION SYSTEMS

Figure 7.2-4 DESIGN TO ACHIEVE ISOLATION BETWEEN CHANNELS

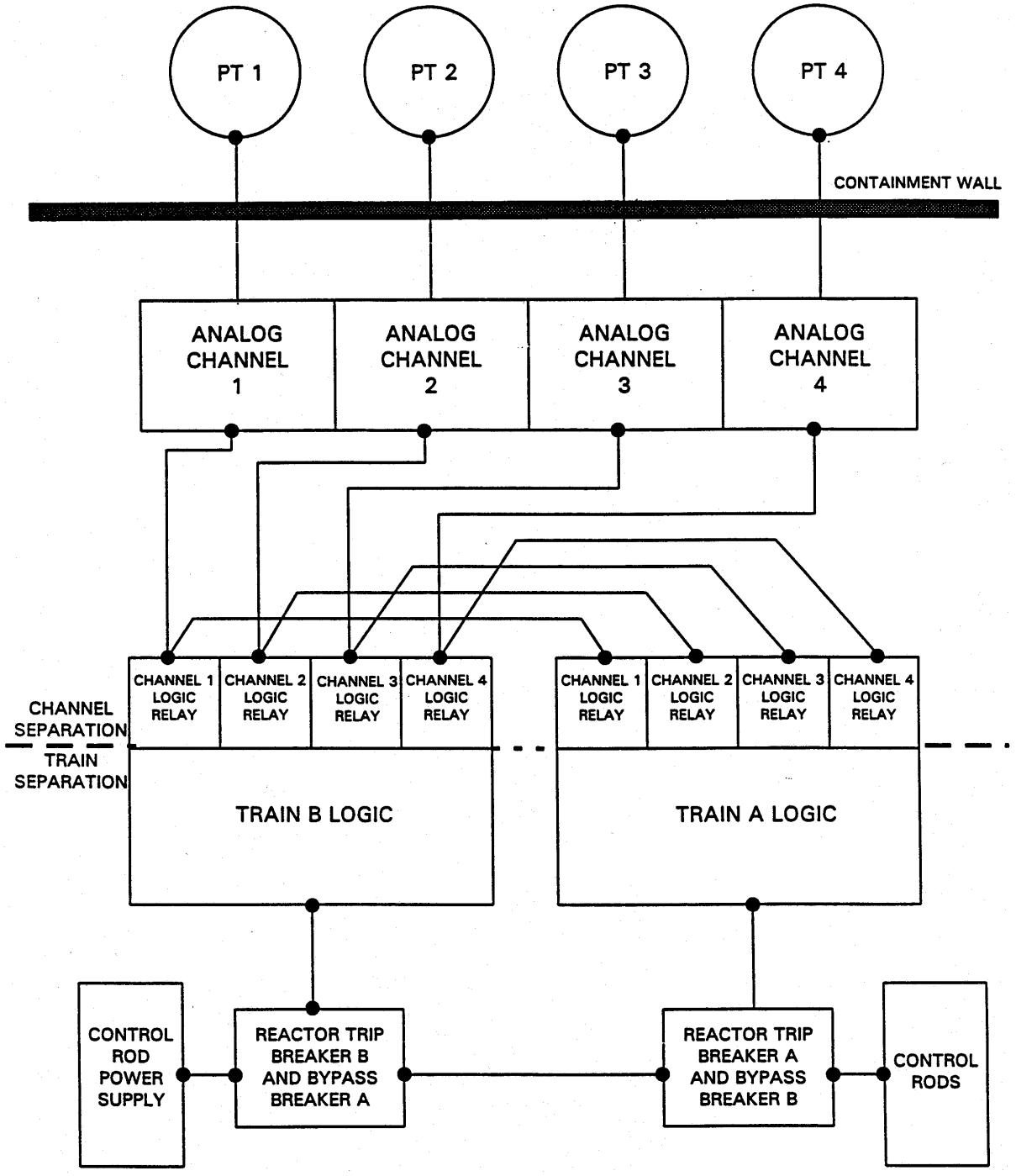


Figure 7.2-5 BASIC ELEMENTS OF AN ANALOG CHANNEL

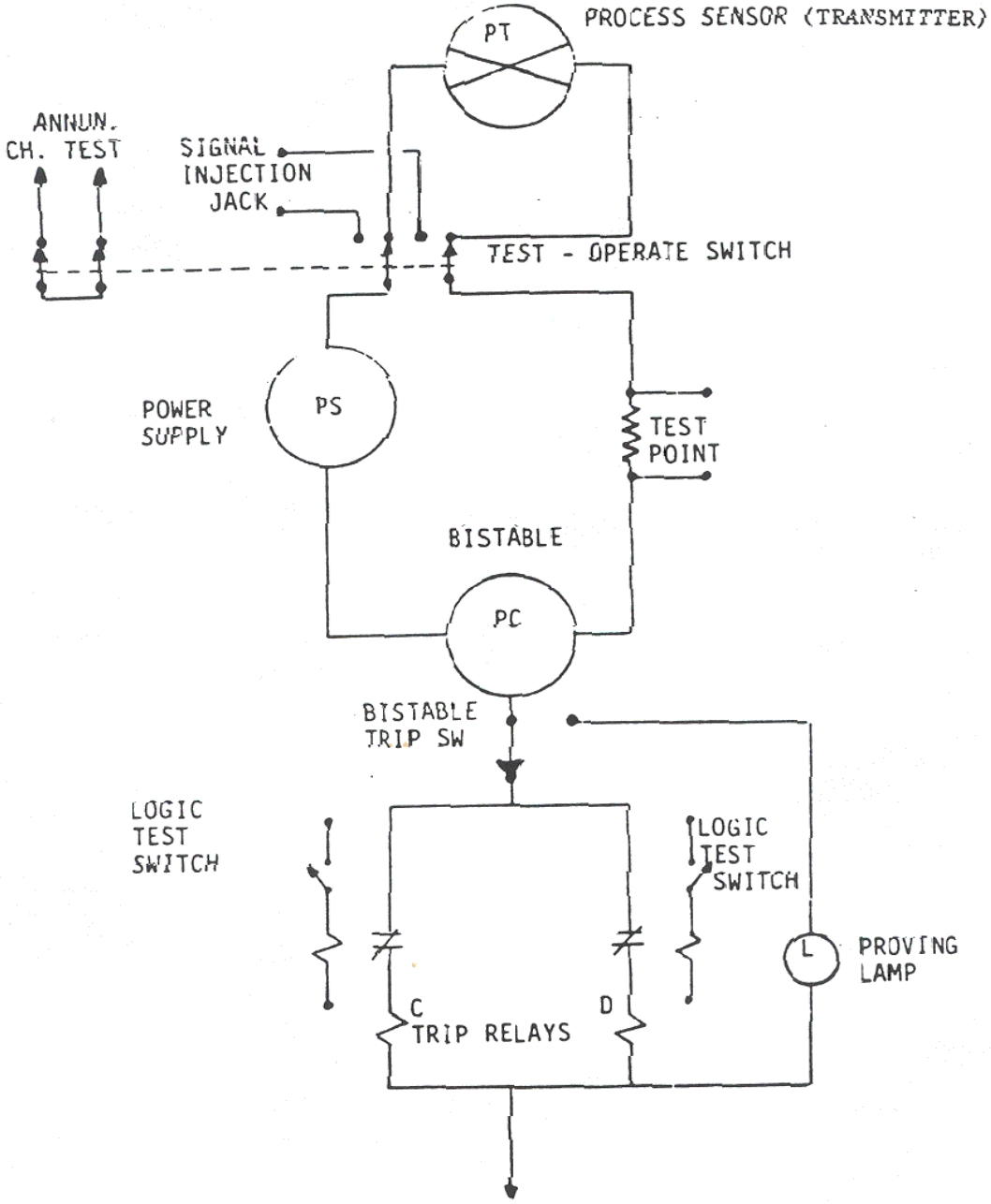


Figure 7.2-6 SIMPLIFIED TRIP LOGIC TRAINS

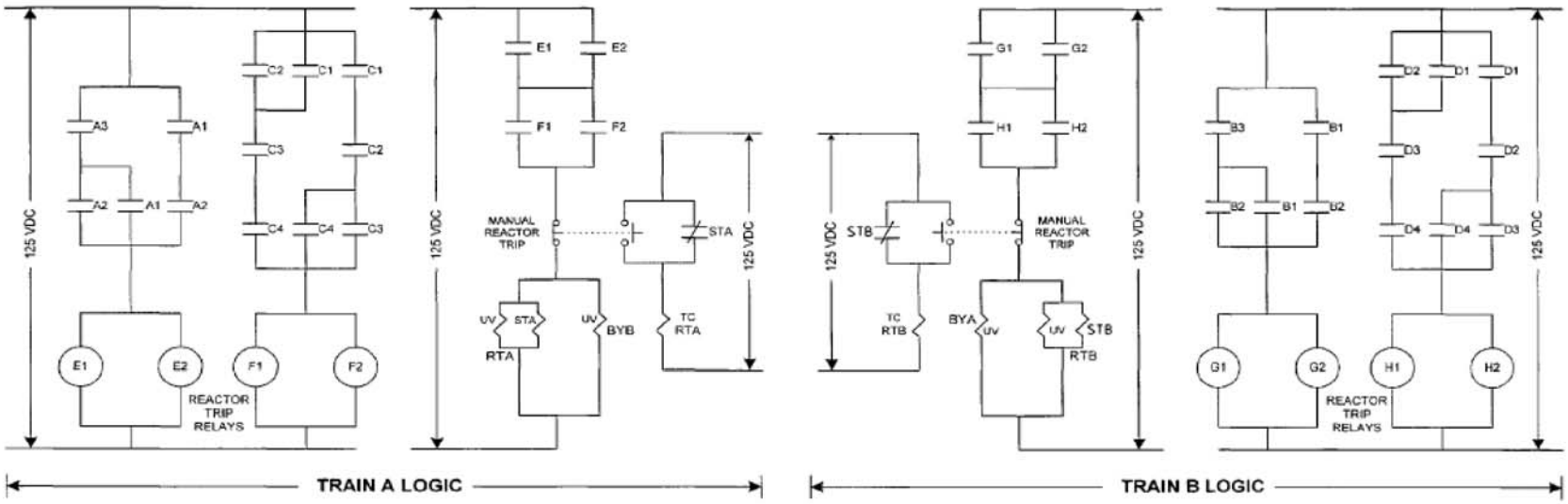
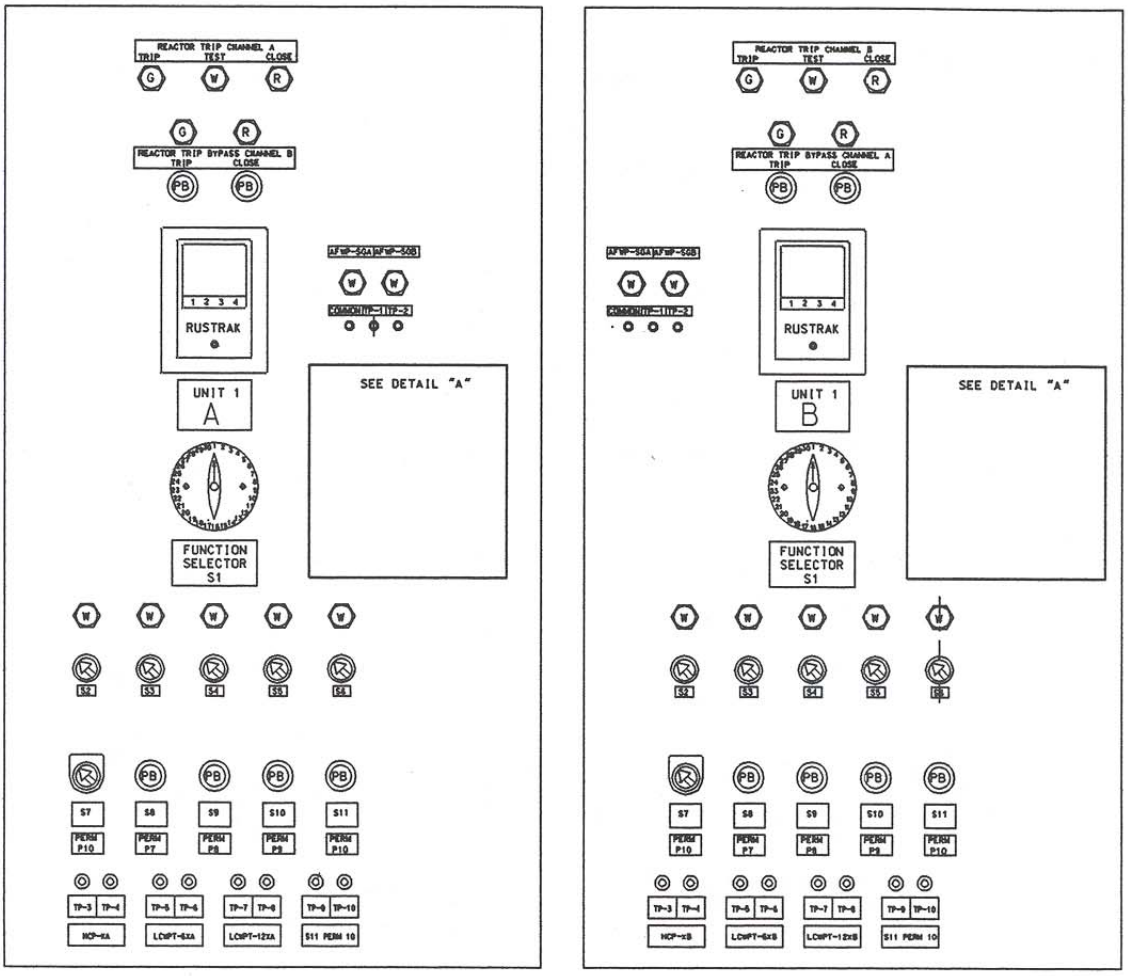
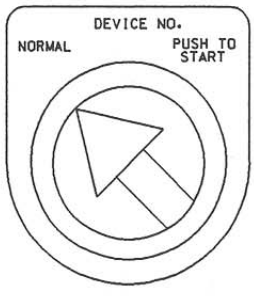


Figure 7.2-7 LOGIC CHANNEL TEST PANELS (UNIT 1)



DETAIL "A"

S1 SELECTOR SWITCH		TEST BUTTON				
POS.	FUNCTION	S2	S3	S4	S5	S6
1	NI-FLUX-SOURCE RANGE	1NC31D	1NC32D	1-1/N33A	1-1/N31B	1-1/N32B
2	NI-FLUX-INTERMEDIATE RANGE	1NC36F	1NC36F	1-1/N38A	1-1/N36A	1-1/N34A
3	POWER RANGE-NI-FLUX-LO TRIP	1NC41P	1NC42P	1NC43P	1NC44P	1-1/N47A
4	NUCLEAR PWR., @ X%	1NC41M	1NC42M	1NC43M	1NC44M	
5	INTERMEDIATE RANGE-P6	1NC35D	1NC36D	1-1/N39A	1-1/N39B	
6	PRESSURIZER LOW PRESSURE	1PC429E	1PC430H	1PC431J	1PC449A	
7	OVERTEMPERATURE ΔT	1TC406C	1TC406C	1TC407C	1TC408C	
8	OVERPOWER ΔT	1TC408A	1TC408A	1TC407A	1TC408A	
9	LOW STM. GEN. FDW. FLOW/LEVEL	1FC466C	1FC467B	1LC462C	1LC463E	
10	LOW STM. GEN. FDW. FLOW/LEVEL	1LC472C	1LC473E	1FC476C	1FC477B	
11	POWER RANGE-HI FLUX-HI TRIP	1NC41R	1NC42R	1NC43R	1NC44R	
12	NUCLEAR POWER @2%	1NC41S	1NC42S	1NC43S	1NC44S	
13	NUCLEAR POWER @Y%	1NC41N	1NC42N	1NC43N	1NC44N	
14	4160 V BUS VOLTAGE	1-27J/A01	1-27J/A01	1-27J/A02	1-27J/A02	
15	PRESSURIZER HI WATER LEVEL	1LC426A	1LC427A	1LC426A		
16	REACTOR COOLANT FLOW	1FC411	1FC412	1FC413		
17	REACTOR COOLANT FLOW	1FC414	1FC415	1FC416		
18	PRESSURIZER HI PRESSURE	1PC429A	1PC430A	1PC431A		
19	TURBINE AUTO STOP	1-63/AST3	1-63/AST4	1-63/AST5		
20	LO LO STM. GEN. WATER LEVEL	1LC461B	1LC462A	1LC463C		
21	LO LO STM. GEN. WATER LEVEL	1LC472A	1LC473C	1LC471B		
22	LOSS OF CIRC. WATER PUMPS	1A52-06	1A52-12			
23	REACTOR COOLANT-LOSS OF PWR.	1RCPA	1RCPB			
24	CLOSE STOP VALVES-TURBINE	1-33AC-SL	1-33AC-SR			
25	TURBINE POWER @X%	1PC469A	1PC469A			
26	SAFETY INJECTION	1S111X-A	1S121X-B			
27	HIGH CONDENSER PRESSURE	1PC484A				
28						
29						
30						



TYPICAL LEGEND PLATE MARKINGS

CGS fig7_2_7.DGN

FIG. 7.2-7
UNIT 1
JUNE 1999

Figure 7.2-8 $T_{AVG}/\Delta T$ CONTROL AND PROTECTION SYSTEM

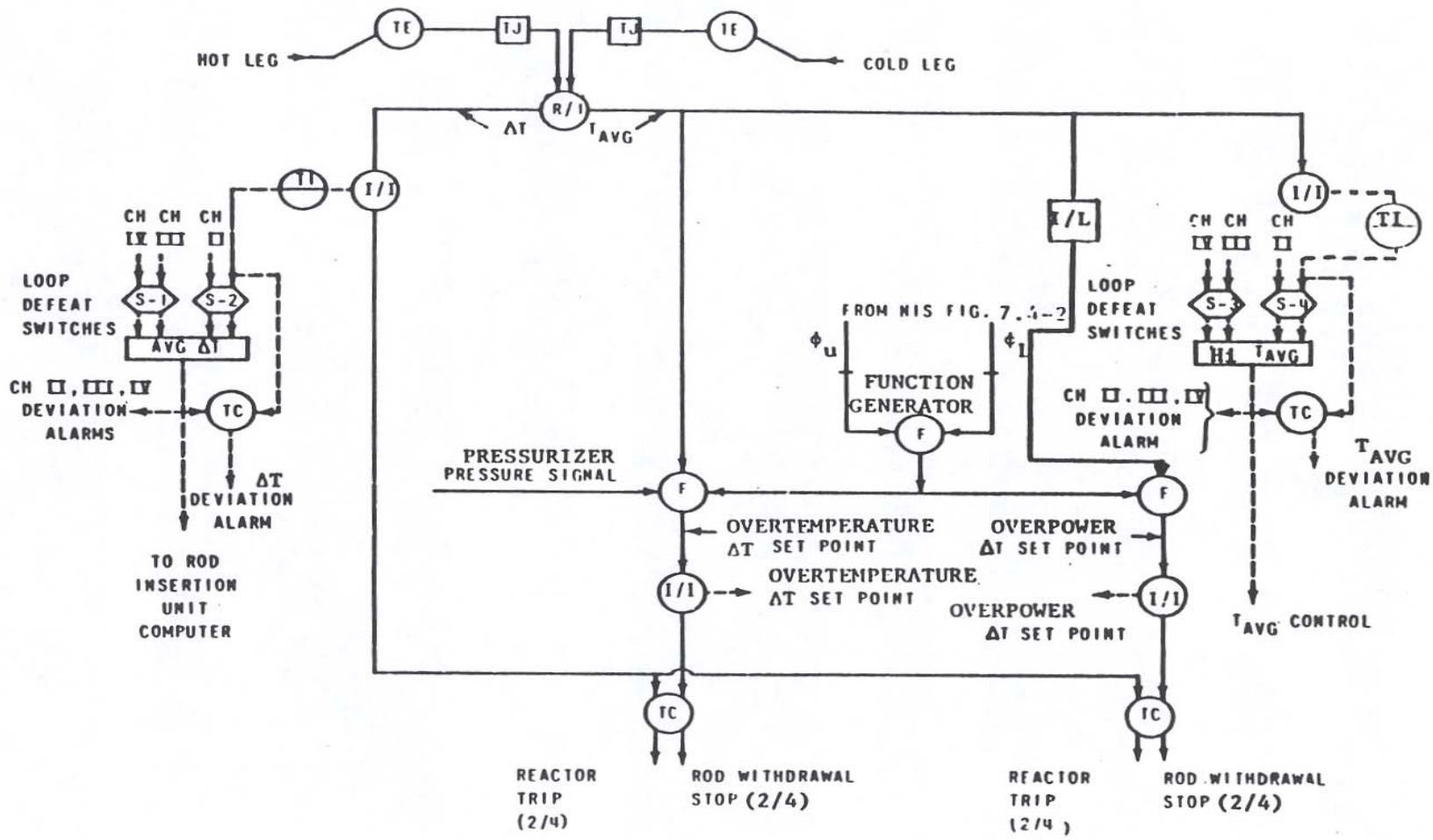


Figure 7.2-9 ANALOG SYSTEM SYMBOLS

Al	-	Alarm
BUF	-	Buffer
F	-	Special function (such as a pressure compensation unit lead/lag compensation, summer, etc.)
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-Low	-	Low level
Lo L	-	Low level
Lo LRT	-	Low level reactor trip
Lo PRT	-	Low pressure reactor trip
L_{ref}	-	Programmed reference level
LT	-	Level transmitter
NC	-	Nuclear flux controller
NE	-	Nuclear detector
NI	-	Nuclear flux indicator
NQ	-	Nuclear Power supply
PC	-	Pressure controller (off-on unless output signal is shown)
PI	-	Pressure indicator
P_{ref}	-	Programmed reference pressure
PS	-	Power supply
PT	-	Pressure transmitter
R/I	-	Resistance to current connector
S	-	Control channel transfer switch (used to maintain auto channel during test of the protection channel)
SI	-	Safety injection
T	-	Built-in test point
TE	-	Temperature element
TJ	-	Test signal insertion jack
TP	-	Test point
$\phi_{U,L}$	-	Out of core upper or lower ion chamber flux signals

Figure 7.2-10 PRESSURIZER PRESSURE CONTROL AND PROTECTION SYSTEM

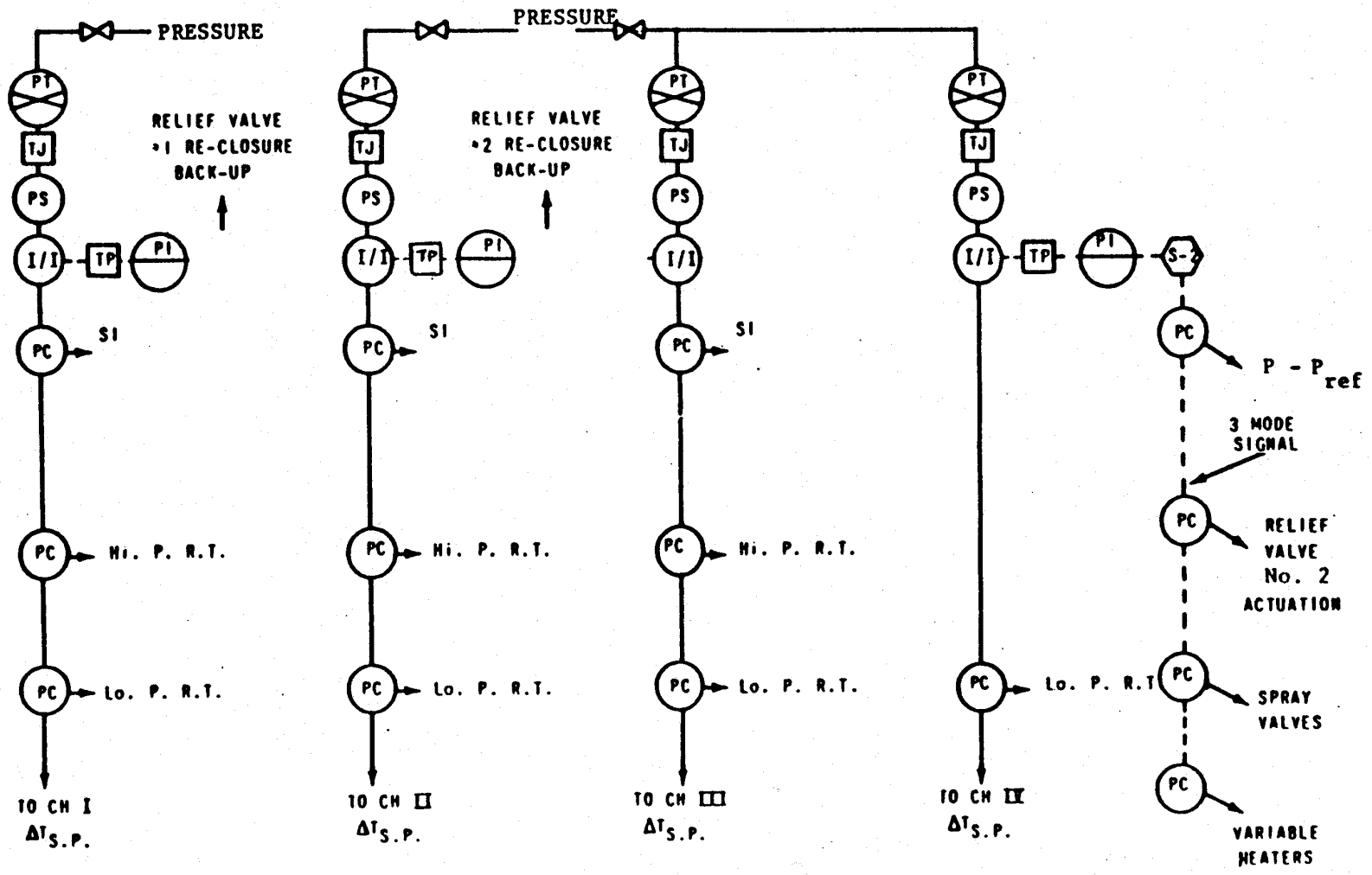


Figure 7.2-11 PRESSURIZER LEVEL CONTROL AND PROTECTION SYSTEM

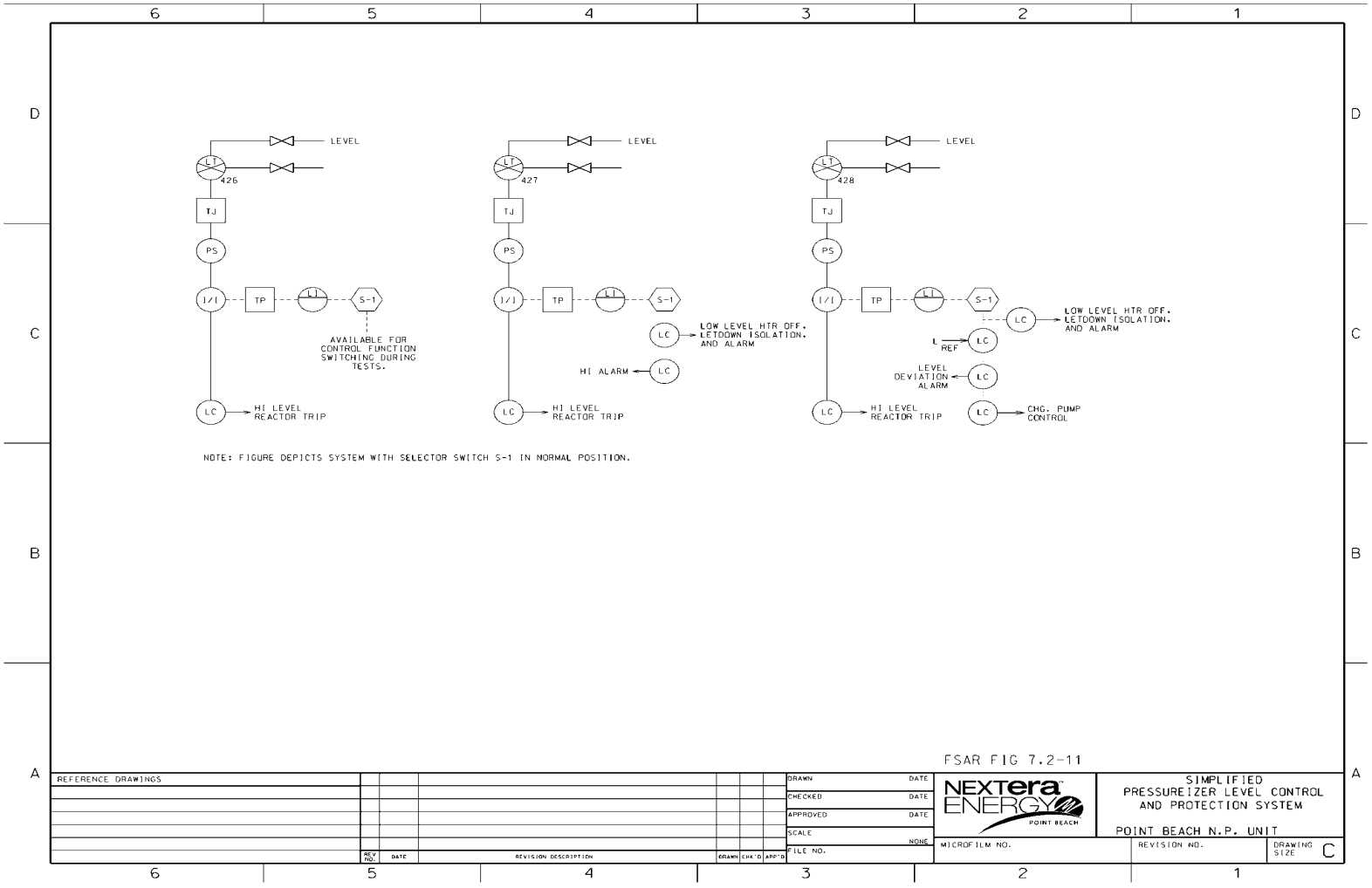
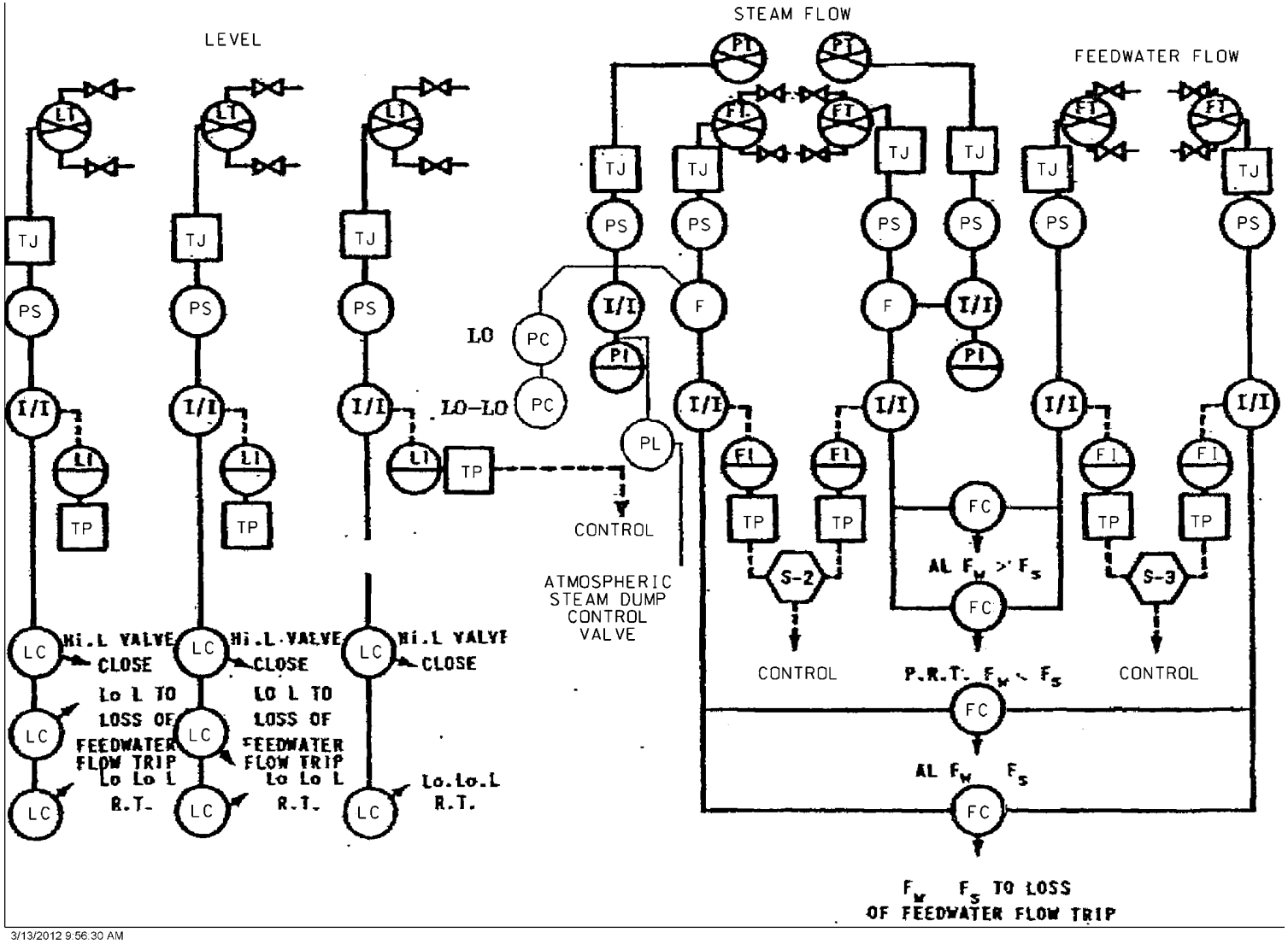


Figure 7.2-12 STEAM GENERATOR LEVEL CONTROL AND PROTECTION SYSTEM



7.3 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

The Engineered Safety Features Actuation System (ESFAS) monitors plant conditions that require Engineered Safety Features (ESF) equipment actuation and automatically initiates ESF equipment to mitigate plant accidents. Actuated ESF equipment (depending on the type and severity of the accident) includes the Safety Injection System, the Containment Spray System, the Containment Air Recirculation Cooling System, Containment Isolation, Steam Line Isolation, Feedwater Isolation, and the Auxiliary Feedwater System.

7.3.1 DESIGN BASES

The following PBNP General Design Criteria (GDC) described in Section 7.1.2 are applicable to the Engineered Safety Features Actuation System:

Criterion 12	Instrumentation and Control Systems
Criterion 15	Engineered Safety Features Protection Systems
Criterion 19	Protection Systems Reliability
Criterion 20	Protection Systems Redundancy and Independence
Criterion 23	Protection Against Multiple Disability for Protection Systems
Criterion 25	Demonstration of Function Operability of Protection Systems
Criterion 26	Protection Systems Failure Analysis Design

In addition to the above GDCs, the Engineered Safety Features Actuation System is designed to IEEE 279, "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems," dated August 1968.

7.3.1.1 Conformance to IEEE 279-1968

IEEE 279 Section 3 provides a list of design bases for a protection system, and IEEE 279 Section 4 lists protection system design requirements. The following criteria correspond to specific points in these IEEE 279 sections.

a. Plant Conditions that Require ESFAS Protective Action

The ESFAS protective action is automatic actuation of ESF equipment. ESF equipment actuation is necessary during certain accidents to protect each of the three physical barriers that guard against the uncontrolled release of radioactivity; (1) the fuel clad, (2) the reactor coolant system pressure boundary, and (3) the containment boundary. The plant conditions that require ESF equipment actuation are those plant accident analyses in Chapter 14 that credit automatic ESF actuation for accident mitigation. Note that different accidents may actuate different types of ESF equipment, and not all accidents described in Chapter 14 require automatic ESF actuation.

b. Plant Variables that Cause Protective Action

The ESFAS variables that actuate various ESF equipment are identified in Table 7.3-1.

c. Minimum Number of Sensors for Each Variable

The minimum number of sensors assigned to each ESFAS variable is listed in Technical Specifications.

d. Prudent Operational Limits for Each Variable

The normal operational limits for each ESFAS variable are defined in the plant operating procedures and Technical Specifications.

e. Margin Between Operational Limits and Onset of Unsafe Conditions

The margin between each ESFAS variable's operational limit and the analytical limit required for automatic ESF actuation is determined by the ESFAS setpoint established for the variable in the Technical Specifications.

f. Variable Levels that Require Protective Action

The analytical limits established in the accident analyses (Chapter 14) determine the point at which the variable requires ESFAS actuation.

g. Conditions for System Performance

The operational conditions (e.g., environmental, seismic, power source, etc.) under which the ESFAS equipment must function are discussed in Section 7.3.3.6 and Section 7.3.3.7.

h. Performance Requirements of ESFAS Variables

The range, response time, and accuracy requirements of the ESFAS equipment are chosen to ensure the assumptions of the accident analyses for the variable being monitored are met.

i. Single Failure

The ESFAS is designed such that any single failure within the protection system or in an associated system which supports its operation will not prevent the protective actions (ESF actuations) assumed in the accident analyses from occurring.

j. Redundancy and Independence

The protection system is redundant and independent for all vital inputs and functions. Each channel is functionally independent of every other channel and receives power from a separate AC power source. Each actuation train is functionally independent of the redundant train and receives power from a separate DC power source.

k. Manual Actuation

Means are provided for the manual initiation of protective actions. Failures in the automatic system will not prevent the manual actuation of protection functions. Manual actuation is designed to require the operation of a minimum of equipment.

l. Channel Bypass or Removal from Operation

The ESFAS is designed to permit any one channel to be maintained, tested, or calibrated during power operation without causing ESF actuation. During such operation, the active parts of the system continue to meet the single failure criterion, since the bypassed channel is placed in a tripped condition.

EXCEPTION: “One-out-of-two” trip logic is permitted to violate the single failure criterion during channel bypass provided that acceptable reliability of operation can be otherwise demonstrated.

m. Capability for Test and Calibration

The relay logic portions of the protection system provide trip signals only after signals from analog channels reach preset values. Capability is provided for calibrating and testing the performance of the analog channel trip bistables and various combinations of coincidence logic during reactor operation.

The sensor channels of the protection system provide an analog signal of the process parameter. The sensor channels can be checked in various ways during power operation, such as:

- Varying the monitored parameter;
- Introducing and varying a substitute transmitter signal; and
- Cross checking between channels that bear a known relationship to each other and that have readouts available.

The design of the system provides for administrative control for the purpose of manually bypassing channels for test and calibration purposes. The design also provides for administrative control of access to all trip settings, module calibration adjustments, test points, and signal injection points.

n. Information Readout

The protection system provides the operator with complete information pertinent to system status and plant safety. Indication is provided on the main control board if some part of the system has been administratively bypassed or taken out of service. The ESF logic cabinets are maintained locked to prevent an inadvertent bypass that could be unmonitored. ESF actuation is indicated and identified down to the channel level.

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

Alarms are also provided to alert the operator of deviation from normal operating conditions so that corrective action may be taken prior to reaching an ESF actuation setting. Further, actuation of any ESFAS channel will actuate an alarm.

o. Operating Bypasses

Where operating requirements necessitate automatic or manual bypass of a protection function, the design is such that the bypass is automatically removed whenever the permissive conditions are not met. Devices used to achieve automatic removal of the bypass of a protection function are part of the protection system.

p. Indication of Bypasses

In addition to administrative controls (such as locked logic cabinets) to prevent inadvertent bypass, indication is provided on the main control board if some part of the system has been administratively bypassed or taken out of service.

q. Completion of Protective Action

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

r. Protective Actions

For anticipated abnormal conditions, protection systems in conjunction with inherent plant characteristics and engineered safety features are designed to assure that limits for energy release to the containment and for radiation exposure are not exceeded.

s. Adverse Environment

The ESFAS equipment is either located in a mild environment (such as the control room) or a potentially harsh environment (such as containment). The environmental qualification of the equipment is discussed further in Section 7.3.3.7.

7.3.1.2 Exceptions to IEEE 279

Some ESFAS functions (backup actuations that are not assumed in the accident analyses) may not fully conform to IEEE 279 criteria. Exceptions to IEEE 279 criteria in backup ESFAS functions are discussed in Section 7.3.3.2.

7.3.2 SYSTEM DESIGN

7.3.2.1 Engineered Safety Features Actuation System Description

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. ESFAS subsystems monitor plant parameters indicative of different accidents. When the minimum number of channels of a monitored variable reaches a preset limit, trip bistables satisfy coincidence logic for an individual subsystem and the subsystem is automatically initiated. ESFAS subsystems include:

- Safety Injection Actuation
- Containment Isolation
- Containment Ventilation Isolation
- Containment Spray Actuation
- Steam Line Isolation
- Auxiliary Feedwater Pump Start
- Feedwater Isolation

Figure 7.3-1 is a logic diagram for various ESFAS subsystems. A simplified block diagram illustrating the channel and relay logic architecture of the engineered safety features actuation

system is shown in Figure 7.3-2. On the channel level, the four ESFAS channels share protection racks with the four Reactor Protection System channels, because some of the same plant variables used to initiate reactor trip also actuate ESFAS subsystems. Not all four channels are used for each ESFAS variable, because most ESFAS subsystem coincidence logics rely on less than four channels to actuate. Each channel is energized from a separate AC power feed.

On the train level, the racks for the two ESFAS logic trains in Figure 7.3-2 are independent and separate from the racks for the two Reactor Protection System logic trains. Each train is energized from a separate DC power feed.

To automatically actuate the various ESFAS subsystems above, the system monitors the following plant variables:

- pressurizer pressure
- steam line pressure
- containment pressure
- containment gaseous radioactivity
- steam line flow
- steam generator level
- RCS temperature (T_{avg})
- 4 kV bus voltage

The specific plant variables that initiate each ESFAS subsystem and their associated coincidence logic are listed in Table 7.3-1. The table also explains any other conditions or interlocks that must be satisfied for ESFAS subsystem actuation to occur.

7.3.2.2 Protective Actions

The following is a brief description of the protective actions performed by the ESFAS subsystems in response to the various plant variables listed in Table 7.3-1.

a. Safety Injection Actuation

A manual or automatic safety injection signal initiates:

1. High head safety injection and low head (RHR) pump start and valve stroking
2. Emergency diesel generator start
3. ESF (safeguards) load sequencing
4. Reactor trip
5. Motor-driven and turbine-driven auxiliary feedwater pump start
6. Service water pumps start
7. Containment fan cooler start and increased fan cooling water flow
8. Non essential service water branch isolation
9. Containment isolation of nonessential systems (from automatic SI signal only)
10. Containment ventilation isolation
11. Feedwater isolation
12. Permissive for Steam Line Isolation

13. Stripping non-safeguards equipment such as the Standby Steam Generator Feedwater Pumps and certain 480 V motor control centers.

A discussion of the ESF (safeguards) load sequencing that occurs on SI actuation may be found in Chapter 8.

b. Containment Isolation

A manual or automatic containment isolation signal closes normally-open power-operated containment isolation valves in the non-essential fluid lines passing through containment, to prevent the uncontrolled release of radioactivity from the containment atmosphere to the outside environment in the event of a Loss-of-Coolant Accident (LOCA). The containment isolation valves associated with each non-essential penetration are identified inSection 5.2.

c. Containment Ventilation Isolation

During shutdown/refueling conditions when the containment ventilation supply and exhaust penetrations may be open, the Train "A" Containment Ventilation Isolation signal (see Table 7.3-1) isolates valves in these penetrations to prevent the uncontrolled release of containment atmosphere radioactivity to the outside environment. Blank flanges are installed inside containment on these penetrations during power operation.

d. Containment Spray Actuation

A manual or automatic containment spray actuation signal starts the containment spray pumps and aligns the associated system valves to initiate containment spray.

e. Steam Line Isolation

A manual or automatic steam line isolation signal closes the main steam isolation valve associated with the loop (steam generator) which generates the signal (indicative of a steam line break).

f. Auxiliary Feedwater Pump Start

The turbine-driven and motor-driven auxiliary feedwater pumps are automatically started to supply emergency feedwater to the steam generators for primary system heat removal under various conditions. Refer to Table 7.3-1 for the conditions under which the pumps are started.

g. Feedwater Isolation

A Safety Injection Actuation signal will isolate the main feedwater lines by closing the Main Feedwater Isolation Valves and Main Feedwater Regulating Valves (main and bypass valves) and tripping the main feedwater pumps, thus closing the pump discharge valves. In addition, a high steam generator water level will close the Feedwater Regulating Valves to prevent steam generator overfill.

h. Auxiliary Feedwater Pump Suction Transfer

The turbine-driven and motor-driven auxiliary feedwater pumps' suction source is automatically transferred from the condensate storage tanks (CST) to service water on low pump suction pressure or low CST level. See Section 7.4.3.

7.3.2.3 System Safety Features

a. Isolation of Redundant Protection Channels and Trains

The same channel and train isolation and separation criteria as described for the reactor protection circuits in Section 7.2.2.3.a are applied to the engineered safety features actuation system.

b. Loss of Power

The four ESFAS channels, which share cabinets with the four Reactor Protection System channels, receive 120 VAC power from the four independent, battery-backed instrument buses. The logic racks for the two ESFAS trains that actuate ESF equipment receive battery-backed power from redundant 125 VDC sources.

Availability of power to the engineered safety features actuation channels and trains is continuously indicated. Loss of AC power to an individual ESFAS channel (except the containment spray actuation channels) will cause the associated channel's output bistables to trip. This "deenergize-to-operate" design is similar to the Reactor Protection System analog channels discussed in Section 7.2.2.3.b. Since a typical ESFAS coincidence trip logic requires more than one channel to cause an actuation, a power failure to a single channel will not cause inadvertent ESF actuation. The exception to this design is the containment spray actuation channels, which are "energize-to-operate" to avoid inadvertent containment spray operation on multiple analog channel power failures.

Two ESFAS actuation trains are provided to actuate the two ESF equipment trains associated with each unit. As an example, the ESFAS 'A' train Safety Injection Actuation signal actuates the 'A' SI pump and the 'B' train actuates the 'B' SI pump. The control circuit for a safety injection pump motor is typical of the control circuit for a large pump motor operated from switchgear. The normally-deenergized SI actuation output relay in the logic rack supplies a normally open contact to the SI pump motor control circuit. When an SI signal is generated from the coincidence logic, the SI actuation output relay is energized and the output contact closes to energize the circuit breaker closing coil, thus closing the breaker, energizing the motor, and starting the pump.

Because the ESFAS output relays are "energize-to-operate," the consequence of a power failure to the ESFAS logic trains differs from the Reactor Protection System logic train's "deenergize-to-operate" design. Unlike the RPS, the ESF output relay design prevents inadvertent ESF equipment actuation on power failure of an actuation train. A single ESF actuation train failure due to loss of power is an acceptable single failure, because the unaffected ESFAS logic train will actuate sufficient engineered safety features to meet the minimum ESF equipment criteria for adequate core cooling and containment functions.

c. ESF Actuation Signal Testing

GDC 25 requires suitable testing of protection system components while the reactor is in operation to determine if failure or loss of redundancy has occurred.

During power operation, each engineered safety features actuation channel and logic train is capable of being calibrated and tripped independently by simulated signals to verify its operation up to the final actuation device (output relay). The at-power testing approach is similar to the analog channel testing and logic testing for the reactor protection system described in Section 7.2.2.3.c. However, it is not possible to test the ESFAS output relays at power to verify that individual ESF equipment actuation occurs, because actuating ESF equipment during normal operation would disrupt power operation. Instead, a resistance check is performed on the output relay coils to verify coil continuity during power operation, and a full verification of ESF equipment actuation is performed during refueling shutdowns.

d. Monitoring ESF Equipment Operation after Actuation

The post-accident monitoring instrumentation used to verify appropriate ESF equipment operation after actuation during an accident is discussed inSection 7.6.2.

7.3.3 SYSTEM EVALUATION

The design of the engineered safety features actuation system meets the applicable protection system General Design Criteria and IEEE 279-1968 criteria. The following sections describe specific areas related to these criteria. The methodology used for setpoint calculations is described in FSAR 7.2.3.6.

7.3.3.1 Specific Control and Protection Interactions

IEEE 279 Section 4.7 requires analysis for control/protection interactions when protection system variables also provide control signals. ESFAS variables that supply control signals were evaluated in WCAP-7306 as follows:

a. Steam Line Pressure

Three steam line pressure channels per loop are used for steam break protection (two-out-of- three low pressure in either steam line actuates safety injection). One of the three pressure channels per steam line is used to automatically control the atmospheric steam dump valve on that steam line, causing the valve to open on a high pressure condition. Each atmospheric steam dump valve is rated at approximately 5% of the full load steam flow. If a spurious high pressure signal occurs in the channel used for control, the associated atmospheric steam dump valve will open and cause low steam line pressure. The steam release rate caused by spurious opening of the dump valve is evaluated in Section 14.2.7. The hypothetical steamline break is limiting with respect to minimum DNBR, and bounds the inadvertent opening of a steam generator relief or safety valve. Therefore, the inadvertent opening of a steam generator relief or safety valve is no longer analyzed for Point Beach as discussed in Section 14.2.7. However, protective action for the spurious opening of an atmospheric steam dump valve can still be provided by other trip signals that are independent of the low steamline pressure trip (e.g., low pressurizer pressure), and is bounded by the hypothetical steamline break. Therefore, a control failure of a steam line pressure channel does not create a need for protective action that relies on the same variable, the IEEE 279 Section 4.7 criterion is met, and two-out-of-three coincidence logic for this variable is acceptable.

b. Pressurizer Pressure

Safety injection actuation occurs when two-out-of-three pressurizer pressure channels indicate low pressure. The three pressure channels also supply control signals for pressurizer pressure control, including signals that open the pressurizer spray valves and pressurizer power operated relief valves (PORVs) on high pressure. The PORV control logic is interlocked to prevent either PORV opening unless two independent pressure channels agree that a high pressure condition exists. As a result, a single pressure channel failing high will not fail a PORV open and initiate an RCS depressurization/blowdown transient requiring safety injection actuation on low pressurizer pressure. Therefore, PORV control does not create a control/protection interaction condition under IEEE 279 Section 4.7.

A single pressure channel failing high could also fail a pressurizer spray valve open, resulting in a gradual RCS depressurization transient as spray cools the pressurizer steam space. The resulting depressurization transient may cause both a reactor trip and safety injection actuation on low pressurizer pressure. However, because there is no mass loss from the RCS, a safety injection actuation signal is not required to mitigate this transient. As discussed in Section 7.2.3.2.c, the reactor trip on low pressurizer pressure is a two-out-of-four coincidence, which meets the control/protection interaction criterion for this transient. Because a failed-open spray valve transient does not require safety injection actuation to mitigate the transient, a control/protection interaction condition does not exist between spray valve control and the SI actuation logic.

Based on the above, the two-out-of-three coincidence logic for SI actuation on low pressurizer pressure meets the control/protection interaction criterion of IEEE 279 without the need for a fourth pressure channel and two-out-of-four coincidence.

c. Steam Generator Level

Feedwater isolation occurs on a two-out-of-three high-high steam generator water level in either steam generator. One of the three steam generator level channels is shared with the feedwater control function. If the shared channel failed low, control action would open the feedwater control valve associated with the steam generator, while at the same time failing to detect a high level condition. The two remaining level channels would both be required to detect high-high level and initiate feedwater isolation to prevent SG overfill. With an additional single failure required by IEEE 279, this arrangement would represent a violation of the control/protection criterion.

Steam generator overfill protection was reviewed generically for Westinghouse plants under NUREG-1217 and NUREG-1218 as part of the evaluation for Unresolved Safety Issue A-47, “Safety Implication of Control Systems in LWR Nuclear Power Plants.” NUREG-1218 Section 7, the existing logic arrangement was accepted because "changes to improve the existing overfill-protection systems from a two-out-of-three to a two-out-of-four steam generator high-high level trip do not significantly reduce risk." Therefore, this condition represents an allowable exception to the IEEE 279 control/protection interaction criterion for Westinghouse plants.

Unresolved Safety Issue A-47 resulted in the issuance of Generic Letter 89-19 (Reference 1). The PBNP overfill protection system design is consistent with the Westinghouse Group I design described in enclosure 2 to the generic letter, with the exception of not tripping the main

feedwater pumps on SG water level. NRC acceptance of the steam generator overfill protection system design was based on: 1) the two credited SG level channels being separate from the feedwater control system with separate power supplies, 2) the components not being located in the same cabinets as the feedwater control system, and 3) because emergency procedures exist which specify operator actions to ensure feedwater isolation for fires which could affect both the feedwater control system and the overfill protection system simultaneously. Additionally, plant Technical Specifications ensure operability and provide surveillance requirements for the overfill protection system (Reference 2).

7.3.3.2 Specific Exceptions to IEEE 279-1968

a. Containment Gaseous Radioactivity

The containment radiation detectors that initiate containment ventilation isolation on high gaseous radioactivity are not classified as safety-related and are not seismically-qualified. Use of non-safety-related detectors for containment ventilation isolation is acceptable, because no Chapter 14 accident relies on these detectors to function for containment ventilation isolation. The offsite dose analysis for a fuel handling accident does not credit containment ventilation isolation, and conservatively assumes that all radioactivity released during the accident is vented from containment.

b. Auxiliary Feedwater Initiation Contacts

The field contacts that start Auxiliary Feedwater pumps on bus undervoltage are not classified as safety-related and are not seismically-qualified. Some AMSAC field contacts also may not be classified as safety-related or seismically-qualified. Use of non-safety-related contacts for starting AFW pumps is acceptable, because no Chapter 14 accident relies on these inputs to start the AFW pumps.

For both cases above, the field wiring between the non-safety-related detectors/contacts and the safety-related circuits that actuate ESF equipment may not fully meet separation criteria for safety-related wiring. The basis for allowing exceptions to separation criteria for this wiring is that the non-conforming circuits are electrically isolated such that an electrical fault in the non-safety-related field wiring will not propagate into and disable the primary actuation circuits. Therefore, any failure in the non-safety-related field wiring will not affect the primary actuation functions assumed in the accident analyses.

7.3.3.3 Operating Bypasses and Resets

a. SI Block Function

IEEE 279 Section 4.12 requires that where operating requirements necessitate automatic or manual bypass of a protective function, the design shall be such that the bypass will be removed automatically whenever permissive conditions are not met.

To prevent unnecessary safety injection actuation during normal plant shutdown/cooldown due to either low pressurizer pressure or low steam line pressure, a manual SI block function is provided. Blocking SI actuation on both variables allows the primary system to be depressurized for maintenance and refueling operations without causing safety injection actuation. This manual SI

block function is permitted at a preset pressurizer pressure below normal operating pressure but above the setpoint for low pressurizer pressure SI actuation. The logic is designed so that the blocking action is automatically removed if operating pressure increases above the pressure at which the manual block is permitted. When the SI block condition is in effect, the condition is continuously annunciated in the control room, as required by IEEE 279 Section 4.13. The SI block function does not prevent SI actuation on high containment pressure.

b. SI Actuation Reset

IEEE 279 Section 4.16 requires that once initiated, a protective action shall go to completion, and return to operation shall require subsequent deliberate operator action. The SI actuation circuitry is provided with a reset function to allow the operator to regain control of equipment after SI actuation goes to completion. A time delay in the circuit prevents any operator interference in SI actuation for approximately 1-2 minutes after actuation occurs. After the time delay times out, the operator can manually reset the SI actuation circuitry to regain control of individual actuated equipment.

c. Containment Isolation and Containment Ventilation Isolation Reset

NUREG 0578 Item 2.1.4 and NUREG 0737 Item II.E.4.2 require that the containment isolation design shall be such that resetting the isolation signal will not result in the automatic reopening of containment isolation valves, and that reopening of containment isolation valves shall require deliberate operator action. Resetting of safety injection, containment ventilation isolation, or containment isolation will not automatically open any of the fluid paths to or from containment which are isolated upon receipt of the initiating signal. The valves must be individually opened by deliberate operator action. Resetting of Safety Injection does not reset containment ventilation isolation or containment isolation. Resetting containment isolation can only occur after safety injection has been reset. Resetting containment ventilation isolation can only occur if safety injection has been reset and if both high radiation signals that can initiate containment ventilation isolation are not present.

d. Containment Spray Reset

The containment spray actuation circuitry is provided with a manual reset function to allow the operator to regain control of equipment after the high-high containment pressure actuation signal has cleared. After containment spray is reset the spray additive tank outlet control valves will return to the preset position on their hand control station (normally closed).

e. General Design Features for Safety Injection, Containment Isolation, Containment Ventilation Isolation and Containment Spray Reset Circuits

The following common design features are applicable to the above safeguards reset circuits.

- Except for the spray additive tank outlet control valves, associated safety related equipment remains in its emergency mode upon reset of an ESF actuation signal (Reference 3).
- Resetting a safeguards circuit will not prevent subsequent manual actuation of the circuit.

- Separate reset switches are provided for each train and each reset switch is fitted with a cover to prevent inadvertent or accidental operation.

f. Feedwater Isolation Reseset
Feedwater isolation reset capability is provided for Train A and B by a single pushbutton for each feedwater loop. Operating the pushbutton allows control of the feedwater regulating bypass valve by its auto/manual controller. Feedwater isolation reset does not affect the main feedwater regulating valves. Circuit design prevents feedwater isolation reset if SI has not been reset or if a high-high level exists in the associated steam generator.

7.3.3.4 Manual AFW Flow Control During Plant Shutdown

The successful operation of the engineered safety features only involves actuation, with one exception. This exception is manually controlling steam generator water level using the auxiliary feedwater pumps during plant shutdown, to remove reactor decay and sensible heat. This manual control involves positioning the auxiliary feedwater flow control valves in order to maintain proper steam generator water level. Steam generator water level indication and controls are located in the control room and at a local control station. Safety related backup pneumatic supplies are provided for the motor-driven auxiliary feedwater pump flow control valves and the motor-driven and turbine-driven auxiliary feedwater pump minimum flow recirculation valves (See Section 10.2.2). If a loss of operating air occurs, or an auxiliary feedwater pump minimum flow recirculation valve fails closed, manual operator action may be required to prevent the potential failure of the pump(s). By procedure, the operator will use the manual gag to open the minimum recirculation valve(s) to prevent pump damage that could be caused by overheating.

7.3.3.5 Separation of SI Reactor Trip Signals

The SI actuation contacts that supply a signal to the reactor trip logic originate in each of the two ESFAS logic trains. Each ESFAS logic train supplies a reactor trip signal to both trains of reactor protection logic. This leads to a unique condition where the ESFAS logic A train is communicating with the RPS logic B train (as well as with the A train), and the ESFAS B train is communicating with the RPS A train (as well as with the B train). This condition does not create an electrical separation conflict between redundant trains because the inputs to reactor protection are channel-related. Within each train of reactor protection, the two inputs from SI actuation train A & B enter two separate channel-related racks. There, the inputs drive separately fused isolation relays.

7.3.3.6 Seismic Qualification of ESF Actuation System Equipment

The protection system components seismic qualification test program described in Section 7.2.3.4 for reactor protection system components also applies to ESFAS components.

7.3.3.7 Environmental Qualification of Protection System Equipment

The protection system equipment that is located in a mild environment (an environment that would, at no time, be more severe than the normal service environment, such as the control room or cable spreading room) is not required to be environmentally qualified in accordance with 10 CFR 50.49. However, the design for normal service conditions and the PBNP quality assurance, maintenance, and surveillance programs ensure that the equipment is capable of performing its safety function on demand throughout its installed lifetime.

ESFAS equipment that is located in a potentially harsh environment (a design basis accident environment which is significantly more severe than normal service conditions), such as sensors inside containment, is designed to perform its safety function throughout its installed lifetime under the operating service conditions of its installed location. Regarding qualification to continue to function under a harsh post-accident environment, ESFAS components located in potentially harsh environments only require formal environmental qualification if: 1) the component is required to mitigate the accident that creates the harsh environment and the harsh environment degrades the component performance before the protective function occurs, or 2) the component is used for post-accident functions not related to the protection function.

7.3.3.8 Environmental Qualification of ESF Equipment

Engineered Safety Features electrical equipment has been evaluated with respect to its local design basis accident environment. The equipment is designed and qualified as necessary to ensure that it can perform its safety function in such conditions throughout its installed lifetime.

Electrical equipment which could be subjected to a harsh accident environment is listed in Table 7.3-2 with its general operating mode and time to complete its ESF function. This equipment is environmentally qualified in accordance with 10 CFR 50.49. The safety related electrical equipment qualification is controlled and documented in accordance with administrative procedures. Regulations governing qualification are described in Section 6.1.1.

Factors considered in qualification include aging in normal service, harsh post-accident environments, and the time required for performing the safety function. Environmental parameters evaluated are temperature, pressure, chemical spray, relative humidity, radiation exposure, and submergence, if applicable. The design considerations and specifications used in selection of motors which must function in a post-accident environment are discussed in Section 6.2, Section 6.3, and Section 6.4. Similar application criteria apply to the specifications of control, instrumentation, and other equipment.

Areas of high radiation would exist inside the containment and in those portions of the auxiliary building near emergency core cooling system equipment following a major loss-of-coolant accident. The maximum expected dose rate inside the containment would be in the range of 10^6 rads per hour. The maximum expected dose rate in high radiation areas of the auxiliary building (e.g., residual heat removal compartments) would be less than one 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 bearing lubrication.

The electrical equipment for the emergency core cooling system located in the containment uses inorganic, silicone, and epoxy plastic insulating materials. These materials have a threshold for radiation damage, which might affect their function, of 10^8 rad or higher. Therefore, considerable margin is provided above the maximum post-accident radiation dose that would result from the dose rates specified above and exposure times listed in Table 7.3-2. The lower ambient temperatures and radiation levels in the auxiliary building permit the use of normal elastomer or plastic insulation materials. These materials have a threshold for radiation damage of 10^6 rad or higher.

Where required, because of location in possible high radiation areas, motor bearings are lubricated with suitable environmentally qualified lubricants.

7.3.4 REFERENCES

1. Generic Letter 89-19, "Request for Action Related to Resolution of Unresolved Safety Issue A-47 - Safety Implication of Control Systems in LWR Nuclear Power Plants," dated September 20, 1989.

2. NRC Safety Evaluation dated December 8, 1994, "Safety Evaluation by the Office of Nuclear Reactor Regulation Related to Licensee Response to Generic Letter 89-19 and Proposed Technical Specification Upgrades."

3. NRC Safety Evaluation, "Licensee Response to I&E Bulletin 80-06, Engineered Safety Features (ESF) Reset Controls," enclosed with NRC Memorandum, Point Beach 1 and 2 -ESF Reset Control-I&E Bulletin 80-06, dated July 7, 1981.

4. NRC Safety Evaluation, PBNP Units 1 and 2- Issuance of License Amendments Regarding Extended Power Uprate, May 3, 2011.

5. NRC Safety Evaluation, "Point Beach Nuclear Plant Units 1 and 2- Issuance of License Amendments Re: Auxiliary Feedwater System Modification," dated March 25, 2011.

Table 7.3-1 LIST OF ENGINEERED SAFETY FEATURES ACTUATION SIGNALS
Sheet 1 of 3

ESFAS SUBSYSTEM	COINCIDENCE CIRCUITRY	COMMENTS
SAFETY INJECTION ACTUATION		
1. Low Pressurizer Pressure	Two-out-of-three (2/3)	Low pressurizer pressure and low steam line pressure SI signals may be manually blocked with RCS pressure below SI block setpoint. The block is automatically removed above the setpoint. SI in either unit trips both SSG Pumps if running.
2. Low Steam Line Pressure	Two-out-of-three (2/3) either loop	
3. High Containment Pressure	Two-out-of-three (2/3)	
4. Manual SI Actuation	One switch per train	
CONTAINMENT ISOLATION		
5. Safety Injection Signal	See Items 1-3	Auto SI only; manual SI does not initiate CI
6. Manual Containment Isolation	One switch per train	
CONTAINMENT VENTILATION ISOLATION		
7. Safety Injection Signal	See Items 1-4	Both auto and manual SI initiate CVI
8. Containment High Gaseous Activity	One-out-of-two (1/2)	
9. Manual Containment Spray	See Item 12	
10. Manual Containment Isolation	See Item 6	
CONTAINMENT SPRAY ACTUATION		
11. High-High Containment Pressure	Two-out-of-three (2/3) taken twice	
12. Manual Spray Actuation	Two-out-of-two (2/2) per train	

Table 7.3-1 LIST OF ENGINEERED SAFETY FEATURES ACTUATION SIGNALS
Sheet 2 of 3

ESFAS SUBSYSTEM	COINCIDENCE CIRCUITRY	COMMENTS
STEAM LINE ISOLATION		
13. High Steam flow coincident with low T_{avg}	One-out-of-two (1/2) per loop Two-out-of-four (2/4) low T_{avg} and Safety Injection signal	
14. High-High Steam Flow	One-out-of-two (1/2) per loop and Safety Injection signal	
15. High-High Containment Pressure	Two-out-of-three	
16. Manual Steam Line Isolation	One switch per steam line	
AUXILIARY FEEDWATER PUMP START		
17. Turbine-Driven Pump Start	Safety Injection, or 2/3 Low-Low S/G level in either S/G, or 1/2 loss of voltage on both A01 and A02 or AMSAC signal.	The turbine-driven AFW pump supplies both S/Gs; A01/ A02 signals are non-safety grade
18. Motor-Driven Pump Start	Safety Injection, or 2/3 Low-Low S/G level in either S/G, or 1/2 loss of voltage on both A01 and A02, or AMSAC signal.	The motor-driven AFW pump supplies both S/Gs. Pump starts a nominal 10.5 seconds after any auto start signal with offsite power available and starts a nominal 32.5 seconds after closure of either of its associated EDGs' breaker (no auto start signal required) following a loss of offsite power. Automatic start signal trips both SSG feedwater pumps. A01/A02 signals are non-safety grade.

Table 7.3-1 LIST OF ENGINEERED SAFETY FEATURES ACTUATION SIGNALS
Sheet 3 of 3

FEEDWATER ISOLATION		
19. Safety Injection Signal	See Items 1-4	Both auto and manual SI initiate FW Isolation. Closes Main Feedwater Isolation Valves and MFW Regulating and Bypass Valves. Trips MFW pumps which generates a closure signal for the pump discharge valves, but these are not credited ESF functions.
20. High-High SG Level	2/3 per SG	Closes MFW Regulating and Bypass Valves.
AUXILIARY FEEDWATER PUMP SUCTION TRANSFER TO SERVICE WATER		
21. Turbine-Driven Pump	One-out-of-one low pump suction pressure	Suction transfer on low-low-low CST level is not a credited ESF actuation
22. Motor-Driven Pump	One-out-of-one low pump suction pressure	Suction transfer on low-low-low CST level is not a credited ESF actuation

Table 7.3-2 GENERAL OPERATING TIME REQUIREMENTS FOR ENVIRONMENTAL QUALIFICATION OF ELECTRICAL EQUIPMENT
Sheet1 of 3

Equipment Name	Operating Mode	Time to Operate[a]
Instrumentation		
Reactor Protection System	Continuous	30 minutes
Safeguards Protection System	Continuous	30 minutes
Post Accident Monitoring	Continuous	Available for one year (one day for Containment Spray System)
Valve Operators		
Air-Operated Containment Isolation Valves	Shut on Containment Isolation Signal	10 seconds
Safety Injection System Motor-Operated Valves	Open on Safety Injection Signal	30 minutes
RHR Heat Exchanger Discharge to SI Pump Suction Motor-Operated Valves	Open on Manual Signal for Boron Precipitation Control	Available for 7 hours [b]
Low-Head Reactor Vessel Injection Motor-Operated Valves	Throttle on Manual Signal for Boron Precipitation Control	Available for 7 hours [b]
Containment Sump Suction Isolation and Component Cooling Supply to RHR Heat Exchangers Motor-Operated Valves	Continuous	Available for one year
RHR Heat Exchanger Discharge and Bypass Air-Operated Throttle Valves	Continuous	Available for one year

a. This is the time after the accident in which it is expected that the item will have completed its safety function.
b. Conservatily based on time to initiate low-head vessel injection to preclude boric acid precipitation for a small break LOCA. See FSAR 6.2.2.

Table 7.3-2 GENERAL OPERATING TIME REQUIREMENTS FOR ENVIRONMENTAL QUALIFICATION OF ELECTRICAL EQUIPMENT
Sheet 2 of 3

Equipment Name	Operating Mode	Time to Operate[a]
Valve Operators, Continued		
Containment Spray Air-Operated and Motor-Operated Valves	Continuous	Available for one day
Sample System Air-Operated Valves for Post-Accident Sampling	Continuous	Available for one year
Steam Supply to Turbine-Driven Auxiliary Feed Water Pump Motor-Operated Valves	Open on Turbine-Driven AFW Pump Start Signal	10 minutes
Main Feedwater Regulating and Bypass Air-Operated Valves	Close on Safety Injection Signal	12 seconds (Includes 2 second signal processing delay)
Power Operated Relief Valve Blocking Motor Operated Valve	Continuous	Available for 4 hours
Reactor Coolant System Gas Vent System Solenoid Isolation Valve	Continuous	Available for one year
Motors		
Containment Emergency Fan Cooler Motors	Continuous	Available for one year
Safety Injection and RHR Pump Motors	Start on Safety Injection Signal	Available for one year
Component Cooling Water Pump Motors	Continuous	Available for one year

a. This is the time after the accident in which it is expected that the item will have completed its safety function.

Table 7.3-2 GENERAL OPERATING TIME REQUIREMENTS FOR ENVIRONMENTAL QUALIFICATION OF ELECTRICAL EQUIPMENT
Sheet 3 of 3

Equipment Name	Operating Mode	Time to Operate[a]
Miscellaneous Equipment		
Safeguard Equipment Power, Control, and Instrumentation Cable; Splices; Electrical Penetration Assemblies	Continuous	Consistent with Operating time of associated equipment

Note: Lubricants used in Safeguard Equipment are Environmentally qualified consistent with the operating time of the associated equipment.

a. This is the time after the accident in which it is expected that the item will have completed its safety function.

Figure 7.3-1 ENGINEERED SAFETY FEATURE LOGIC DIAGRAM

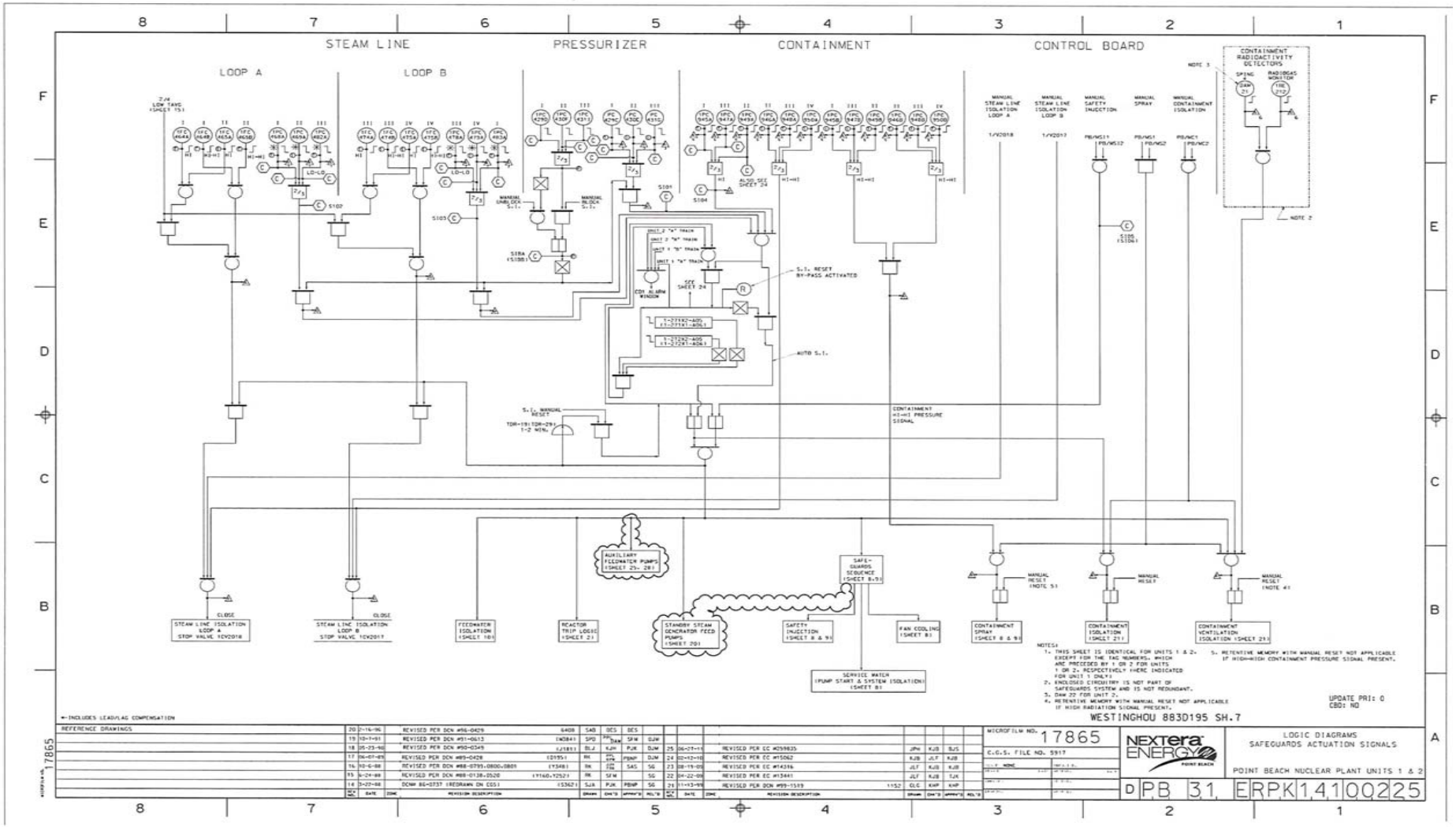
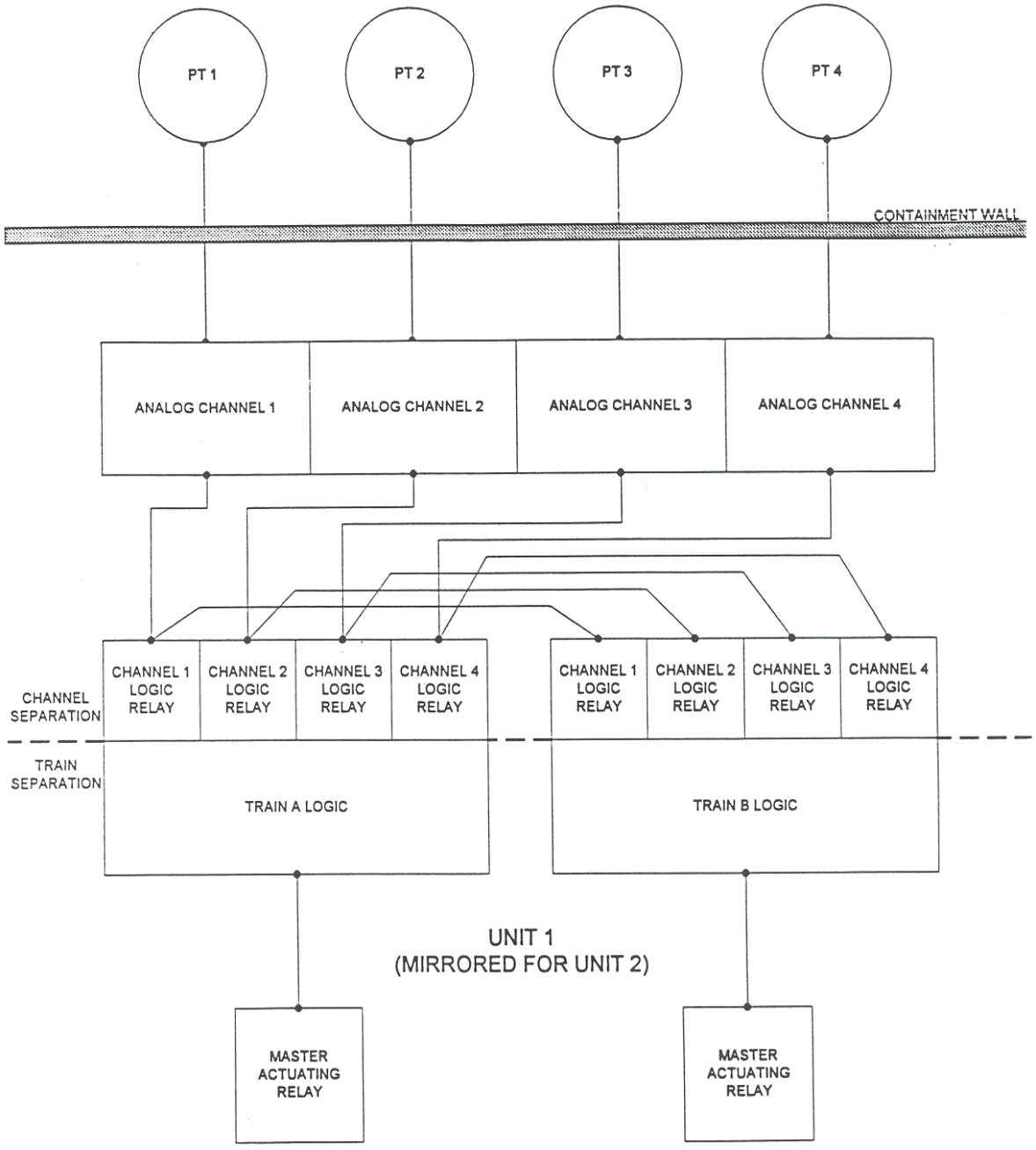


Figure 7.3-2 ENGINEERED SAFETY FEATURE LOGIC MATRIX



7.4 OTHER ACTUATION SYSTEMS

This section addresses actuation systems not included in the Reactor Protection System (RPS) or Engineered Safety Features Actuation System (ESFAS), discussed in Section 7.2 and Section 7.3.

7.4.1 AMSAC

AMSAC stands for an ATWS (Anticipated Transient Without Scram) Mitigating System Actuation Circuitry and is required per 10 CFR 50.62.

AMSAC is classified as Non-Class 1E, except for where it interfaces with the auxiliary feedwater pumps start circuits. The Class 1E, seismically qualified output relays are used to provide the isolation between the auxiliary feedwater pump start circuits and the AMSAC initiation circuitry.

7.4.1.1 Design Bases

The AMSAC System design is based on the requirements of 10 CFR 50.62 (c) (1), which requires a system that is independent and diverse from the Reactor Protection System that will automatically initiate the auxiliary feedwater system and initiate a turbine trip for an ATWS event. The AMSAC System must be capable of operating during a loss-of-offsite-power.

7.4.1.2 System Design

AMSAC, also known as the Loss of Feedwater Turbine Trip (LOFWTT), is designed to trip the main turbine and starts the motor-driven auxiliary feedwater pump and the turbine-driven auxiliary feedwater pump on loss of main feedwater when the reactor is above 40% nominal power. The AMSAC design is based on the conceptual design presented in Section 5.0 of WCAP-10858-P-A, Rev. 1, "AMSAC Generic Design Package."

Turbine power is determined from turbine first stage pressure from which the AMSAC arming permissive P-20 is derived. A bistable actuates a time delay relay at approximately 30% turbine power and arms AMSAC. The 30 % turbine power setpoint ensures AMSAC is armed before exceeding 40% reactor power. On decreasing power the time delay relay keeps AMSAC armed for approximately 60 seconds after turbine power has decreased below the P-20 setpoint. The AMSAC design incorporates a nominal 30 second time delay from initially sensing the loss of main feedwater to initiating signals to trip the turbine and start the auxiliary feedwater pumps. An additional delay time of 60 seconds is assumed for auxiliary feedwater pump start response time as discussed in Section 10.2.1. The 30 second time delay was based on full power operating condition, and should allow the reactor protection system to actuate prior to AMSAC. However, at lower power levels above P-20 AMSAC may cause a turbine trip, and subsequent reactor trip prior to an RPS initiated reactor trip. A turbine trip caused by AMSAC appears no different than any other turbine trip, which has been analyzed as a Loss of Electrical Load in Section 14.1.9.

AMSAC monitors the availability of main feedwater by way of the main feedwater pumps breaker position and the valve position of the main feedwater regulating valves (MFRVs) and main feedwater isolation valves (MFIVs); refer to Figure7.4-1. Loss of main feedwater is identified when either:

- Both main feedwater pumps breaker's are open
- Both main feedwater regulating valves are shut
- Both main feedwater isolation valves are shut
- A MFRV and/or a MFIV in each feedwater line are shut

Each main feedwater pump breaker has two redundant, physically independent contacts that close when the pump breaker is open. The contacts are connected in a matrix arrangement that actuates AMSAC when one-out-of-two contacts associated with both breakers are closed. This configuration was used because no single failure of a contact will prevent AMSAC from actuating when both breakers are open, nor can a single contact failure cause AMSAC to actuate when both breakers are closed.

Each MFRV (CS-466 and CS-476) and MFIV (CS-3124 and CS-3125) has two redundant position (limit) switch contacts that close when the valve closes. The position switch contacts are connected in a matrix arrangement that actuates AMSAC when one-out-of-two switches associated with either valve in both feedwater lines are closed. Similar to the main feedwater pump breaker contacts, this configuration was used because no single failure of a switch contact will prevent AMSAC from actuating when both feedwater lines are isolated, nor can a single switch contact failure cause AMSAC to actuate when both feedwater lines are not isolated.

The MFRVs and MFIVs were chosen because one valve closing in both feedwater lines will result in the complete loss of feedwater flow at power. Since AMSAC is not armed until the plant is above permissive P-20 the main feedwater regulating bypass valves, which are normally closed at power level greater than 20% to 30%, did not need to be included in the AMSAC design. In addition, since the main feedwater pump discharge valves can only automatically close if the main feedwater pump breakers are open, and because AMSAC monitors the breaker position of the pumps, these valves did not need to be included in the AMSAC design.

Separate latching type relays are used for actuation of the motor-driven auxiliary feedwater pump, opening the turbine-driven auxiliary feedwater pump steam supply valve MS 2019 and opening the turbine-driven auxiliary feedwater pump steam supply valve MS 2020. Separate latching type relays are also used for initiating the main turbine auto stop trip (AST) and the main turbine emergency trip (ET).

The NRC staff reviewed the information submitted related to ATWS for the extended power uprate (EPU) and concluded that the effects on ATWS were adequately accounted for and that AMSAC will continue to meet the requirements of 10 CFR 50.62 following implementation of the EPU. The generic Westinghouse ATWS analyses was confirmed with plant-specific, bounding analyses to be reflective of uprated conditions and indicated that the peak primary system pressure following an ATWS event will remain below the acceptance limit of 3200 psig (Reference 1 and Reference 2).

7.4.1.3 System Evaluation (Reference 3)

a. Diversity

Reasonable equipment diversity between AMSAC equipment and RPS equipment, to the extent practical, is required to minimize the potential for common-cause failures.

The pressure transmitter (PT-5971) used to measure first stage turbine pressure (turbine power) and the bistable (PC-5971) used to provide the P-20 permissive within AMSAC are diverse from those used to provide permissives in the Reactor Protection System (RPS).

Latching relays and time delay relays are used in AMSAC. Latching relays and time delay relays are used in the Engineered Safety Features Actuating System (ESFAS); however, they are not used in RPS. Since AMSAC is only required to be diverse from RPS to minimize a common-cause failure, the use of the latching relays and time delay relays is acceptable.

Although AMSAC hardware not involved in the logic, such as switches, lights, wire and annunciators, are not diverse from those used in RPS, AMSAC has been determined to meet the requirements of diversity associated with the ATWS Rule (10 CFR 50.62).

b. Logic Power Supplies

AMSAC is not redundant and only has one source of power. Each unit's AMSAC is powered from its associated 120 VAC instrument bus (1Y-06 / 2Y-06), which is derived from a diesel generator backed bus (1B-03 / 2B-04) via a 480 VAC to 120 VAC transformers. The diesel generators supply rated voltage to these buses within 10 seconds after a Loss-Of-Offsite-Power (LOOP). This power is diverse and independent from the 125 VDC battery power and 120 VAC inverter power used in the RPS.

IF a unit's AMSAC is armed, the 60 second time delay dropout arming relay prevents it from disarming during a LOOP.

If ATWS conditions have been met for less than 30 seconds prior to a LOOP, the time delay actuation relay will lose power and reset. When the associated diesels restore electrical power AMSAC will function to start auxiliary feedwater pumps after ATWS conditions have been met for 30 seconds. Therefore, a LOOP could delay AMSAC actuation under ATWS conditions for 10 to 40 seconds. Upon actuation the output relays latch to provide a continuous AMSAC actuation signal, regardless of power until the circuit is manually reset.

c. Safety Related Interface

The AMSAC safety related interface is with the auxiliary feedwater pump starting circuits. This interface is through the latching relays. There is no direct interface between AMSAC and RPS; therefore, RPS will perform its required safety function without interference from AMSAC.

d. Quality Assurance

The AMSAC output relays that interface with the safety related Auxiliary Feedwater System and the wires used for the connections are QA components and are subject to the PBNP nuclear quality assurance program. The remainder of the AMSAC system is Augmented Quality (AQ). The controls applied to the AQ portions of the system meet the requirements of 10 CFR 50.62 and Generic Letter 85-06 as clarified in NRC Information Notice 92-06 (Reference 4).

e. Maintenance Bypasses

Key operated Bypass and Test switches are provided on the local AMSAC test panel. The switches allow for maintenance and partial testing of the AMSAC system. Placing the key switches in the Bypass or Test position, results in annunciation in the main control room.

f. Operating Bypasses

The AMSAC system is automatically armed at approximately 40% power, based on turbine first stage pressure, by the P-20 permissive, and automatically disarmed below approximately 40% power. The system remains armed for a nominal 60 seconds after power decreases below 40%. The status of the P-20 permissive signal is continuously indicated in the control room via the annunciator.

g. Means for Bypassing

The permanently installed key operated Bypass switch described above is used to bypass AMSAC during testing and maintenance. A human factors review was performed as part of the modification process.

h. Manual Initiation

No additional manual initiation switches or buttons were installed as part of the AMSAC System, because the control room operator can manually trip the turbine and start the auxiliary feedwater system from the main control room. Therefore, no additional manual initiation capability is required for the AMSAC System.

i. Electrical Independence from existing Reactor Protection System

Independence is required from the sensor output to the final actuation device at which point non-safety related circuits must be isolated from safety related circuits by qualified Class 1E isolators.

The inputs to AMSAC are separate from and independent of RPS. No sensors are common to the RPS and AMSAC Systems. The only safety related interface associated with AMSAC is at the Auxiliary Feedwater System. The isolation between AMSAC and the Auxiliary Feedwater System is through the Class 1E output latching relays, which were tested in accordance with Appendix A of the Safety Evaluation of Topical Report (WCAP-10858-P-A, Rev. 1), "AMSAC Generic Design Package" dated July 1987.

j. Physical Separation from existing Reactor Protection System

The AMSAC circuitry is physically isolated from the RPS circuitry. The equipment associated with AMSAC is located in a cabinet separate from the RPS cabinets. There are no incoming signals from the RPS System to the AMSAC cabinet; therefore, the existing separation criteria for the RPS is not compromised by AMSAC.

k. Environmental Qualification

The equipment installed for AMSAC does not require environmental qualification for the AMSAC function, since it is either located in a mild environment or is not required to operate during or following exposure to potentially harsh environments resulting from design basis accidents. The AMSAC components are qualified for all anticipated environments expected to occur prior to or during an ATWS event. Although environmental qualification is not a design requirement for AMSAC operation, the limit switches on the main feedwater regulating valves are environmentally qualified for High Energy Line Break (HELB) considerations, so that the limit switches added for AMSAC meet the same qualifications as the existing limit switches on the main feedwater regulating valves.

l. Testability at Power

Portions of the AMSAC System, such as the bistables, time delay relays and logic relays, can be tested at power by use of the Bypass and Test switches. These portions of the system are tested semi-annually. The remaining portion of the system, such as the output latching relays, valve position switch contacts and the main feedwater pump circuit breaker position can not be tested at power; therefore, a complete end-to-end test of the AMSAC System is performed during refueling outages.

m. Completion of Mitigative Action

The AMSAC output relays are latching type relays. Once set (actuated), the relay remains in the set position, even if the power is removed. Deliberate operator action is required to reset the relays.

The turbine remains tripped, even when the initiating signal is no longer present. Deliberate operator action is required to relatch the turbine after the trip signal has cleared.

The auxiliary feedwater pumps continue to run, even when the initiating signal is no longer present. Deliberate operator action is required to secure the auxiliary feedwater pumps once started by an automatic signal.

Therefore, once the AMSAC system is initiated it will go to completion until reset by the operator.

7.4.2 LOW TEMPERATURE OVERPRESSURE PROTECTION (LTOP)

7.4.2.1 Design Bases

A Low Temperature Overpressure Protection (LTOP) System is required to protect the reactor vessel from exceeding the 10 CFR 50, Appendix G allowable pressure limits at low temperatures.

7.4.2.2 System Design

The LTOP System is required to provide a diverse means of relieving pressure during periods of solid water operation when the reactor is ≤ LTOP enabling temperature as defined in TRM 2.2; Pressure Temperature Limits Report.

The diverse means of relieving pressure is provided by the two logic trains that open the two pressurizer Power Operated Relief Valves (PORVs) on increasing pressure when the LTOP System is armed. The PORVs are armed for low pressure relief via a key switch on section C04 of the main control board. An Indicating light located above the key switch on the main control board is provided, and is lit when the LTOP System is armed.

Pressure is monitored by a wide range reactor coolant system pressure transmitter (PT-420) to actuate one PORV, and by a pressurizer pressure transmitter (PT-493) to actuate the other PORV. Prior to actuation of the PORVs, an alarm is initiated to warn the operator of increasing pressure. If pressure continues to increase, the pressurizer PORVs will open at ≤ LTOP PORV lift setting limits as defined in TRM 2.2; Pressure Temperature Limits Report.

7.4.3 AFW PUMP SUCTION TRANSFER AND TRIP ON LOW SUCTION PRESSURE

7.4.3.1 Design Bases

Auxiliary Feedwater (AFW) pump trip on low suction pressure was installed on the four original AFW pumps (P38A/P-38B and 1/2P-29) to address Item II.E.1.1 of NUREG-0737. AFW system modifications associated with the extended power uprate (EPU) added unit specific electric AFW pumps 1/2 P-53 which replaced the shared motor-driven AFW Pumps (P-38A/P-38B) as the credited pumps. Low suction pressure trip on low suction pressure was provided for pumps 1/2P-53 and retained on P-38A/P-38B. Additionally, automatic suction transfer from condensate to service water was added for 1/2 P-53 and the steam-driven AFW pumps 1//2P-29.

7.4.3.2 System Design (P-53 and P-29)

The safety-grade automatic suction transfer to service water for AFW pumps P-53 and P-29 on low suction pressure or low-low-low level in either condensate storage tank is designed to provide a continued suction source for the pumps on a loss of condensate storage tank water supply, which could result from a tornado or seismic event.

The suction pressure for each pump is monitored by its associated pressure transmitter. A low suction pressure initiates two time delay relays. When sustained low suction pressure conditions exists the first time delay relay will provide a signal to open the pump's service water suction supply valve. If this action does not re-establish pump suction pressure, the second time delay relay trips the associated pump. A motor-driven pump is tripped by opening its supply breaker and a turbine-driven pump is stopped by isolating the steam supply to the pump by closing its trip throttle valve (MS-2082). No time delay is provided for suction transfer on low-low-low condensate storage tank level.

In addition to tripping the AFW pumps, the following additional actions are performed by the system:

- Blocks the start of the pump or the opening of the trip throttle valve,
- Provides annunciation in the main control room for suction pressure low, low suction pressure trip and suction pressure trip disabled
- Establishes a permissive to manually override the low suction pressure trip.

The trip is overridden by the associated control switch on the main control board, which is used for starting a motor-driven pump or opening the trip throttle valve associated with a turbine-driven pump. When the trip is disabled any subsequent low suction pressure trips associated with that pump are blocked. The trip disabled signal is cleared by operation of the control switch for a motor-driven pump or the override reset pushbutton for the turbine-driven pump.

The low suction pressure circuitry for each pump does not interfere with local operation of the AFW pumps.

7.4.4 REFERENCES

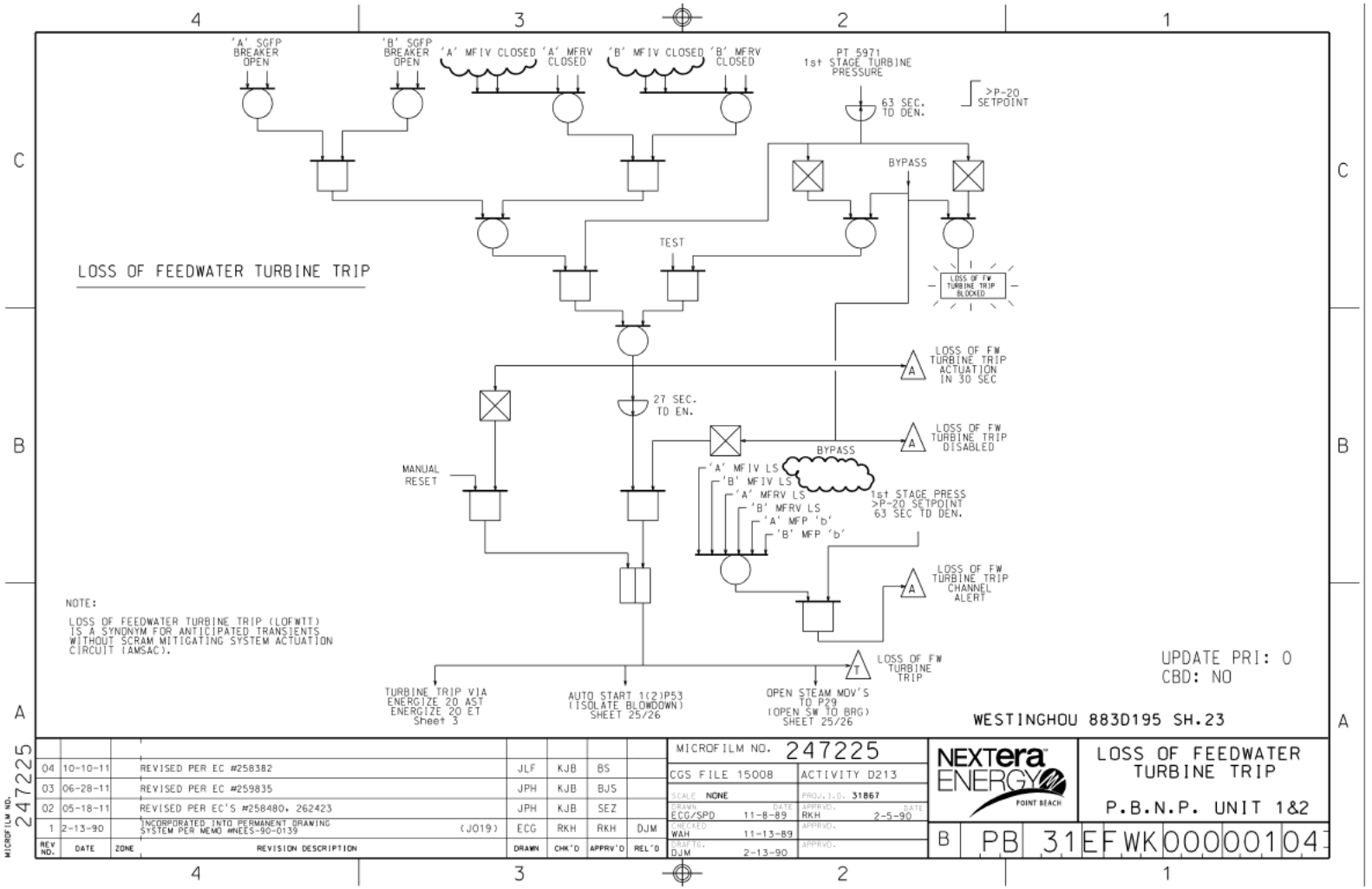
1. NRC SER, "Point Beach Nuclear Plant - Units 1 and 2, Issuance of License Amendments Regarding Extended Power Uprate, dated May 3, 2011

2. Westinghouse letter to NRC, NS-TSM-2182, "ATWS Submittal," dated December 30, 1979.

3. NRC Safety Evaluation "Compliance with ATWS Rule 10 CFR 50.62," dated August 4, 1988.

4. Commitment Change Evaluation 2000-003, dated May 18, 2000.

Figure7.4-1 LOSS OF FEEDWATER TURBINE TRIP



7.5 OPERATING CONTROL STATIONS

7.5.1 CONTROL STATIONS LAYOUT, INFORMATION DISPLAY AND RECORDING

The principal criterion of control station design and layout is that all controls, instrumentation displays and alarms required for the safe operation and shutdown of the plant are readily available to the operators in the control room.

7.5.1.1 Load Dispatching

FPLE Power Marketing, Inc., located at the FPL Corporate office in Juno Beach, FL, is responsible for generation planning, dispatch, and energy trading. The Point Beach units are generally base loaded with load swings performed by licensed plant operators at the request of the system control supervisor.

The Point Beach operator controls the 345 kV generator breakers, the 345 kV circuit switchers, and the 13.8 kV circuit breakers for the high voltage station auxiliary transformers in the switchyard. All 345 kV line and bus section breakers are controlled from the Pewaukee System Control Center by supervisory control.

7.5.1.2 Reactor and Turbine Generator Control Board

The reactor is controlled by the manipulation of the chemical shim (boron concentration) and control rods as discussed in Section 7.7. The control system allows the plant to accept step load changes of 10% and ramp load changes of 5% per minute over the load range of 15 to 100% power under nominal operating conditions. It is also designed to sustain operation following a rapid load decrease of 50% power at a rate up to 200% / minute (Reference 5).

Complete supervision of both the reactor and turbine generator is accomplished from the control room. Units 1 and 2 share a common control room, which is an integral part of the turbine hall. The control room layout including location of control boards for each unit is shown in Figure 7.5-1.

The Main Control Board design minimizes the amount of board area that the control operator needs to manage for the safe operation of both the Nuclear Steam System and conventional plant equipment. Control stations on the board are packaged in a modular concept and are grouped according to function to minimize the possibility of operator error. Mimic buses are also included, for critical systems, to assist the operator. In addition, control stations that consist of both automatic and manual positions are provided with “bumpless” transfer functions.

Indicators, recorders, and annunciator panels are incorporated in the vertical section of the Main Control Board to provide the operator with indication of the monitored plant parameters (e.g., flows, pressure, temperatures, etc.). In addition, alarms are provided by the annunciator panel to indicate parameters that are out-of-limit and which require operator action.

The console section of the Main Control Board contains control devices (switches and control stations) and related indicating lights.

Referring to Figure 7.5-1, sections 1C04 and 1C03 contain the controls, indications and alarms for the primary and secondary systems of Unit 1, respectively. Sections C01 and C02 contain the controls, indications and alarms for common systems as well as the engineered safeguards and electrical systems for both units. Sections 2C04 and 2C03 are the Unit 2 counterparts of 1C04 and 1C03, and are mirror images of sections 1C04and 1C03, respectively.

The rear panels of all the sections are used for controls and indications not normally requiring frequent use and/or observation during normal operation (e.g., bearing temperature recorders, protective relaying, and containment and auxiliary building ventilation, excluding the containment recirculation coolers).

Section 1C04 contains all the controls, indications and alarms required to control the Nuclear Steam supply system. The rod control and nuclear instrumentation systems are located on the left portion of this section, which includes the individual rod position indicators and bottom lights, and all of the controls and nuclear instrumentation required to operate the reactor. On the center and right portions are the controls, indications and alarms for the reactor subsystems (RCS and CVCS), which include the pressurizer pressure and level, and reactor makeup. Also in this section are the indication lights that monitor the bistables associated with the Reactor Protection and Safeguards logic systems, which allows the operator to monitor the status of these systems.

Section 1C03 contains the controls, indications and alarms for the auxiliary coolant system, and the secondary plant, which includes the condensate and feedwater systems, turbine and its auxiliaries, and the portion of the auxiliary feedwater system associated with the Unit 1 turbine driven and motor driven auxiliary feedwater pumps.

Section C01 contains the controls, indications and alarms associated with the engineered safeguards systems for both Unit 1 and Unit 2, which are completely separated between the units. Redundant indicators are provided where required for high reliability. Extensive use is made of mimics and indicating light arrays in order to provide a means of rapidly evaluating the status of these systems in both the active and standby modes. Also in this section are the controls, indications and alarms for those common secondary plant systems that have safeguards functions, which includes the service water system.

Section C02 contains the controls and indication for the electrical systems for both units, which includes the emergency diesel generators, the gas turbine and the 345 kV and 13.8 kV breakers as well as the 4.16 kV and 480 V distribution systems. Unit separation is again maintained. A unique mimic bus (candy stripe) provides for immediate recognition of the 4.16 kV and 480 V safeguards buses and their tie and supply breakers.

7.5.1.3 Auxiliary Safety Instrumentation Panels (ASIPs)

In addition to the controls, indications and alarms available to the operator on the main control board, the Auxiliary Safety Instrumentation Panels (ASIPs) have been installed for the primary purpose of assessing critical parameters in the reactor coolant system and containment structure post-accident. There is one ASIP primarily dedicated to each unit (1C20 and 2C20). These panels are located along the rear (east) wall of the control room as shown in the control room layout, Figure 7.5-1.

Each ASIP is a seismically designed, Class 1E panel which provides analog displays for an integrated set of plant parameters. Although its primary function is critical parameter display and recording for the post-accident environment, it is not intended to be an "isolated" display panel to be used only in that situation. Some of the displayed parameters and control functions are also applicable to routine operations of the plant, such as reactor vessel head and pressurizer vent controls used for startup and shutdown evolutions, and normal operating parameters such as subcooling, reactor vessel water level, RCS temperatures and pressures. Table 7.5-1 summarizes the indications and controls available at each ASIP. In addition to the unit specific indications and controls, the ASIPs also contain common instrumentation such as instrument bus power supply status indicators, meters and controls, and a remote panel for the control room fire detection system. Both ASIPs contain annunciators for these and other systems where this display location is appropriate. Some of the parameters associated with ASIP are described below:

a. RCS Gas Vent System

The RCS Gas Vent System is described in Section 4.2.

b. Reactor Coolant System Hot and Cold Leg Temperatures

Hot and cold leg temperatures are measured using dual-element platinum RTDs. The RTDs are inserted in wells penetrating the main reactor coolant system piping in both the hot and cold legs of the system. In addition to providing temperature indications at the ASIP, the hot leg RTDs can be operator selected as inputs to the Subcooling Monitor System.

c. Reactor Coolant System Wide Range Pressure

Three bourdon tube type transmitters provide pressure indication at the ASIP. Two sense pressure in loop A (cold leg and hot leg) while the third senses pressure in loop B (cold leg). These pressure detectors also provide input to the Subcooling Monitor System and the Reactor Vessel Water Level System.

d. Containment High-Range Radiation

Independent of the Radiation Monitoring System (RMS) described in Section 11.5, three radiation detectors per containment structure sense high radiation levels which might exist in the post-accident environment. Each detector feeds an indicator on the ASIP which indicate on a logarithmic scale over a range of 1 to 10^8 Roentgen/hr. An annunciator also alarms at the high setpoint.

e. Wide Range Containment Pressure

Two diaphragm type transmitters sense pressure in each containment structure. The transmitters are located outside containment and sense containment pressure through a containment penetration. Both indicators and recorders display containment pressure on the ASIP over a range of -5 to 195 psig.

f. Containment Hydrogen Concentration

Four detectors per containment monitor hydrogen concentration in the 0 to 10% range. The detectors input signals to two microprocessors. Each microprocessor receives signals from two detectors in each containment. Four indications per unit are available at the ASIP, corresponding to the four detector locations.

The detectors employ a platinum-based alloy in their sensing mechanism. The alloy generates an electrical potential in the presence of hydrogen proportional to the hydrogen concentration. The detector voltage is sensed and converted by the microprocessor to a value of hydrogen concentration at the sensor location.

g. Reactor Vessel Water Level

Four detectors per unit measure reactor vessel water level by sensing the differential pressure between the bottom of the reactor vessel and the bottom of a reference leg connected to the reactor vessel head via a seal chamber. The four detectors are differential pressure transmitters which share a common reference leg. Two detectors are designated wide range, and can be used when either or both reactor coolant pump(s) are running. They can also be used with reactor coolant pumps off, but with reduced sensitivity when compared with the narrow range instruments. Two detectors are designated narrow range, and are used when reactor coolant pumps are off. All four detectors provide independent indication on the ASIP.

Temperature and pressure are necessary inputs to the reactor vessel level computation. Temperature input is provided from incore thermocouples, while pressure input is obtained from the reactor coolant system wide range pressure detectors described above. The reference leg is density compensated, where density is calculated based on temperatures sensed by thermocouples located along the reference leg tubing.

h. Containment Sump Level

Four level detectors provide indication of water levels in sump A at the keyway below the vessel, and sump B above the containment base level (8 foot elevation). Two detectors are provided in each sump. The detectors in sump A overlap each other and overlap the sump B detectors to measure a continuous level from sump A to sump B. Both detectors in sump B measure the same level. The detectors are float-type devices. Sump level indication is provided on the ASIP.

i. RCS Subcooling

This digital display is used to provide an indication of the temperature differential existing between sensed conditions in the reactor coolant system and the calculated saturation temperature. This two-channel system inputs pressure information from the RCS wide-range pressure detectors and temperature information from one of two operator selected sources-incore thermocouples or hot leg RTDs.

The pressure signal is converted to an equivalent saturation temperature (T_{sat}) through a function generator. This T_{sat} is then compared to either of the temperature sources in a summing device. The temperature difference, or margin, is then displayed on the ASIP. Warning alarms are provided through ASIP mounted annunciators to alert operators to a low subcooling margin condition.

j. Containment Air Temperature

Four platinum RTDs monitor temperature in containment at the 66 foot level, 46 foot level, and two at the 11 foot level. The RTDs on the 11 foot level are labeled Containment Sump Temperature.

k. Steam Generator Wide Range Level

Four detectors (two for SG A and two for SG B) measure steam generator level and indicate on the ASIP. Each detector is a differential pressure transmitter and senses the differential pressure between the steam generator liquid volume (variable leg) and a reference leg.

Each reference leg is maintained in a constant full condition with water provided from a condensing pot.

l. Pressurizer Safety Valve Position Indicator

Lift Indicating Switch Assemblies (LISAs) provide independent and redundant position indication for the two pressurizer pressure relief safety valves. These assemblies operate using magnetically sensitive reed switches which open and shut based on valve position. Each LISA on a valve has two sets of three switches, providing redundant indication of the closed, intermediate, and open positions. A multiple position display is provided for each valve on the ASIP.

m. Core Exit Temperature

Core exit temperature indicating system is described in Section 7.6.

In addition to the indications provided on the ASIP, a list of post-accident monitoring variables, required to meet the intent of Regulatory Guide 1.97 is located in Table 7.6-1.

7.5.1.4 Plant Process Computer System

A scanning, monitoring, logging and historical data storing Plant Process Computer System (PPCS) is installed to assist the operator and technical support personnel in the surveillance of critical plant functions. The PPCS is used to provide supplementary information to the operator, to assist in the normal operation of the Nuclear Steam Supply System, and to inform the operator of off-normal conditions. The plant design includes adequate instrumentation for the operator to operate the plant in a safe manner at all times, regardless of the availability of the computer system.

The PPCS obtains plant data through data acquisition multiplexers located in the computer room and elsewhere within the plant boundaries including the ISFSI cask storage facility. Plant data that was connected to the original PPCS computer remains wired to the computer room multiplexers which are each powered by corresponding uninterruptible power supplies from Unit 1 and Unit 2. Data for both Unit 1 and Unit 2 is collected by the common multiplexing equipment, and transmitted to a fully-redundant distributed computer system. In addition, the PPCS obtains data from the Radiation Monitoring System through separate serial communication links. Application programs on the PPCS are also included for surveillance of reactor control and protection system operations, and for nuclear process calculations. All of this data is available on display/ keyboard stations located in the Control Room (CR), Technical Support Center (TSC) and the Emergency Operations Facility (EOF) located at the Site Boundary Control Center.

PPCS data available in the control room includes logs, sequence of events reports, post-trip reviews, alarm transitions, primary to secondary leakage, wind direction/speed/atmospheric stability, heatup/cooldown rates and requested application program output.

The sequence of events and time history recording capabilities of PPCS, including the selection of parameters and the storage, retrieval, and presentation of the information, were evaluated as being acceptable for satisfying Item 1.2 of Generic Letter 83-28 (Reference 2).

a. Safety Assessment System

The Safety Assessment System (SAS) consists of function dedicated application programs on the PPCS. The SAS is designed to provide easily understandable information from the highly reliable PPCS data acquisition system in human engineered formats. SAS was designed to meet the SPDS (Safety Parameter Display System) requirements of NUREG-0696, NUREG-0737 Item I.D.2, and NUREG-0737 Supplement 1. Although primarily designed for use in accident situations, it can be used in normal day-to-day plant operation. Major features of the SAS include:

1. Plant mode dependent high level display of key parameters used to assess the safety status of the plant.

2. Thirty-minute trend graphs of groups of related parameters.

3. A Critical Safety Function Monitor which defines conditions to assess the status of six critical safety functions.

All SAS screens are available on any PPCS display station via the graphical user interface.

b. Feedwater Leading Edge Flow Measurement (LEFM) System

A CALDON LEFM √2000FC feedwater leading edge flow measurement system was installed in both units to support a 10 CFR 50 Appendix K 1.4% power measurement uncertainty recapture (MUR) uprate. With the LEFM system in operation providing feedwater flow, temperature, and pressure inputs to the PPCS Reactor Thermal Output (RTO) program, operation at the licensed core power of 1800 MWt is allowed. If the LEFM is not in service or is not providing inputs to the PPCS RTO program, power operation is limited per TRM 3.3.2 to a core power of 1775 MWt. (Reference 1 and Reference 3)

The LEFM does not impact the control and protection functions performed by the feedwater flow venturis.

7.5.1.5 Local Control Stations

Local control stations are provided for certain systems and components, which do not require full time operator attendance, or are not used on a continuous basis. Such systems are the Waste Disposal System, Sampling System, Boron Recycle System, heating boilers and the Turbine-Generator Hydrogen Cooling System. Appropriate alarms are located in the control room and are activated to alert the operators of equipment malfunction or approach to unsafe conditions, for these systems.

The waste disposal control board is located in the auxiliary building, in the vicinity of the boric acid and waste evaporators. This board permits the auxiliary operator to control and monitor the processing of wastes from a central location in the general area where the associated equipment is located. Alarm signals from the waste disposal components annunciate on this board. Actuation of any alarm on this board actuates a general "Waste Disposal" alarm on the main control board. In this manner the control room operator can maintain oversight of the system from the control room, and by means of the public address system, dispatch an auxiliary operator to the waste disposal control board if necessary.

Although the waste disposal control board provides the instrumentation required to control the release of wastes, instrumentation provided to monitor activity release is indicated and/or alarmed in the control room. The auxiliary operator has complete knowledge of permissible discharge rates and quantities before any scheduled release is made, and the waste disposal board permits him to control those parameters. By monitoring the release from the control room, the control room operator maintains oversight of the activity.

7.5.2 COMMUNICATIONS SYSTEMS

Communications systems available to the Control Room are as follows:

- A five-channel page-party public address system is provided. This system permits communication from any plant area, including the control room, to all other plant areas by a speaker system. The five channels are separate, simultaneous communication party lines (Reference WE SER 95-012).
- Administrative control consists of the automatic telephone switchboard and the plant communication system outlined above.
- A separate communication system is provided for communication between the control room, the reactor area, and spent fuel pool area during refueling operations.
- AC powered phone jacks, together with an interconnecting wiring system, is provided at each main control panel and at several locations in the plant.
- The public address system is used for emergency alarm. The system is also used to communicate the reactor containment evacuation alarm during refueling or outage periods when containment evacuation becomes necessary. (Reference WE SER 95-012)
- FM radios link the Control Room to Plant Security and to the Manitowoc County Sheriff.

Additional FM radio systems are used throughout the plant and adjacent areas to enable operations, security, health physics, and maintenance personnel to communicate during normal and/or emergency situations.

7.5.3 OCCUPANCY

The General Design Criterion (GDC) for PBNP's Control Room habitability is Criterion 11, which is described in Section 7.1.2. Safe occupancy of the control room during abnormal conditions have been provided for in the design.

7.5.3.1 Control Room Habitability

Adequate shielding has been provided to maintain tolerable radiation levels in the control room during accident conditions, as described in FSAR Section 11.6.

The control room ventilation system normally combines outside makeup air with a large percentage of recirculated air. The radiation monitoring system monitors radiation levels in the control room and in the air supply to the control room. The control room ventilation system is automatically placed in emergency Mode 5 by a high radiation signal from the control room area monitor RE-101, by a high radiation signal from the noble gas monitor RE-235 located in the supply duct to the control room or by a containment isolation signal. Refer to Section 9.8 for further discussion of control room ventilation system performance capability.

7.5.3.2 Fire Prevention Design

Refer to the Fire Protection Evaluation Report (FPER) for information concerning fire protection features and contingency actions related to postulated control room fires.

7.5.3.3 Station Blackout (SBO)

a. Ventilation

Since control room ventilation will be lost during a station blackout event, openings equaling about 10% of the ceiling area exist to prevent the control room from overheating for the hour ventilation is assumed to be lost. Calculations have been documented which demonstrate that with the assumption of a one hour loss of control room ventilation resulting from a station blackout event, the control room temperature will remain acceptable.

b. Emergency Lighting

Emergency lighting is provided as follows:

Upon total loss of station power, the control room, vital switchgear rooms, diesel generator rooms, and passage ways between these rooms are illuminated by incandescent lighting fixtures which are supplied from the station batteries. These fixtures are normally deenergized and are transferred automatically to station batteries when AC supply to the transfer switch control circuit is lost. Permanently mounted emergency lighting units with an 8-hour battery supply are provided in areas needed for operation of safe shutdown equipment and in access and egress routes to and from these areas. In addition, portable lanterns are available in the control room, auxiliary feedwater pump room, and the auxiliary building operators station. Upon availability of power from the diesel generators, additional illumination will be provided in the aforementioned areas, as well as throughout the plant, by a separate AC emergency lighting system.

7.5.4 EMERGENCY SHUTDOWN CONTROL

The Control Building, its equipment, and furnishings have been designed so that the likelihood of fire or other conditions which could render the control room inaccessible, even for a short time, is extremely small.

As a further measure to assure safety, provisions have been made so that plant operators can shut down and maintain the plant in a safe condition by means of controls located outside the control room. During such a period of control room inaccessibility, the reactor will be tripped and the plant maintained in the hot shutdown condition. If the period extends for a long time, the Reactor Coolant System can be borated to maintain shutdown as xenon decays.

Local controls are located such that the stations to be manned, and the times when attention is needed, are within the capability of the plant operating crew. The plant communication system provides communication among the personnel so that the operation can be coordinated.

The functions for which local control provisions have been made are discussed in Section 7.5.4.1 below. Indication and controls provided outside the control room are discussed in Section 7.5.4.2.

See the Fire Protection Evaluation Report (FPER) for information related to postulated fires that require emergency shutdown control from outside the Control Room.

7.5.4.1 Functions With Local Control Provisions

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

- Open rod control breakers at the reactor trip switch gear, or
- Actuate the manual turbine trip on the turbine (above 50% power).

Following evacuation of the control room the following systems and equipment are provided to maintain the plant in a safe shutdown condition and have provisions to allow operation from outside the control room:

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

a. Residual Heat Removal

Following a normal plant shutdown the condenser steam dump control system dumps steam to the condenser and maintains the reactor coolant temperature at its no load value. Redundancy and full protection where necessary is built into the system to ensure the continued operation of the steam generator units. If the automatic condenser steam dump control system is not available, power operated relief valves (one on the each main steam line) maintain the steam pressure. These relief valves are further backed up by safety valves on each main steam line. Numerous calculations, verified by startup tests on the Connecticut-Yankee and San Onofre Power Plants have shown that with only the main steam line safety valves, the reactor coolant system maintains itself close to the nominal no load condition. For decay heat removal it is only necessary to maintain the control on one steam generator.

For the continued use of the steam generators for decay heat removal, it is necessary to provide a source of water, a means of delivering that water, and finally, instrumentation for pressure and level indication.

During shutdown the source of water for steam generator makeup is the condensate storage tank with additional water available from the service water system. Feedwater may be supplied to the steam generators by the auxiliary feedwater pumps (electrical and/or steam driven). These pumps and associated valves have local controls.

b. Reactivity Control

Following a plant shutdown to hot shutdown condition, soluble poison (boron) is added to the primary system to maintain subcriticality. The chemical and volume control system is used for adding boron to the reactor coolant system. Boration requires the use of:

> Charging pumps and volume control tank with associated piping. Boric acid transfer pumps with tanks and associated piping, letdown station, nonregenerative heat exchanger and associated equipment, component cooling system, and the service water systems.

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 10 to 15 hours after shutdown. Also, additional time will elapse before the 1% reactivity shutdown margin provided by the control rods is reduced. This delay would provide ample time for emergency measures.

c. 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 temperature reduces the water volume in the system and requires water makeup if continued pressure control is to be maintained.

Makeup water to control pressurizer level is supplied by the chemical and volume control system during normal operation. The equipment required for boration is described above; however, makeup water is only required for level control. The makeup water is obtained from the normal source, the volume control tank.

d. Operation of Other Equipment

Technical Specification 3.6.5 requires the air temperature inside containment to be kept below 120°F. For this reason the containment air recirculation fan coolers and service water pumps must be operated as required.

e. Electrical Systems

Offsite or onsite emergency power must be available to supply the above systems and equipment for the hot shutdown condition.

7.5.4.2 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:

a. Indication

1. Level Indication for the Individual Steam Generators.
   - One set in the room containing the Turbine Driven Auxiliary Feedwater (TDAFW) and Standby Steam Generator (SSG) Feedwater Pumps.

2. Pressure Indication for the Individual Steam Generators.

   - In the room containing the TDAFW and SSG Feedwater Pumps.

3. Pressurizer Level and Pressure Indicators.
   - One set near the charging pump local control point.

4. Pressurizer Level Indication
   - In the room containing the TDAFW and SSG Feedwater Pumps.

5. Reactor Coolant System Hot and Cold Leg Temperatures
   - In the room containing the TDAFW and SSG Feedwater Pumps.

6. Source Range Reactor Power (Count Rate and Startup Rate)
   - Each near charging pump local control point.
   - Each in the room containing the TDAFW and SSG Feedwater Pumps.

b. Controls

Local stop/start pushbutton motor control stations are provided at each of the following motors. The motor control stations are provided with a selector switch that will transfer control of the switchgear from the control room to local motor control stations at the motor. Placing the local selector switch in the local operating position will initiate an annunciator alarm in the main control room and will extinguish the motor control position lights on the main control room panel. The control function circuitry for each Motor Driven Auxiliary Feedwater Pump flow recirculation valve is isolated when the pump is operated from the local control station. Automatic speed control to maintain pressurizer level is also not available for any charging pump in local control.

- Motor Driven Auxiliary Feedwater Pumps.
- Charging Pumps.
- Boric Acid Transfer Pumps.

Local control of the service water pumps and containment cooling accident fans may be performed by operating their normal 480 V feed breaker in the cable spreading room.

[redacted]

Alternative motor control locations are not required for the following:

Component Cooling Water Pumps: Normally in operation. On loss of off-site power, the emergency diesel generators will automatically restore power to the safeguards buses. This will allow the associated CC Pump to automatically restart unless the loss of power is coincident with a safety injection.

Instrument Air Compressors: Normally in operation. Backup to instrument air for some components is provided by nitrogen bottles or air accumulators as discussed in Section 9.7, Instrument Air (IA)/Service Air (SA). On loss of off-site power, the emergency diesel generators will automatically restore power to the safeguards buses. The compressors may be manually energized. The control point is in the control room.

1. Speed Control

   Speed controls are provided locally for:

   - The Turbine Driven Auxiliary Feedwater Pump
   - The Charging Pumps

2. Valve Control

   Valve controls are provided locally for:

   - Main Feedwater Control Valves.
   - Auxiliary Feedwater Control Valves (These valves are located local to the auxiliary feed pumps).
   - Atmospheric Relief Valves (Auto control normally at hot shutdown).
   - All other valves requiring operation during hot standby can be locally operated at the valve.
   - Letdown orifices isolation valves locally to the charging pumps. Local pushbuttons with selector switch and position lamp.

3. Pressurizer Heater Control

   Stop/start buttons controls located near the charging pumps are provided to control two 200 kW backup heater groups. The local control station is provided with a selector switch that will transfer control of the heaters from the main control room to the local control station.

c. Lighting

   Emergency lighting is provided in all operating areas as identified under Section 7.5.3.3.b.

d. Communications

   The communication network described in Section 7.5.2 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 the control room.

7.5.5 REFERENCES

1. NRC Safety Evaluation dated November 29, 2002, “Issuance of Amendments Re: Measurement Uncertainty Recapture Power Uprate (TAC Nos. MB4956 and MB4957).”

2. NRC Safety Evaluation dated September 25, 1990, “Safety Evaluation by the Office of Nuclear Reactor Regulation Related to Generic Letter 83-28, Item 1.2 - Post-Trip Review Data and Information Capability, Wisconsin Electric Power Company Point Beach Nuclear Plant, Unit Nos. 1 and 2.”

3. NRC Safety Evaluation, PBNP Units 1 and 2 - Issuance of License Amendments Regarding Extended Power Uprate, May 3, 2011.

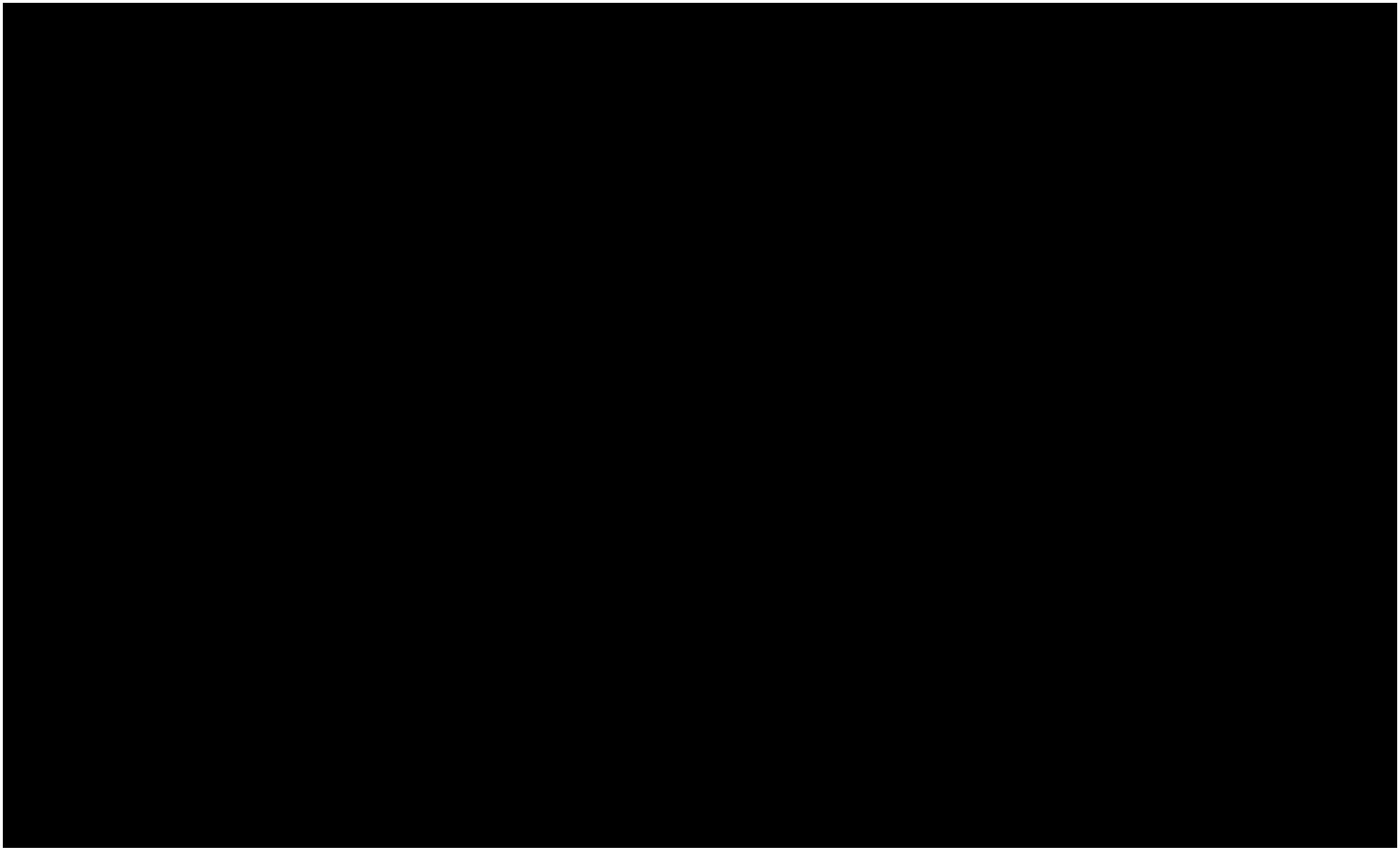
4. NRC Safety Evaluation, "Point Beach Nuclear Plant Units 1 and 2-Issuance of License Amendments Re: Auxiliary Feedwater System Modification," dated March 25, 2011.

5. Westinghouse WCAP-16983-P, Point Beach Units 1 and 2 Extended Power Uprate (EPU) Engineering Report, September 2009.

Table 7.5-1 UNITS 1 AND 2 ASIP INSTRUMENTATION, CONTROLS, AND INDICATION

1. Reactor Vessel Head and Pressurizer Vent System Valves
2. RCS Hot Leg Temperatures (Loops A and B)
3. RCS Cold Leg Temperatures (Loops A and B)
4. RCS Wide-Range Pressure (Loops A and B)
5. Containment High-Range Radiation
6. Wide-Range Containment Pressure
7. Containment Hydrogen Concentration
8. RCS Gas Vent Header Pressure
9. Reactor Vessel Water Level (Wide and Narrow Range)
10. Containment Sump Level (Sumps A and B)
11. Subcooling Monitor (Loops A and B)
12. Instrument Bus Power Supply (common)
13. Containment Air Temperature (46 and 66' Elevations)
14. Containment Sump Temperature
15. Steam Generator Wide-Range Level (Steam Generators A and B)
16. Containment Wide-Range Pressure Recorders
17. Containment Air Sampling System Controls
18. Pressurizer Safety Valve Position Indicators
19. Core Exit Temperature (4 Thermocouples Per Core Quadrant)

Figure 7.5-1 MAIN CONTROL ROOM LAYOUT



7.6 INSTRUMENTATION SYSTEMS

The instrumentation systems described in this section monitor plant conditions, provide signals for protection and control, or provide control room indication of variables for plant operation. The instrumentation systems include:

- Nuclear Instrumentation
- Post-Accident Monitoring Instrumentation
- Incore Instrumentation
- Loose Parts Monitoring

7.6.1 NUCLEAR INSTRUMENTATION SYSTEM

The Nuclear Instrumentation (NI) system consists of two subsystems:

The original Westinghouse-supplied NI system consists of eight out-of-core neutron detectors providing three overlapping ranges (source, intermediate, and power) of neutron flux monitoring. Outputs from the system are used for reactor protection and control, as well as neutron flux indication during reactor startup, operation, and shutdown.

An additional wide-range out-of-core neutron flux detector was added after TMI to provide post-accident neutron flux monitoring capability, to meet the intent of Regulatory Guide 1.97. The wide-range detector is used only for monitoring, and does not provide any protection or control function.

7.6.1.1 Design Bases

The following PBNP General Design Criteria (GDC) described in Section 7.1.2 are applicable to the Nuclear Instrumentation (NI) System:

Criterion 12 Instrumentation and Control Systems
Criterion 13 Fission Process Monitors and Controls

For those portions of the Nuclear Instrumentation System associated with the Reactor Protection System, the design is also required to comply with IEEE 279-1968. In addition, the wide-range detector is required to meet the intent of Regulatory Guide 1.97 design criteria for Type B Category 2 post-accident monitoring instrumentation.

7.6.1.2 System Design

a. Original Westinghouse-supplied NI System

A block diagram of the original NI system is shown in Figure 7.6-1. The system consists of eight neutron flux monitoring channels divided into three overlapping ranges: two source range channels, two intermediate range channels, and four power range channels. The three ranges combine to provide a continuous, overlapping measurement of approximately eleven decades of reactor power, from a completely shutdown condition to 120% of full power. The power range channels are capable of recording overpower excursions up to 200% of full power. The relationship and approximate overlap between the three monitoring ranges is shown in Figure 7.6-2.

The source, intermediate, and power range channels provide control room indication and recording of reactor neutron flux during core loading, shutdown, startup, and power operation. Reactor trip and rod stop control and alarm signals are provided by this system for safe plant operation. Control and permissive signals are transmitted to the reactor control systems and reactor protection system for automatic plant control. Information on equipment failures and test status is annunciated in the control room.

Source Range Channels

Two independent source range channels are provided covering the lowest six decades of leakage neutron flux. Each channel receives pulse-type signals from a proportional counter. The preamplified detector signal is received by the source range instrumentation conditioning equipment located in control room racks. The detector signal, which is a random count rate proportional to leakage neutron flux, is converted to an analog signal proportional to the logarithm of the neutron flux count rate.

Isolated analog signals from each channel are sent to recording and indicating devices to provide the operator with necessary startup information. Startup rate indication is also provided for each source range channel on the main control board. Bistable units located in the racks generate alarms and reactor trip signals if limits are exceeded during reactor startup. Trip signals from the bistables are transmitted to relays in the reactor protection relay racks, where the necessary reactor trip logic is performed. Section 7.2.2.2 describes the source range reactor trip function and source range block function once source range protection and indication is no longer needed during reactor startup.

An isolated count rate signal derived from either source range channel is connected to a scaler-timer. The scaler-timer feeds an audio count rate channel that provides an audible count rate signal proportional to the neutron flux. Speakers are provided both in the containment and in the control room.

Intermediate Range Channels

Two independent compensated ionization chambers provide eight decades of flux coverage from the upper end of the source range to approximately 100% power. The equipment for each channel, including the high voltage and compensating voltage power supplies, is located in a separate drawer. To maintain separation between these redundant channels, the drawers are mounted in separate racks. The signal conditioning equipment furnishes an analog output voltage proportional to the logarithm of the neutron flux. Isolation amplifiers (for startup rate circuits, remote recording, remote indication, etc.) and bistables (for permissives, rod stop and reactor trip) use this analog voltage to indicate plant status and provide the necessary plant control and protection functions. Startup rate indication is also provided for each intermediate range channel on the main control board.

Bistable units located in the intermediate range channels generate alarms and reactor trip signals during reactor startup. Trip signals from the bistables are transmitted to relays in the reactor protection relay racks, where the necessary reactor trip logic is performed. Section 7.2.2.2 describes the intermediate range reactor trip function and intermediate range block function, once intermediate range protection is no longer needed during reactor startup.

Power Range Channels

Four independent, dual-section, uncompensated ionization chambers monitor slightly more than two decades of power range flux leakage. One section of each chamber monitors lower core flux and the other section monitors upper core flux. Each chamber provides two current signal outputs (one from each section) to signal conditioning equipment in the control room racks. Each chamber has an independent high voltage power supply. The individual current signals obtained from each section of the detector are proportional to upper core and lower core neutron flux, respectively. These signals provide core flux status information locally at the instrument racks and remotely, through isolation amplifiers, at the control console. A separate output furnishes bias signals used in the overtemperature ΔT reactor trip function. The individual current signals are combined to provide an average signal proportional to average core flux in the associated core quadrant. This average signal is conditioned to provide an analog voltage signal for use in permissive, control, and protection bistables.

The average power analog signal also provides isolated control signals and core power status information to the operator and computer. The four power range channels are powered from separate vital 120 VAC instrument buses and are housed in separate racks so that a single failure will not affect more than one channel nor cause loss of protection functions.

Isolated analog outputs from each power range channel are compared in a separate auxiliary channel drawer. This comparator provides the operator with annunciation of deviations in average power between the four power range channels. Switches are provided to defeat this comparison for a failed channel, so that subsequent deviations or failures among the three remaining channels are annunciated.

Bistable units located in the four power range channels generate alarms and reactor trip signals during reactor power operation. Trip signals from the bistables are transmitted to relays in the reactor protection relay racks, where the necessary reactor trip logic is performed. Section 7.2.2.2 describes the reactor trip functions which rely on power range channels, including the trip functions for overtemperature ΔT.

If a power range channel failure occurs, switches are provided to permit the failed power range channel's overpower rod stop function to be bypassed, and its average power signal to the reactor control system to be replaced by a signal derived from an active channel. This allows normal power operation to continue while the failed channel is repaired.

Neutron Detector Locations

The neutron detectors for each of the three measurement ranges are mounted in the primary shield wall external to the reactor vessel. The detector locations relative to the reactor core are shown on Figure 7.6-3. The eight detectors are located in six radial locations peripheral to the vessel (two proportional counters shared with two compensated ionization chambers, and four dual-section uncompensated ionization chamber assemblies). Windows in the primary shield wall facing the reactor vessel minimize leakage flux attenuation and distortion.

The two source range proportional counters are located 180 degrees apart on opposite "flat" sections of the reactor core. The source range detectors have a nominal thermal neutron sensitivity of 10 counts per neutron per square centimeter per second, and provide pulse signals to the source range channels. The source range detectors are installed at an elevation approximating the lower quarter core height.

Two intermediate range compensated ionization chambers are installed above the source range detectors in the same detector wells. The intermediate range detectors have a nominal thermal neutron sensitivity of 4×10^{-14} amperes per neutron per square centimeter per second. Gamma sensitivity is less than 3×10^{-11} amperes per Roentgen per hour when operated uncompensated, and is reduced to approximately 3×10^{-13} amperes/R/hr in compensated operation. The detectors are positioned at an elevation approximating the core center height.

The shared detector assemblies each contain one source range and one intermediate range detector. High-density polyethylene, used as a moderator-insulator within the detector assemblies, will be confined at temperatures associated with a loss-of-coolant accident. The detectors are connected to the junction box at the top of the detector well by special high temperature, radiation resistant cables.

The four dual-section power range detector assemblies are mounted at 90 degree intervals around the core, approximately 45 degrees from the two source/intermediate range detector locations, as shown in Figure 7.6-3. These detectors have a total neutron sensitive length of ten feet and a nominal thermal neutron sensitivity for each section of 1.7×10^{-13} amperes per neutron per square centimeter per second. Gamma sensitivity of each section is approximately 10^{-10} amperes per Roentgen per hour. The detectors are located within one foot of the reactor vessel to minimize neutron flux pattern distortions. Signal cables from power range detector wells to the containment penetrations and to the instrument racks in the control room are routed in individual conduits, with physical separation between the penetrations and conduits associated with redundant reactor protection channels.

Protection Philosophy

Redundant channels of the three nuclear instrumentation ranges each support the reactor protection system, as described in Section 7.2. Separation of redundant NI channels in each range is maintained from the neutron sensor to the signal conditioning equipment in the control room and to isolated output devices.

Reactor trips supported by the nuclear instrumentation include source range high level, intermediate range high level, power range high level (low setting), and power range high level (high setting). In addition, the power range channels provide flux difference signals to the overtemperature ΔT trip.

During reactor startup, the source range, intermediate range, and power range (low setting) reactor trips provide low power core protection until reactor power increases sufficiently to allow these trips to be manually bypassed (blocked). Blocking of these low power trips is necessary for full power operation. Two permissive circuits, P-6 and P-10, are used to allow manual blocking of the source range reactor trip (on P-6) and the intermediate and power range (low setting) reactor trips (on P-10). The reactor protection provided by the power range high flux (high setting) trip is never blocked or bypassed.

A P-6 permissive signal would occur during startup when one-of-two intermediate range channels increase above the P-6 setpoint. Above the P-6 setpoint, the operator depresses the manual block switches associated with the source range reactor trip logic circuitry, causing source range detector voltage cutoff and blocking the source range reactor trip function. The P-6 permissive status is continuously displayed by control board status lights.

As power continues to increase during startup, a P-10 permissive signal would occur when two-of-four power range channels exceed approximately 10% of full power. The operator would be alerted to this condition by a control board P-10 permissive status light. Indicators (one per power range channel) and a recorder also provide percent full power indication. If the operator does not initiate manual blocking of the intermediate range trip at this point and continues power escalation, a rod stop will automatically occur from either of the intermediate range channels. Depressing the manual block switches for the intermediate range block above P-10 will block the intermediate range rod stop and the intermediate range reactor trip function. Similarly, depressing the manual block switches for the power range block above P-10 will block the power range (low setting) reactor trip function. If the source range reactor trip was not manually blocked at P-6, the P-10 permissive will also automatically block the source range trip and initiate source range detector voltage cutoff. Blocking of any reactor trip function is indicated by control board status lights.

Automatic removal of the above reactor trip blocks when they are no longer needed is a protection system requirement of IEEE 279. Automatic trip block removal on decreasing power level is discussed under the system evaluation in Section 7.6.1.3.

Where redundant protective channels are combined to provide non-protection functions, the required signals are derived through isolation amplifiers. These amplifiers are designed so that open or short circuit conditions, as well as the application of 120 VAC or 125 VDC, to the isolated side of the circuit will have no effect on the input or protection side of the circuit. As such, failures on the non-protection side will not affect the individual protection channels. Redundant channels are powered from independent power sources, each channel being provided with the necessary power supplies for its detectors, signal conditioning equipment, trip bistables and associated trip relays. The nuclear instrumentation channels are mounted in four separate racks to provide the necessary physical separation between redundant channels.

Testing and Calibration Features

On-line testing and calibration features are provided for each NI channel. The test signals are superimposed on the normal sensor signal during plant operation. This permits valid trip conditions to override the test signal since the sensing elements are never removed from the circuit.

Source and intermediate range channels which provide reactor protection through one-of-two coincidence logic matrices are equipped with positive detent type trip bypass switches to enable a channel to be tested without initiating a reactor trip. The trip-bypass condition for individual channels is indicated at the control board and at the nuclear instrumentation racks.

A test-calibrate module is included in each source range drawer for self-checking of that particular channel. A multi-position switch on the source range drawer front panel controls this module and also the operation of the built-in test oscillator circuits in the source range pre-amplifiers (one per channel), located just outside of containment in the pipeways. The module is capable of injecting test signals of either 60, 10^3, 10^5 and 10^6 cps (counts per second) at the input to the drawer post amplifier, or a variable DC voltage corresponding to 1 to 10^6 cps at the input to the source range pre-amplifier.

An interlock between the trip bypass switch and the source range test-calibrate switch prevents inadvertent actuation of the reactor trip circuits, (i.e., the channel cannot be put in the test mode unless the trip is defeated). Trip bypass is annunciated on the source range drawer and on the main control board per IEEE 279 Section 4.13. Operation of the test-calibrate module is annunciated on the control board as "NIS Channel Test." This common annunciator for all NI channels is alarmed when any channel is placed in the test position, and alerts the operator that a test is being performed at the NI racks.

A built-in test-calibrate module that injects a test signal at the input to the log amplifier provides administrative testing of each intermediate range channel. The signal is controlled by a multiposition switch on the front of each intermediate range drawer. A fixed 10^{-11} ampere signal is available along with a variable 10^{-10} through 10^{-3} signal, selectable in one decade increments.

As in source range testing, the test switch on the intermediate range must be operated in coincidence with a trip bypass on the drawer. An interlock between these switches prevents injection of a test signal, until the trip bypass is in operation. Removal of the trip bypass also removes the test signal. The test-calibrate module provided on each power range is capable of injecting test signals at several points in the channel. In all cases, the test signals are superimposed on the normal signal. The bypass switch from each power range channel activates a common annunciator, "NIS Rod Drop Bypass," but individual bypass status lights identify the particular channel in test. The bistables for the remaining channels not under test do not require bypasses, since the power range reactor trips operate on two-out-of-four coincidence logic. Test signals can be injected independently or simultaneously at the input of either ammeter-shunt assembly to appear as the individual ion chamber currents. Operation of the test-calibrate switch on any power range channel causes the common "Channel Test" annunciator to be alarmed on the main control board.

b. Wide-range Neutron Detector

In addition to the NI system described above, an additional wide-range neutron detector manufactured by Gamma-Metrics was added to each unit after TMI for post-accident monitoring of core neutron flux. The new detector was necessary because the original Westinghouse-supplied NI detectors were not qualified for containment post-accident harsh environment conditions. The Wide Range Neutron Detectors (N-40) may be used to provide visual neutron indication in conjunction with N-31 or N-32 while core geometry changes are in progress.

The location of the wide-range detector relative to the reactor core is shown in Figure 7.6-3. The detector is mounted in its own well in the primary shield wall, 90 degrees from the opposing source/intermediate range detector wells.

The approximate detector range is shown on Figure 7.6-2. The dual fission chamber detector provides neutron flux measurements up to 100% power over twelve decades using two overlapping ranges (source range and percent log power). Each fission chamber is an ion chamber consisting of two uranium-coated aluminum electrodes, insulators, and fill gas. The fission chambers have a sensitive length greater than 40 inches and provide a neutron sensitivity of 2.0 cps/nv or greater.

Equipment for the wide-range channel includes the detector assembly and in-containment cable assembly, an amplifier cable assembly (from containment penetration to pre-amplifier), a pre-amplifier, a signal processor, and an output expansion module. The detector and cable assemblies are environmentally qualified for operation in a harsh containment environment. All electrical equipment is seismically supported. The channel is designed to operate under normal conditions and to survive a loss-of-coolant accident, providing reliable flux measurement before, during, and after an accident. The qualification of this equipment (detector and cable assemblies only) will be maintained during the period of extended operation by the EQ Program. (NRC SE dated 12/2005, NUREG-1839)

[redacted] The pre-amplifier panel houses the power supplies and electronics which condition the detector signal for transmission to the signal processor panel. Signal conditioning includes amplification, pulse shaping, and discrimination against alpha, gamma and electronic noise. Circuitry in the pre-amplifier panel provides continuous self-diagnostics of the integrity of the detector, cables, and power supplies. The signal processor converts the signal from the pre-amplifier into signals that represent the source range count rate, the reactor power level, and the rate-of-change of the reactor power level. The output expansion module provides electrical isolation of output signals from the signal processor.

The wide-range channel function is indication only, and does not provide input to the reactor control or protection systems. The wide-range channel provides indication on the main control board and at four local safe-shutdown panels (two per unit), and also provides inputs to the plant process computer. Indicators provided on the main control board include source range count rate, source range start-up rate, wide range start-up rate, and wide range percent log power. Indicators provided on local safe-shutdown panels include source range count rate and source range start-up rate.

The wide-range channel is powered from the blue instrument bus supply. An alternate supply independent from the normal supply is provided via station batteries and a local inverter.

The wide range detection channel is environmentally qualified for operation in a harsh environment (detector and cable assemblies only). All electrical equipment is seismically supported. The system is designed to operate under normal conditions and to survive a loss-of-coolant accident (LOCA) environment, providing reliable measurement before, during, and after the LOCA. The qualification of this equipment (detector and cable assemblies only) will be maintained during the period of extended operation by the EQ Program. (NRC SE dated 12/2005, NUREG-1839)

7.6.1.3 System Evaluation

a. Conformance to IEEE 279-1968

Protection Philosophy

During plant shutdown and operation, three discrete independent levels of nuclear protection are provided from the three ranges of out-of-core nuclear instrumentation. The basic protection philosophy is that the three ranges each provide reliable, rapid, and restrictive level-trip protection (as opposed to startup rate protection) which is not dependent upon operation of higher range instrumentation.

Reliability is obtained by providing redundant channels which are physically and electrically separated. Fast trip response is an inherent advantage of using level-trip protection in lieu of startup rate protection (with a long time constant) during plant startup. More restrictive operation is an inherent feature, since an increase in plant power cannot be performed until satisfactory operation is obtained from higher range instrumentation, which permits administrative bypass of the lower range instrumentation. On decreasing power level, protection is automatically made more restrictive. Startup accidents while in the source range are rapidly terminated without significant increases in neutron flux and with essentially no power generation or reactor coolant temperature increase.

The indications and administrative actions required by this protection system during reactor startup are readily available to the operator and result in safe, uncomplicated power escalation.

Reactor Trip Block Removal

IEEE 279 Section 4.12 requires that operating bypasses of protective actions must be automatically restored when the conditions requiring the bypass no longer exist. When reactor power drops to the level that the reactor trip blocks manually installed for the source, intermediate, and power range (low setting) trips are no longer necessary, the reactor trips are automatically restored. The intermediate range and power range (low setting) trips are restored on decreasing power when three of four power range channels are below the P-10 permissive setpoint. The source range trip is restored when two of two intermediate range channels are below the P-6 permissive. The P-6 and P-10 permissive circuitry associated with administrative blocking of reactor trips and the automatic reactivation of the trips on decreasing power is designed to the same separation and redundancy criteria as the reactor trip functions.

b. Rod-Drop Indication

The nuclear instrumentation rod drop indication is provided by comparison of the average nuclear power signal with the same signal which is conditioned by an adjustable lag network. This method provides a response to dynamic signal changes associated with a dropped rod condition, but does not respond to the slower signal changes associated with normal plant operation. A power range rod drop alarm from at least one of the four power range channels will occur for any dropped rod condition.

c. Control and Alarm Functions

Various control and alarm functions are obtained from the three ranges of out-of-core nuclear instrumentation during shutdown, startup and power operation. These functions are used to alert the operator of conditions which require administrative action and 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.

1. Source Range

   No control functions are obtained from the source range channels. Alarm functions are provided, however, to alert the operator of any inadvertent changes in shutdown reactivity. Visual annunciation of this condition is at the control board, with audible annunciation performed in the containment and control room. This alarm can either be blocked prior to startup or can serve as the startup alarm in conjunction with administrative procedures.

2. Intermediate Range

   Both alarm and control functions are supplied by the intermediate range channels. Blocking of rod withdrawal is initiated by either intermediate range on high flux level. This condition is alarmed at the control board to alert the operator that rod stop has been initiated. In addition, the intermediate ranges provide an alarm when either channel exceeds permissive P-6 level. This alerts the operator to the fact that he must take administrative action to manually block the source range trips to prevent an inadvertent trip during normal power increase.

3. Power Range

   The power range channels provide alarm and control functions similar to those in the intermediate ranges. An overpower rod stop function from any of the four power range channels blocks rod withdrawal and is alarmed at the control board. The power ranges also provide an alarm function when 2 of 4 channels exceed the P-10 permissive level. As in the case of P-6 in the intermediate range, this alerts the operating personnel that administrative action (namely, blocking of intermediate and power range (low setting) trips) is required before any further power increase may take place.

   The power range channels also support two additional permissive functions. The P-8 and P 9 permissives bypass certain reactor trips at low power levels based on plant conditions that include 3 of 4 power range channels less than approximately 35% for P-8 and 50% (35% if Tavg < 572°F) for P-9. A permissive status light is provided for P-8, “Nuclear Power Below P-8”. The extinguishing of the P-8 permissive status light alerts the operator that certain reactor trips on low loop flow and open RCP breakers are now active. These trips are blocked at low power while the status light is on.

d. Loss of Power

The nuclear instrumentation draws its primary power from the vital instrument buses whose reliability is discussed in Section 8.0. Redundant NI channels are powered from separate buses.

Loss of a single vital instrument bus would result in the initiation of reactor trips signals associated with the channel deriving power from that source. During power operation, the loss of a single bus would not result in a reactor trip since the source and intermediate range trips are bypassed and the power range high flux reactor trip function operates from a 2 of 4 logic. If the bus failure occurred during low power operation while the source or intermediate range trips (1 of 2 logic) are in effect, a reactor trip would result.

e. Power Range Channel Accuracy

The relation of the power range channels to the Reactor Protective System has been described in Section 7.2. To maintain the desired accuracy in trip action, the total error from drift in the power range channels is held to ±1.0% at full power. Routine tests and recalibration ensure that this degree of deviation is not exceeded. Bistable trip set points of the power range channels are also held to an accuracy of ±1.0% of full power.

7.6.2 POST-ACCIDENT MONITORING INSTRUMENTATION

7.6.2.1 Design Basis

The General Design Criterion (GDC) applicable to the post-accident monitoring instrumentation is Criterion 12, Instrumentation and Control Systems, described in Section 7.1.2.

In addition to GDC 12, the post accident monitoring instrumentation is also required to meet the intent of Regulatory Guide 1.97, Rev. 2, "Instrumentation to Assess Plant and Environs Conditions during and following an Accident."

7.6.2.2 System Design

Consistent with Regulatory Guide 1.97, the post-accident monitoring instrumentation is grouped into five types related to the importance of the information to the operator, as follows:

TYPE A variables are those variables that provide the primary information required to permit the control room operator to take specific manually controlled actions for which no automatic control is provided and that are required for safety systems to accomplish their safety functions for design basis accident events.

TYPE B variables are those variables that provide information to indicate whether plant safety functions are being accomplished.

TYPE C variables are those variables that provide information to indicate the potential for being breached or the actual breach of the barriers to fission product releases.

TYPE D variables are those variables that provide information to indicate the operation of individual safety systems and other systems important to safety.

TYPE E variables are those variables to be monitored as required for use in determining the magnitude of the release of radioactive materials and continually assessing such releases.

The post-accident monitoring instrumentation is also separated into three qualification categories, depending on the importance of the variable:

Category 1 provides the most stringent requirements and is intended for key variables. Full qualification, redundancy and continuous real-time display are provided and battery-backed (standby) power is required.

Category 2 provides less stringent requirements and generally applies to instrumentation designated for indicating system operating status. This category provides for qualification, although it is less stringent than Category 1. Category 2 may require seismic qualification if the instrumentation is part of a safety related system; redundancy; or continuous display. A high reliability power source (not necessarily standby power) is also required.

Category 3 is intended to provide requirements that will ensure that high-quality off-the-shelf instrumentation is obtained and applies to backup and diagnostic instrumentation. It is also used where the state of the art will not support requirements for higher qualified instrumentation.

Refer to Table 7.6-1 for a complete listing of post-accident monitoring instrumentation variables and their associated type and category.

7.6.2.3 System Evaluation

The post-accident monitoring instrumentation meets the intent of Regulatory Guide 1.97, Rev. 2. The original response to Generic Letter 82-33 on RG 1.97 implementation dated 9/1/83 identified specific exceptions taken to the regulatory guidance, including the justification for those exceptions. Table 7.6-1 reflects the current list of post-accident monitoring variables that meet the commitments made in the GL 82-33 response.

7.6.3 INCORE INSTRUMENTATION

7.6.3.1 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 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.

7.6.3.2 System Design

The in-core instrumentation system consists of thermocouples, positioned to measure fuel assembly coolant outlet temperature at preselected locations, and flux thimbles, which run the length of selected fuel assemblies to measure the neutron flux distribution within the reactor core.

The measured 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 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 an estimate of the coolant flow distribution.

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

a. Thermocouples

Chromel-alumel thermocouples are threaded into guide tubes that penetrate the reactor vessel head through seal assemblies, and terminate at the exit flow end of the fuel assemblies. The pressure boundary between the reactor vessel head seal assembly and the thermocouple column is formed by the compression of grafoil packing rings. (See Figure 7.6-4) The thermocouples are enclosed in stainless steel sheaths within the above tubes to allow replacement if necessary. Outputs from 16 thermocouples per unit (4 per core quadrant) are displayed on direct indicating devices on the ASIP Panels. Core exit thermocouples are provided as inputs to the plant computer system. The computer provides display and recording functions. The support of the thermocouple guide tubes in the upper core support assembly is described in Section 3.0.

There are 39 thermocouple locations per reactor, however some thermocouples are no longer operable. Due to reactor coolant leaks that have occurred in some thermocouple sheaths, several thermocouples in each reactor have been cut or removed and permanent caps or plugs installed to seal the thermocouple assembly.

b. Movable Miniature Neutron Flux Detectors

Four fission chamber detectors (employing $U_3 0_8$ which is 93% enriched in U_{235}) can be remotely positioned in retractable guide thimbles to provide flux mapping of the core. Approximate chamber dimensions are 0.188 in. in diameter and 2.10 inches in length. The stainless steel detector shell is welded to the leading end of the helical wrap drive cable and the stainless steel sheathed coaxial cable. Each detector is designed to have a minimum thermal neutron sensitivity of 1.0×10^{-17} amps/nv and a maximum gamma sensitivity of 3×10^{-14} amps/R/hr. Operating thermal neutron flux range for these probes is 1×10^{11} to 5×10^{15} nv. Other miniature detectors, such as gamma ionization chambers and boron-lined neutron detectors, can also be used in the system. Retractable thimbles into which the miniature detectors are driven are pushed into the reactor core through conduits which extend from the bottom of the reactor vessel down through the concrete shield area and then up to a thimble seal zone.

The thimbles, which are dry inside, are closed at the leading ends and serve as the pressure barrier between the reactor water pressure and the atmosphere. Mechanical seals between the retractable thimbles and the conduits are provided at the seal line.

During reactor operation, the retractable thimbles are stationary. They are extracted downward from the core during refueling to avoid interference within the core during fuel movement. A space above the seal line is provided for the retraction operation.

The drive system for the insertion of the miniature detectors consists basically of four drive assemblies, four path group selector assemblies and four rotary selector assemblies. The drive system pushes hollow helical-wrap drive cables into the core with the miniature detectors attached to the leading ends of the cables and small diameter sheathed coaxial cables threaded through the hollow centers back to the trailing ends of the drive cables. Each drive assembly generally consists of a gear motor which pushes a helical-wrap drive cable and detector through a selective thimble path by means of a special drive box and includes a storage device that accommodates the total drive cable length. Further information on mechanical design and support is described in Section 3.0.

c. Control and Readout Description

The control and readout system provides means for inserting the miniature neutron detectors into the reactor core and withdrawing the detectors at a selected speed while plotting a level of induced radioactivity versus detector position. Each detector can be driven in or out at speeds of 72 feet per minute or 12 feet per minute outside the reactor core and 12 feet per minute when scanning the neutron flux. The average path length external to the core is 120 feet.

Four separate fuel assemblies can be scanned simultaneously. A full core map is read in approximately 2 hours. 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 drive conduit provide means for pre-recording detector and cable positioning in preparation for a flux mapping operation. Each gear box drives an encoder for positional data plotting. One group path selector is provided for each drive unit to route the detector into one of the flux thimble groups. A rotary transfer assembly is a transfer device that is used to route a detector into any one of up to ten selectable paths. Ten manually operated isolation valves allow free passage of the detector and drive wire when open, and prevents leakage of coolant in case of a thimble rupture, when closed. A path common to each group of flux thimbles is provided 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 core 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” consists, briefly, of selecting (by panel switches) flux thimbles in given fuel assemblies at various core quadrant locations. The detectors are driven or inserted to the top of the core and stopped automatically. An x-y plot (position vs. flux level) is initiated with the slow withdrawal of the detectors through the core from top to a point below the bottom. In a similar manner other core locations are selected and plotted.

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

7.6.3.3 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 thimbles have been chosen to permit measurement of hot channel factors with uncertainty of less than 5% for the Heat Flux Hot

Channel Factor and less than 4% for the Enthalpy Rise Hot Channel Factor (95% confidence). Measured nuclear peaking factors will be increased as described in the Technical Specifications Bases to allow for possible instrument error. The DNB ratio calculated with the measured hot channel factor will be compared to the DNB ratio calculated from the design nuclear hot channel factors. If the measured power peaking is larger than expected, power capability will be reduced.

7.6.4 LOOSE PARTS MONITORING

7.6.4.1 Design Basis

The loose parts monitoring system (LPMS) is designed to provide reliable detection of loose metallic debris impacting within the reactor coolant system (RCS).

Metallic impacts within the RCS generate a pressure wave within the coolant. The pressure wave is detected as an acceleration by strategically placed accelerometers that are part of the LPMS. Other sources of pressure waves, such as pumps starting and control rods stepping, are also present in the RCS. The LPMS differentiates between pressure waves caused by metallic impacts and other pressure waves by comparing the detected acceleration to a typical signature of a metallic impact. Pressure-wave-caused accelerations that are not caused by metallic impacts are ignored. Detected metallic impacts initiate an alarm indication and are recorded on the systems event recorder.

7.6.4.2 System Design

The LPMS consists of specially designed high sensitivity transducers at the natural collection points of the RCS, preamplifiers, connection panel, data input boards, data acquisition computer, video monitor, keyboard/mouse, and audio/alarm board. A block diagram of the system is shown in Figure 7.6-5.

Metallic impacts within the RCS cause a small electrical charge proportional to acceleration to be generated by piezoceramic accelerometers. The charge is transmitted by noise-resistant cable to the charge preamplifier inside containment where it is converted to a voltage signal. The voltage signal is transmitted by normal shielded instrumentation cable to the data acquisition system for processing in the LPMS cabinet located in the computer room and recorded by the data acquisition computer. Historical information can be downloaded for records storage and to remove the records from the LPMS computer.

a. Accelerometer Locations

The LPMS has the capability to monitor 16 channels constantly. Two accelerometers per unit are mounted to the transition sleeves of the flux thimble guide tubes at the reactor vessel bottom. Each steam generator has three accelerometers mounted directly to the shell on the hot leg side: one just above the tubesheet, one on the same elevation as the tubesheet, and one just below the tubesheet.

b. System Electronics Cabinet

Signals from the in-containment preamplifiers are carried through containment penetrations to the system electronics cabinet. The cabinet includes a connection panel, data input boards, data acquisition computer, video monitor, keyboard/mouse, and audio/alarm board.

One input channel is provided for each charge preamplifier. The input channel provides energizing current for the preamplifier, filters the preamplifier output to remove high-frequency noise and signals outside the range of interest, and scales the received accelerometer signal. The scaled and filtered acceleration signal from the input channel is transferred to the computer.

The heart of the system is a central processor unit (CPU). The acceleration signal from one of the channels is selected under CPU control. The frequency and relative amplitude are made available to the microprocessor, which inspects the signal for the characteristics of a metal impact. If it is determined that the accelerometer signal represents a metal impact, the microprocessor communicates this to the audio/alarm board.

c. Displays

In the central cabinet, a monitor (operator interface) displays system operating parameters and the results of automated data analysis. On the events reports displays, essential information needed for fast evaluation of metal impacts is continuously updated and provided automatically to the operator for multiple events, single events, or historical events. Key parameters and setpoints as well as current background noise levels are available on the systems status display. Printouts of each display are available on demand.

The Auxiliary Safety Instrument Panel (ASIP) 1C20 Annunciator Window, which is located in the control room, contains remote alarm indication.

7.6.4.3 System Evaluation

The LPMS provides early detection of loose metallic parts in the primary system. Early detection can provide the time required to avoid or minimize damage to primary system components (e.g., the steam generator tubesheets). The LPMS can also minimize radiation exposure to station personnel by providing for the early detection and general location of abnormal structural conditions within the RCS or S/G secondary side.

The initial system calibration has provided a set of “signatures” from various sized weights striking the surface of the reactor and steam generator vessels near the accelerometers. By analyzing the information from the hard drive and comparing this to the signatures, the approximate mass of the object may be determined. The arrangement of the accelerometers on the steam generators has the additional benefit of providing the approximate location of the loose part. Through the use of triangulation and timing data from recorded metal impact signatures, an approximate location and size of the source can be determined.

Table 7.6-1 POST-ACCIDENT MONITORING VARIABLES

Sheet 1 of 5

POST-ACCIDENT MONITORING VARIABLE	Type and Category	Instrument Description (See Note 1)
Refueling Water Storage Tank Level	A, 1	1(2)-LT-972, 1(2)-LT-973
RCS Pressure (wide-range)	A, 1	1(2)-PT-420A, 1(2)-PT-420B, 1(2)-PT-420C
Containment Pressure (low and intermediate range)	A, 1	1(2)-PT-945. 1(2)-PT-947, 1(2)-PT-949 1(2)-PT-946, 1(2)-PT-948, 1(2)-PT-950
Condensate Storage Tank Level	A, 1	LT-4038, LT-4040 LT-4039, LT-4041
Steam Generator Water Level (narrow-range)	A, 1	1(2)-LT-461, 1(2)-LT-462, 1(2)-LT-463 1(2)-LT-471, 1(2)-LT-472, 1(2)-LT-473
Auxiliary Feedwater Flow to Steam Generators	A, 2	1(2)-FT-4036, 1(2)-FT-4037
Core Exit Temperature	A, 1	1(2)-TR-1A(B) and associated core exit thermocouples
Degrees of Reactor Coolant Subcooling	A, 1	1(2)-TM-970, 1(2)-TM-971, 1(2)-PT-420 A&B, TE-450D & 451D and associated core exit thermocouples
Steam Generator Pressure	A, 1	1(2)-PT-468, 1(2)-PT-469, 1(2)-PT-478, 1(2)-PT-479, 1(2)-PT-482, 1(2)-PT-483
Pressurizer Water Level	A, 1	1(2)-LT-426, 1(2)-LT-427, 1(2)-LT-428
Neutron Flux	B, 2 & 3	1(2)-N-40, 1(2)-N-31 & 32, 1(2)-N-35 & 36
Control Rod Position	B, 3	1(2)-RPI-XY, where XY=Core Position Coordinates
Core Exit Temperature	B, 3	1(2)-TE-1 through 1(2)-TE-39
RCS Soluble Boron Concentration	B, 3	Grab Sample Analysis
RCS Cold Leg Water Temperature	B, 1	1(2)-TE-450A, 1(2)-TE-450C, 1(2)-TE-451A, 1(2)-TE-451C
RCS Hot Leg Water Temperature	B, 1	1(2)-TE-450B, 1(2)-TE-450D, 1(2)-TE-451B, 1(2)-TE-451D
RCS Pressure (narrow-range)	B, 1	1(2)-PT-429, 1(2)-PT-430, 1(2)-PT-431, 1(2)-PT-449
Reactor Vessel Water Level	B, 1	1(2)-LT-494, 1(2)-LT-495 1(2)-LT-496, 1(2)-LT-497
Containment Sump Water Level	B, 1 & 2	1(2)-LT-958, 1(2)-LT-959 1(2)-LT-960, 1(2)-LT-961
Containment Isolation Valve Position (for valves that receive an automatic containment isolation signal)	B, 1	Valves Identified in FSAR Section 5.2

Table 7.6-1 POST-ACCIDENT MONITORING VARIABLES

Sheet 2 of 5

Containment Pressure (wide-range)	B, 1	1(2)-PT-968, 1(2)-PT-969
Radioactivity Concentration in Circulating Primary Coolant	C, 1	Grab Sample Analysis
Analysis of Primary Coolant (Gamma Spectrum for Isotopic Analysis)	C, 3	Grab Sample Analysis
Containment Area Radiation (high range)	C, 1	1(2)-RE-126, 1(2)-RE-127, 1(2)-RE-128
Containment Area Radiation	C, 3	1(2)-RE-102, 1(2)-RE-107
Effluent Radioactivity-Noble Gas Effluent from Condenser Air Removal System Exhaust	C, 3	1(2)-RE-215, RE-225
Core Exit Temperature	C, 1	1(2)-TE-1 through 1(2)-TE-39
Containment Hydrogen Concentration	C, 3	1(2)-HYA-964, 1(2)-HYA-965, 1(2)-HYA-966, 1(2)-HYA-967
Containment Effluent Radioactivity-Noble Gases from Identified Release Points	C, 2	RM-SPING-21 & 22 (U1 & U2 Containment Purge Exhaust)
Radiation Exposure Rate (Inside Buildings or Areas in Direct Contact with Primary Containment near Penetrations and Hatches)	C, 3	Applicable monitors in FSAR Table 11.5-1A, RMS Area Monitors
Effluent Radioactivity-Noble Gases (From Buildings as Indicated Above)	C, 2	RM-SPING-23 & 24 (PAB & Drumming Area Vents)
RHR System Flow	D, 2	1(2)-FT-626
RHR Heat Exchanger Outlet Temperature	D, 2 & 3	1(2)-TE-622, 1(2)-TE-623, 1(2)-TE-627, 1(2)-TE-630
RHR Pump Discharge Pressure	D, 2	1(2)-PT-628, 1(2)-PT-629
Accumulator Tank Level	D, 2	1(2)-LT-934 & 935 (Tank B), 1(2)-LT-938 & 939 (Tank A)
Accumulator Tank Pressure	D, 2	1(2)-PT-936 & 937 (Tank B), 1(2)-PT-940 & 941 (Tank A)
Accumulator Isolation Valve Position	D, 3	1(2)-MOV-841A & B
Boric Acid Charging Flow	D, 2	1(2)-FT-128
Flow in HPI System	D, 2	1(2)-FT-924 & 925
HP Safety Injection Pump Discharge Pressure	D, 2	1(2)-PT-922 & 923
Flow in LPI System (Train B)	D, 2	1(2)-FT-928
RHR Heat Exchanger Inlet Temp. (Containment Sump Water During ECCS Recirculation)	D, 2	1(2)-TE-3294, 1(2)-TE-3295

Table 7.6-1 POST-ACCIDENT MONITORING VARIABLES

Sheet 3 of 5

Reactor Coolant Pump Status	D, 3	1(2)-P-1A & B (Motor Current)
Reactor Coolant System Loop Flow	D, 3	1(2)-FT-411 through 416
Reactor Coolant System Code Safety Valve Position	D, 2	1(2)-RC-434-LISA, 1(2)-RC-435-LISA
Pressurizer Power-Operated Relief Valve (PORV) Position	D, 2	1(2)-POS-430, 1(2)-POS-431C
Pressurizer Power-Operated Relief Valve (PORV) Block Valve Position	D, 2	1(2)-RC-515, 1(2)-RC-516
RCS Code Safety Valve and Pressurizer PORV Discharge Line Fluid Temperature	D, 3	1(2)-TE-436, 1(2)-TE-437, 1(2)-TE-438
Pressurizer Heater Status	D, 2 & 3	1(2)-T-1A, B, C, D, E (Breaker Position)
Pressurizer Temperature	D, 3	1(2)-TE-424, 1(2)-TE-425
Pressurizer Relief Tank Water Level	D, 3	1(2)-LT-442
Pressurizer Relief Tank Temperature	D, 3	1(2)-TE-439
Pressurizer Relief Tank Pressure	D, 3	1(2)-PT-440
RCS Gas Vent Isolation Valve Position	D, 3	1(2)-RC-570A & B, 1(2)-RC-575A & B, 1(2)-RC-580A & B
RCS Gas Vent System Pressure	D, 3	1(2)-PT-498
Steam Generator Water Level (wide-range)	D, 1	1(2)-LT-460A, 1(2)-LT-460B 1(2)-LT-470A, 1(2)-LT-470B
Main Steam Flow	D, 2	1(2)-FT-464 & 465, 1(2)-FT-474 & 475
Main Feedwater Flow	D, 3	1(2)-FT-466 & 467, 1(2)-FT-476 & 477
Auxiliary Feedwater Pump Discharge Line Flow	D, 2	1(2)-FT-4002, 1(2)-FIT-4073
Auxiliary Feedwater Pump Discharge Line Pressure	D, 3	1(2)-PT-4005, 1(2)-PT-4071
Auxiliary Feedwater Pump Suction Line Pressure	D, 2	1(2)-PT-4044, 1(2)-PT-4069
Service Water Header Pressure	D, 2	PT-2844, PT-2845
Containment Spray Flow	D, 2	1(2)-FT-962 & 963
Containment Spray Additive Tank Water Level	D, 2	1(2)-LT-931

Table 7.6-1 POST-ACCIDENT MONITORING VARIABLES

Sheet 4 of 5

Heat Removal by the Containment Emergency Fan Coolers	D, 3	1(2)-TE-3270, 3272, 3274 & 3276 1(2)-FS-3225, 3229, 3239 & 3240 1(2)-W-1A1, 1B1, 1C1 & 1D1 Breaker Position 1(2)-FT-2896, 2898, 2900 & 2902 1(2)-TIS-2893, 2901, 2903 & 2972
Containment Atmosphere Temperature	D, 2	1(2)-TE-3292 & 3293
Letdown Line Flow	D, 2	1(2)-FT-134
Volume Control Tank Water Level	D, 2	1(2)-LT-112 & 141
Component Cooling Water Heat Exchanger Outlet Temperature (Cooling Water to ECCS)	D, 2	1(2)-TE-621
Component Cooling Water Flow	D, 2	1(2)-FT-619
High-Level Radioactive Liquid Tank Level	D, 3	LIT-1001 (Waste Holdup Tank)
Radioactive Gas Decay Tank Pressure	D, 3	PT-1036, 1037, 1038, 1039
Emergency Ventilation Damper Positions	D, 2	VNSSB-3246 & 3247; VNPAB-3258-A1, A2, B1 & B2; VNCOMP-4849A, B & D; VNCR-4849C, E & F; VNCSR-4850, 4850B & 4850C; VNCR-4851A, B, C & D, 6748 & 6748A
Station Battery Discharge Rate	D, 2	D-05, D-06, D-105, D-106 & D-305 Ammeters
125 Volt DC Bus Voltage	D, 2	D-01, D-02, D-03, D-04 Voltmeters
120 Volt AC Instrument Bus Voltage	D, 2	1(2)-Y-01 through Y-04 and 1(2)-Y-101 through Y-104 Voltmeters
4160 Volt AC Safeguards Bus Voltage	D, 2	1(2)-A-05 & A-06 Voltmeters
480 Volt AC Safeguards Bus Voltage	D, 2	1(2)-B-03 & B-04 Voltmeters
Emergency Diesel Generator Voltage, Frequency, Loading	D, 2	G-01, G-02, G-03 & G-04
Emergency Diesel Generator Starting Air Pressure Alarm	D, 2	G-01-AP1 & AP2, G-02-AP1 & AP2, PS-6358A & B, PS-6359A & B
Diesel Fuel Oil Day Tank Level	D, 2	LT-3932 & 3934, LS-3932 & 3934, LS-3930A & B, LS-3931A & B, LIT-3992A & B, LS-3935A & B
Instrument Air Pressure	D, 2	PT-3083 & 3084
Process Radiation Monitor from Steam Generator Safety and Atmospheric Dump Valves	E, 2	1(2)-RE-231, 1(2)-RE-232

Table 7.6-1 POST-ACCIDENT MONITORING VARIABLES

Sheet 5 of 5

Particulate and Halogen Sampling from All Other Identified Release Points, with On-site Analysis Capability	E, 3	Grab Samples From PAB & Drumming Area Isokinetic Stack Sampling System
Airborne Radiohalogens and Particulates Sampling	E, 3	Grab Sample Analysis
Plant and Environs Radiation	E, 3	Portable Survey Instruments, TLDs
Plant and Environs Radioactivity (Isotopic Analysis)	E, 3	Grab Sample Analysis
Wind Direction	E, 3	See Note 2
Wind Speed	E, 3	See Note 2
Estimation of Atmospheric Stability (Vertical Temperature Gradient and Standard Deviation of Wind Direction)	E, 3	See Note 2
Primary Coolant and Sump Grab Samples	E, 3	Gross Activity, Isotopic Analysis, Boron, Chloride, Dissolved Hydrogen, pH
Containment Air Grab Samples	E, 3	Hydrogen, Isotopic Analysis

Notes:

1 Instruments credited for more than one variable are generally listed for the highest applicable type and category. The instrument description is not intended to be a list of all components in each instrument loop that are necessary to perform the monitoring function.

2 Refer to Emergency Plan, Appendix L for detailed description of Meteorological System.

Figure 7.6-1 NUCLEAR INSTRUMENTATION SYSTEM

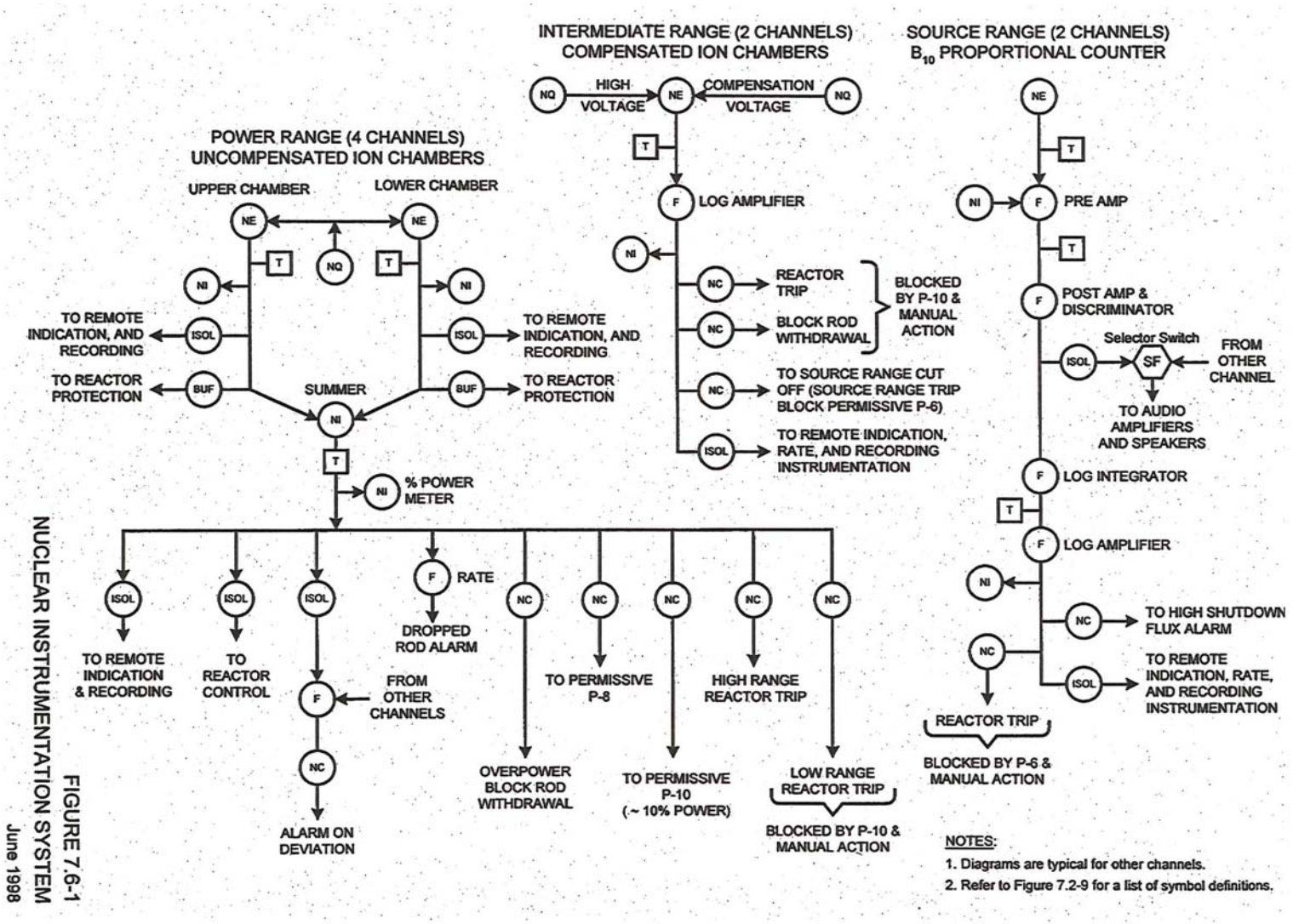


Figure 7.6-2 NEUTRON DETECTORS AND RANGE OF OPERATION

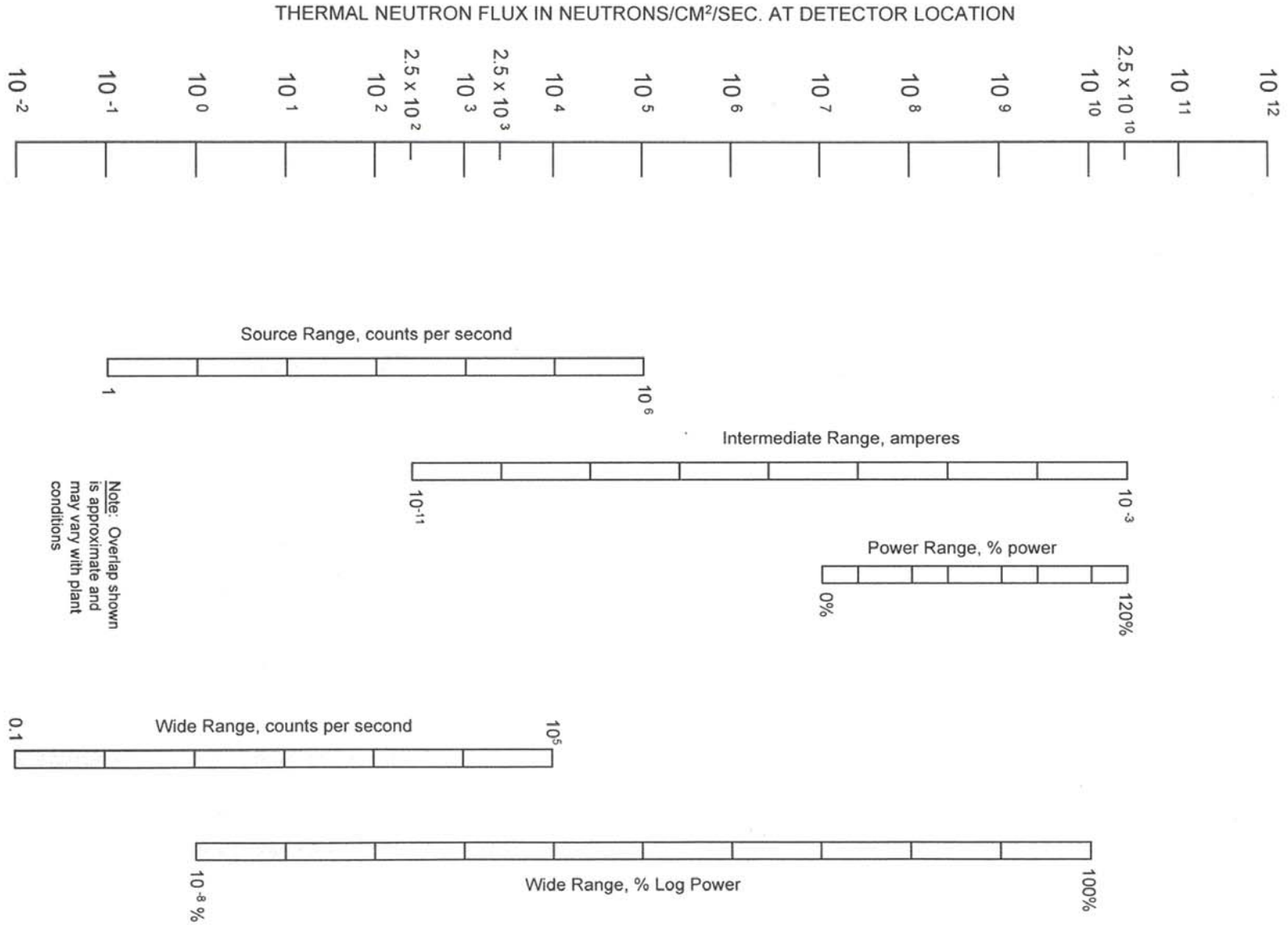


Figure 7.6-3 EX-CORE DETECTOR LOCATIONS RELATIVE TO CORE

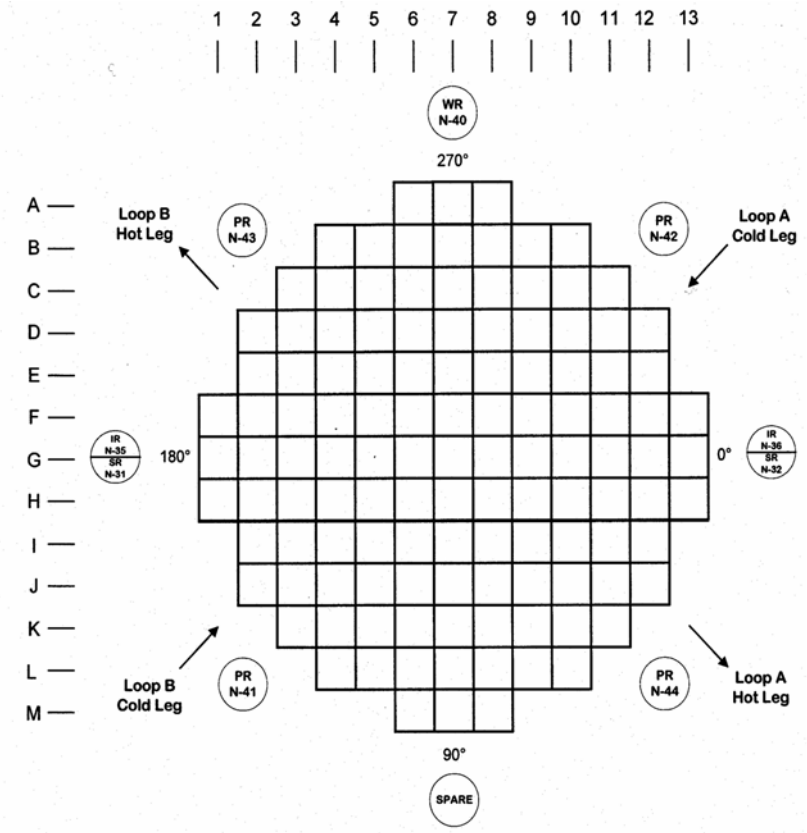


Figure 7.6-4 IN-CORE INSTRUMENTATION - DETAILS

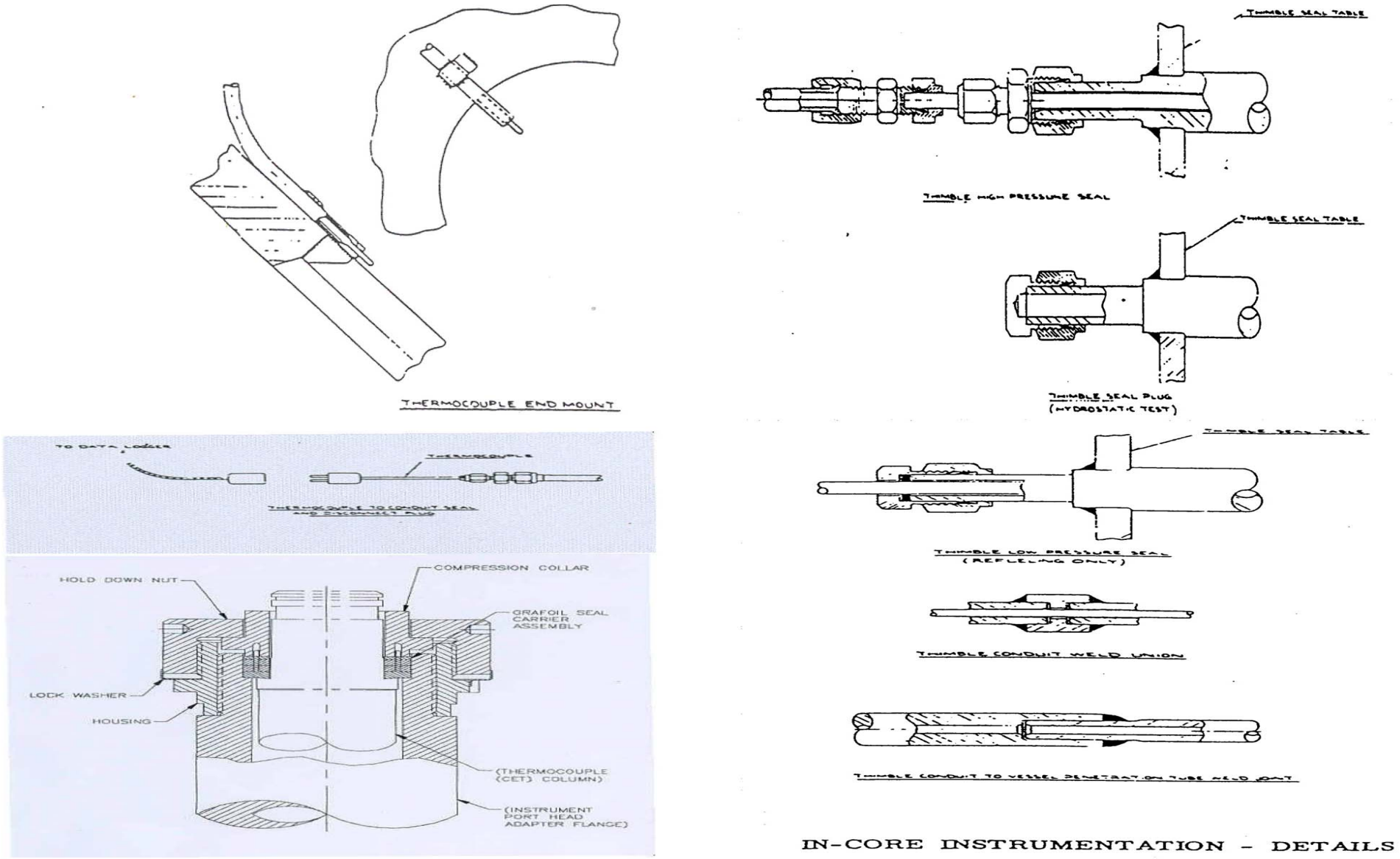
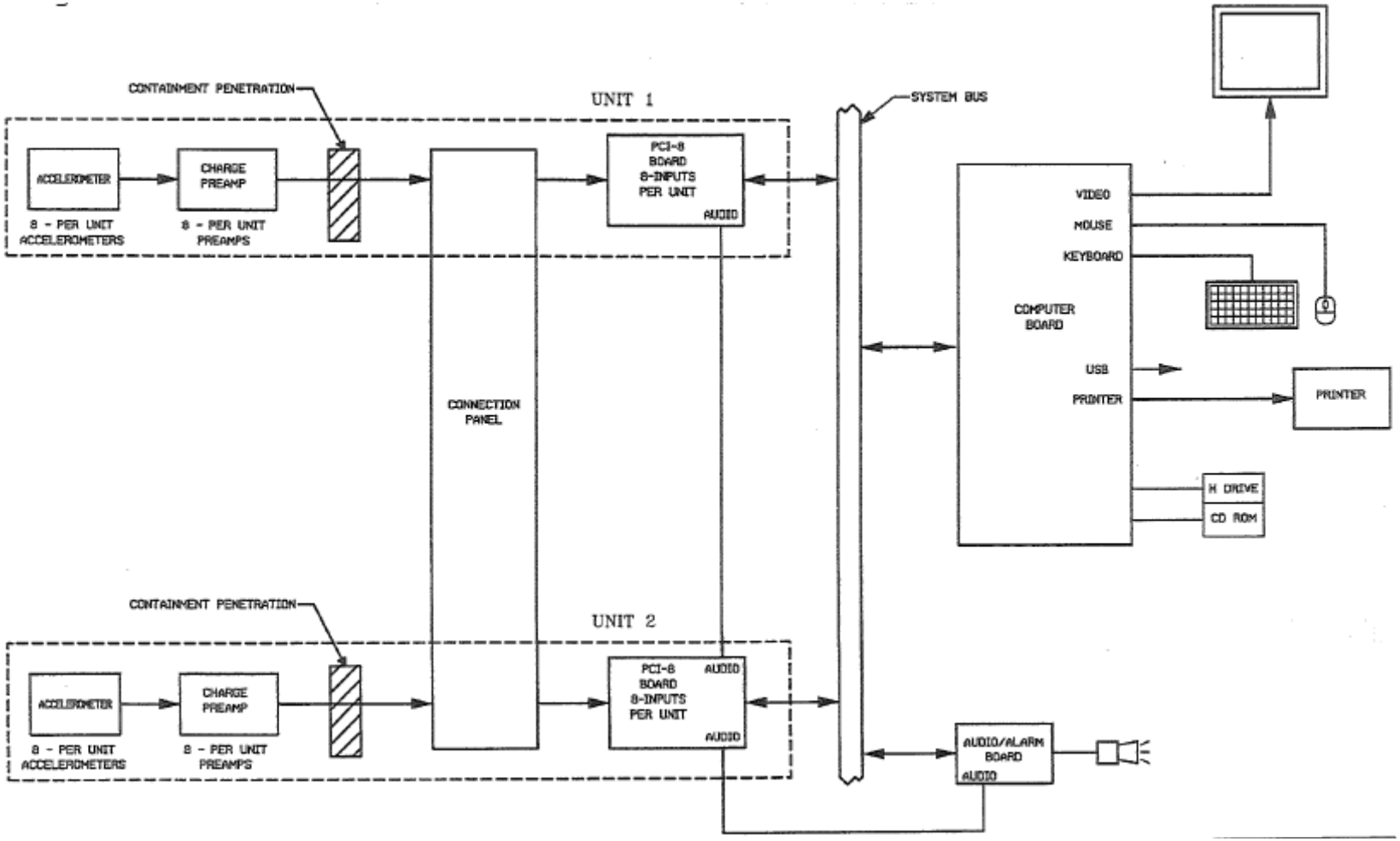


Figure 7.6-5 BLOCK DIAGRAM OF THE LOOSE PARTS MONITORING SYSTEM



7.7 CONTROL SYSTEMS

The basic control system design requirement is to maintain essential reactor facility operating variables within prescribed operating ranges for steady-state operation and for the designed load perturbations, to prevent unnecessary reactor trips.

The control systems are designed to operate as stable systems over the full range of automatic control throughout core life without requiring operator adjustment of setpoints other than the normal calibration procedures. The following sections discuss these control systems.

7.7.1 ROD CONTROL SYSTEM

Overall reactivity control is achieved by the combination of "chemical shim," which is accomplished by injecting boron into the reactor coolant system in the form of boric acid, and RCCAs (Rod Cluster Control Assemblies), also referred to as control rods. Long-term regulation of core reactivity is accomplished by adjusting the concentration of boron in the reactor coolant system, via the chemical and volume control system, which is discussed in Chapter 9.0. Short-term reactivity control for power changes or reactor trip is accomplished by movement of the control rods. Refer to Chapter 3.0 for the design requirements associated with the RCCAs.

The function of the rod control system is to provide automatic control of the control rods during power operation of the reactor. The rod control system uses input signals from different plant parameters, including neutron flux, reactor coolant temperature, and plant turbine load to maintain an average reactor coolant temperature (T_{avg}). T_{avg} increases linearly from zero power to full power.

The rod control system will compensate for reactivity changes caused by fuel depletion and/or xenon transients. Final compensation for these two effects is made by adjusting the boron concentration. The control system then readjusts the control rods in response to changes in T_{avg} resulting from changes in boron concentration.

The rod control system is designed to allow the reactor to follow load changes automatically when the plant output is above approximately 15% 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% and a ramp increase of 5% per minute within the load range of 15% to 100% without a reactor trip, subject to possible xenon limitations. Similar step and ramp load reductions are possible within the range of 100% to 15% of nominal power. The condenser steam dump control system, which is discussed in Section 7.7.2, permits the plant to accept a 50% rapid load decrease at a rate of 200% per minute without a reactor trip. The reactor control system is capable of restoring T_{avg} to within the programmed temperature deadband, following any of the above changes in load. A simplified block diagram of the reactor control system is shown in Figure 7.7-1.

Any unexpected change in the position of the control group under automatic control or a change in reactor coolant temperature under manual control provides a direct and immediate indication of a change in the reactivity status of the reactor. In addition, periodic samples of reactor coolant are

taken to monitor boron concentration. The variation in concentration during core life provides a further check on the reactivity status of the reactor including core depletion.

7.7.1.1 System Design

a. RCCA Grouping

There are 33 RCCAs. The rods are divided into two groups:

- a shutdown group comprising one bank of 8 rod clusters and one bank of 4 rod clusters, and
- a control group comprising 4 control banks (A, B, C, and D), which contain 8, 4, 5, and 4 rod clusters, respectively. Figure 3.2-1 shows the location of the rods in the core.

The four control group banks are the only rods that can be manipulated under automatic control. Two banks are divided into subgroups to obtain smaller incremental reactivity changes. All RCCAs in a subgroup are electrically paralleled to step simultaneously. Position indication for each RCCA type is the same. The drive mechanisms used in conjunction with the shutdown and control RCCAs are the same and are capable of permitting free fall of the assemblies.

1. Shutdown Groups

   The shutdown groups, together with the control groups, are capable of shutting the reactor down. They are used in conjunction with the adjustment of the chemical shim and the control groups to provide a shutdown margin of at least 1% $\Delta k/k$ following a reactor trip, even if the rod with the greatest rod worth is fully withdrawn. The shutdown margin varies over core life. The maximum shutdown margin is required at the end of core life and is based on the value used in the steam line break accident analysis.

   The shutdown groups are manually controlled during normal operation and are moved at a constant speed. Any reactor trip signal causes them to insert into the core. They are fully withdrawn during power operation and are withdrawn first during startup. Criticality is always approached with the control groups after withdrawal of the shutdown groups.

2. Control Groups

   The control groups are divided into four banks (A, B, C and D), with two banks further divided into two subgroups, to allow the system to follow load changes over the full range of power operation. Each subgroup in a bank is driven by the same variable speed rod drive control unit which moves the subgroups 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 T_{avg} about a small temperature deadband.

The operator is able to select either automatic or manual control. In either case, significant motion of the control banks can only be accomplished in their normal sequence, but with some overlap as one bank approaches its fully withdrawn position and the next bank begins to withdraw. The overlap between successive control banks is provided to compensate for low differential rod worth near the top and bottom of the core.

Manual control is provided to move a control bank in or out at a pre-selected fixed speed. Only a single bank of rods can be selected at a time during manual control. This is accomplished with a multi-position switch that allows only one bank to be selected.

Proper sequencing of the control rods is assured by; (1) automatic programming equipment in the rod control system, and (2) through administrative control.

Startup of the plant is accomplished by first manually withdrawing the shutdown rods to the full out position. This action requires that the operator select the SHUTDOWN BANK position on a control board mounted selector switch and then position the IN-HOLD-OUT lever (which will spring return to the HOLD position) to the OUT position.

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

The automatic programming equipment is set so that when the first bank being withdrawn reaches a preset position near the top of the core, the second bank begins to move out simultaneously with the first bank. This staggered withdrawal sequence continues until the plant reaches the desired power level. The staggered insertion sequence is the opposite of the withdrawal sequence, such that 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 be made without rewiring the programmer.

b. Interlocks

Interlocks (permissives), designed to meet the single failure criterion, are provided to preclude simultaneous withdrawal of more than one group of control and shutdown rods except in the overlap regions.

The control rod groups used for automatic control are interlocked with measurements of turbine-generator load to prevent automatic control rod withdrawal below 15% of nominal power. The manual and automatic controls are further interlocked with measurements of nuclear flux and ΔT to prevent approaching an overpower condition. See Table 7.2-2 for a listing of the interlocks.

c. Rod Stops

Rod stops are provided to block the withdrawal of the RCCAs to prevent an unnecessary reactor trip or an abnormal condition from increasing in magnitude. Rod stop contacts are located in the rod control logic cabinet and in the rod speed control analog rack.

A list of rod stops is given in Table 7.7-1. Some of these have been previously noted under the interlocks in Table 7.2-2, but are listed again for completeness.

d. Rod Drive Control

The control banks are driven by a sequencing, variable speed rod drive programmer. In a control bank of RCCAs, control subgroups (each containing a small number of RCCAs) are moved sequentially in a cycle such that all subgroups are maintained within one step of each other.

The sequence of motion is reversible, such that withdrawal sequence is the reverse of the insertion sequence. The sequencing speed is proportional to the control signal from the rod control system. This provides control group speed proportional to the demand signal from the rod control system.

The rod drive mechanism control center receives the signals from the programmer and actuates the Silicon Control Rectifiers (SCRs), which are in series with the coils of the rod drive mechanisms, allowing the control rods to move. The power to the coils is supplied through the two reactor trip breakers, which are discussed in Section 7.2.

The rod control system maintains a programmed T_{avg} by providing speed and direction signals to the control banks, based on High T_{avg} and power mismatch signals. Refer to Figure 7.7-1 for the following descriptions:

1. High T_{avg} Signal

   The average reactor coolant temperature is used to maintain the programmed T_{avg} as accurate as possible. The reactor coolant temperatures are measured by the hot leg and the cold leg reactor protection system resistance temperature detectors (RTDs), which provides two average temperature measurements per loop. The highest of four measured average reactor coolant temperature (HI T_{avg}) is the main control signal. This signal is sent through a lead/lag compensation unit to the T_{avg} summing circuitry where it is compared with the power mismatch signal and the reference average reactor coolant temperature T_{ref}, which is based on turbine first stage pressure and represents turbine power.

   The HI T_{avg} signal is also supplied to the condenser steam dump control system, which is discussed in Section 7.7.2.

2. Power Mismatch Signal

   A power mismatch signal is also employed as a control signal to improve the plant performance. The nuclear power is determined from the signals of the four reactor trip system power range neutron flux instrumentation. The average of the four power range signals is used as the control signal. The power mismatch signal is determined from a comparison of the average nuclear flux signal and the turbine first stage pressure signal, which represents turbine power.

The power mismatch signal is sent to a variable gain unit, which increases the signal based on turbine power. This serves to speed up system response and reduce transient peaks. This signal is

sent to the T_{avg} summing circuitry where it is compared with the HI T_{avg} signal and the reference average temperature T_{ref}, which is based on turbine power.

The above signals are combined by the summing circuitry and the output signal is used to control the direction and speed of control groups, to maintain T_{avg} at its programmed setting.

e. Control Group Rod Insertion Limits

The control group rod insertion limits ensure that the control rods are withdrawn far enough to provide the necessary shutdown margin to achieve hot shutdown following a reactor trip at any time, assuming that the highest worth control rod remains fully withdrawn.

The rod insertion limits, Z_{LL}, are calculated as a linear function of power. The equation is:

$$Z_{LL} = A\ (\Delta T)_{avg} + C$$

where A is a preset manually adjustable gain and C is a preset manually adjustable bias. The $(\Delta T)_{avg}$ is the average of four ΔT measurements based on the reactor coolant hot leg (T_{HOT}) and the cold leg (T_{COLD}) temperatures.

An insertion limit monitor with two alarm setpoints is provided for control banks B, C and D. A single "Bank A Not Fully Withdrawn" alarm is provided for Bank A. A description of control and shutdown rod groups is provided in Section 7.7.1.1. The "Low" alarm alerts the operator of an approach to a reduced shutdown reactivity situation requiring boron addition. If the actuation of the "Low-Low" or "Bank A Not Fully Withdrawn" alarm occurs, the operator should take immediate action to add boron to the system as necessary.

f. RCCA Position Indication

No direct method for monitoring the boron concentration in the reactor coolant system is provided; therefore, the reactivity status of the core is determined by monitoring the position of the control rods in relation to plant power and T_{avg} when the reactor is critical. 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, as described above, to alert the operator to take corrective action in the event a control group approaches or reaches its lower limit.

Two separate systems are provided to measure and display control rod position:

1. Analog System

This system derives the position signal directly from measurements of the drive rod position utilizing a linear variable differential transmitter (LVDT) as a detector. An analog signal is produced for each RCCA by the LVDT. An electrical coil stack is placed above the stepping mechanisms of the control rod magnetic jacks, and is external to the pressure housing.

The drive shaft varies the amount of coupling between the primary and secondary windings of the coils and generates an analog signal proportional to rod position. When the associated control rod

is at the bottom of the core, the magnetic coupling between the primary and secondary windings is small and there is a small voltage induced in the secondary winding. 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. The LVDT signal is conditioned and displayed on individual meters mounted on the control board and on the Plant Computer display.

Direct, continuous readout of every RCCA position is presented to the operator by individual meters. Since each RCCA is provided with a separate indication, no manipulation is required to determine rod position. In addition, the individual rod position signals are provided to the plant computer, which provides additional indication and alarms. The analog Rod Position Indication displayed on the plant computer may be used to satisfy Technical Specification surveillance requirements.

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 bank demand position signal counts pulses generated in the rod drive control system. Readout of the bank demand position is provided from an add-subtract pulse counter, which measures the number of steps that the rods are withdrawn. One bank demand counter is associated with each group (or subgroups) of RCCAs. These readouts are mounted on the control panel.

The reactor operator can compare the digital and analog readings upon receiving a rod deviation alarm. Since the digital and analog systems are separate systems, with each serving as a backup for the other, a single failure in rod position indication does not, in itself, lead the operator to take erroneous action in the operation of the reactor.

g. Rod Deviation

Both the actual rod position (analog system) and the demand position signals (digital system) are monitored by a rod deviation monitoring system. A deviation monitor alarm within the computer is actuated if an individual rod deviates from its subgroup position by a pre-selected distance.

h. Dropped Rod Indication

Two independent and diverse systems are provided to sense a dropped rod:

- a system which senses sudden reduction in out-of-core neutron flux, and
- a rod bottom position detection system.

The primary indication for a dropped RCCA is provided by use of the out-of-core power range nuclear detectors. A backup indication for a dropped RCCA is the rod bottom signal derived from each rod's individual position indication system. With the position indication system, dropped RCCA indication is not dependent on location, reactivity worth or power distribution changes.

The rod drop detection circuit, which is based on neutron flux, consists of a comparison of each of the four power range ion chamber signals with the same signal taken through a first order lag network. Since a dropped RCCA will rapidly depress the local neutron flux, the decrease in flux will be detected by one or more of these circuits. Such a sudden decrease in the power range ion chamber current will be seen as an error signal. Figure 7.6-1 indicates schematically the nuclear instrumentation system, including the dropped RCCA alarm.

i. Rod Drive Power Supply

The control rod drive power supply system consisting of a single scram bus configuration has been successfully employed on all Westinghouse PWR plants. Potential fault conditions with a single scram bus system are discussed in WCAP-90120L. The unique characteristics of the latch-type mechanisms with its relatively large power requirements with the redundant series reactor trip breakers make this system particularly desirable.

The solid state rod control system is operated from two parallel connected 400 kVA generators which provide 260 volt line-to-line, three-phase, four-wire power to the rod control circuits through the two series connected reactor trip breakers. This AC power is distributed from the reactor trip breakers to a lineup of identical solid state power cabinets using a single overhead run of enclosed bus duct which is bolted to, and therefore comprises part of, the power cabinet arrangement. Alternating current from the motor-generator sets is converted to a profiled direct current by the power cabinet and is then distributed to the control rod drive mechanisms (see Figure 7.7-2). A detailed description of the control rod drive power supply is available in "Topical Report, Solid State Rod Control System, Full Length," WCAP-90120L, January 1970 (Westinghouse Proprietary, Class 2).

1. Maintenance Holding Supply

   Each complete rod control system includes a single 70-volt DC power supply, which is used for holding the rod mechanisms in position during maintenance of the normal power supply. This DC power supply and associated switches have been provided to avoid the need to bring a separate DC power source to the rod control system during maintenance on the power cabinet circuits.

   This 70 volt supply, which receives its input from the AC power source downstream of the reactor trip breakers, is distributed to each power cabinet and permits holding of the rod mechanisms in groups of four by manually positioning switches located in the power cabinets. The 30 ampere output capacity limits the holding capacity to eight rods.

2. Trip Breaker Arrangement

   The trip breakers are arranged in the reactor trip switchgear in individual metal enclosed compartments. The 1,000 amp bus work, which makes up the connections between the reactor trip breakers, is separated by metal barriers to prevent the possibility that any conducting object could short circuit, or bypass, the reactor trip breakers contacts.

3. Reactor Trip

   Power to the rod drive mechanisms is interrupted by opening either of the reactor trip breakers. The 70 volt DC maintenance supply is also interrupted, since this supply receives its power through the reactor trip breakers.

7.7.1.2 Generic Letter 93-04

Generic Letter 93-04, "Rod Control System Failure and Withdrawal of Rod Cluster Assemblies," was issued to all licensees with Westinghouse rod control systems. The letter discussed a potential single failure concern with the rod control system as a result of an event at another plant. In response to the generic letter, PBNP submitted a summary of the applicability of WCAP -13803, "Generic Assessment of Asymmetric Rod Cluster Control Assembly Withdrawal," in support of the conclusion that DNB would not have occurred for the worst-case asymmetric rod withdrawal (Reference 1). PBNP also modified the rod control system logic timing in accordance with Westinghouse recommendations and committed to implement enhanced rod control system surveillance testing which meets the intent of Westinghouse Owners Group MUHP 6002, "Recommended Rod Control Surveillance Test." The PBNP surveillance is equivalent to MUHP 6002 Test C; is capable of detecting timing, communication, and regulation failures; and is performed each refueling outage (Reference 2 and Reference 3). The NRC determined that the corrective actions implemented by PBNP in response to GL 93-04 were acceptable (Reference 4).

7.7.2 CONDENSER STEAM DUMP CONTROL

The function of the Condenser Steam Dump (turbine bypass) Control System is to:

- Permit the acceptance of sudden large load decreases without a reactor trip,
- Remove stored energy and residual heat following a reactor trip without actuation of the steam generator safety valves with the plant at equilibrium no-load condition,
- Permit a controlled cooldown to cold shutdown, and
- Provides a means of controlling plant temperature during startup and hot shutdown.

The condenser steam dump system is provided to increase plant operating flexibility for large load reductions of up to 50% of full power at a rate up to 200% per minute. The condenser steam dump system removes steam to reduce the transient imposed upon the reactor coolant system. The control rod system can then reduce the reactor power to a new equilibrium value without causing overtemperature and/or overpressure conditions, which would result in a reactor trip. The condenser steam dump system controls the steam dump valves discussed in Section 10.1.2.

Condenser steam dump can be controlled either by T_{avg} in the automatic mode or main steam header pressure in the manual mode:

7.7.2.1 Automatic Control

In the Automatic Control mode, condenser steam dump is controlled by the error signal between the HI T_{avg} signal, described in Section 7.7.1.1, and the programmed reference temperature (T_{ref}), which is based on turbine first stage pressure (turbine power).

For sudden small changes in load, a difference (error) will exists between the Hi T_{avg} signal and T_{ref}, which will cause the steam dump valves to modulate open. The condenser steam dump flow decreases proportionally as the control rods act to reduce T_{avg} to restore it to within the programmed value of T_{ref}. A deadband is provided to allow the control rods to attempt to control T_{avg} prior to actuating condenser steam dump.

For larger sudden load changes or turbine trips, the error between the Hi T_{avg} signal and T_{ref} becomes larger, which results in the dump valves tripping full open. This allows the sensible heat stored in the reactor coolant to be removed by controlling the steam dump to the condenser and supplying feedwater to the steam generators without actuating the steam generator safety valves. After a reactor and turbine trip the reactor coolant system temperature is reduced to the no-load condition and may be maintained by the steam dump to the condensers, which removes the residual heat.

7.7.2.2 Manual Control

In the Manual Control mode, steam dump is controlled by main steam header pressure. This mode is used for long term removal of residual heat at hot shutdown, or during plant startups or cooldowns.

7.7.3 PRESSURIZER CONTROL

The pressurizer has two separate control systems, which are described below:

7.7.3.1 Pressurizer Pressure Control

The pressurizer pressure control system acts to maintain the reactor coolant pressure within the normal operating band in order to prevent DNB on low pressure and to protect the reactor coolant system from overpressurization due to high pressure. Pressure is controlled by electric immersion heaters, spray valves and power-operated relief valves (PORVs).

The pressurizer pressure is programmed to be controlled to a specified pressure and initiates methods of increasing or decreasing pressure based on the comparison of the programmed value to the measured pressure.

Pressure is normally maintained by automatic control of the heaters, which are located near the bottom of the pressurizer. The heaters are energized and de-energized based on pressurizer pressure, such that the heaters are energized on decreasing pressure and de-energized on increasing pressure. A variable heater is proportionally controlled to correct for small pressure variations due to heat losses, including the heat loss due to a small continuous spray. A small continuous spray is normally maintained to reduce thermal stresses and thermal shock, and to help maintain uniform water chemistry and temperature in the pressurizer. The backup heaters are energized when pressurizer pressure signal is below a given value.

During steady-state operation, the heaters will be energized and de-energized to maintain the programmed pressure value. On decreasing pressure, the heaters are energized. The energization of the heaters cause boiling of the water in the pressurizer, which generates steam and increases the vapor pressure (steam bubble) in the pressurizer, thereby increasing system pressure to the programmed value. On increasing pressure the heaters are de-energized. If system pressure continues to increase, the spray valve, which is located at the top of the pressurizer, will modulate open and inject subcooled water to condense the steam, thereby reducing the system pressure to the programmed value. The spray rate increases proportionally with pressure until it reaches a maximum value.

Changes in plant load can result in changes in the average reactor coolant temperature (T_{avg}), which will either result in decreases or increases in pressure.

Increases in plant loads result in decreases of T_{avg}, which result in an increase in reactor coolant density and a decrease in volume. The decrease in reactor coolant volume results in an outsurge of reactor coolant from the pressurizer, which expands the steam bubble and decreases system pressure. The difference between the programmed pressure and measured pressure will result in the energization of the heaters and the increase in vapor pressure (steam bubble).

Decreases in plant loads result in increases of T_{avg}, which result in a decrease in reactor coolant density and an increase in volume. The increase in reactor coolant volume results in an insurge of reactor coolant into the pressurizer, which compresses the steam bubble and increases system pressure. The difference between the programmed pressure and measured pressure will cause the variable heaters to de-energize and result in the opening of the spray valve, which will condense the steam bubble.

Large reductions in plant loads can result in increases of pressure until it increases to the point at which the two PORVs would open to limit the system pressure to 2,335 psig and allow the pressure in the system to decrease back to the steady-state operating value. Two-out-of-two pressure channels must be above the pressure setpoint to open each PORV. Two spring-loaded safety valves limit the system pressure to 2,485 psig following a complete loss of load without a direct reactor trip or steam dump (turbine bypass).

7.7.3.2 Pressurizer Level Control

The pressurizer level control system monitors the level and automatically maintains the level at a variable programmed value. The level control system varies the charging pump speed to maintain the programmed variable level.

Changes in load result in changes in pressurizer volume. Rather than maintaining a constant level in the pressurizer, level is programmed to be a function of the high average reactor coolant temperature (High T_{avg}). This function will minimize the water inventory adjustments associated with charging and letdown and 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.

7.7.4 STEAM GENERATOR CONTROL

The steam generator level is controlled in order to insure the proper water inventory for various operational and possible accident conditions. The control is achieved by varying feedwater flowrate. The feedwater system is discussed in Section 10.1.

Steam generator level is controlled by two means:

7.7.4.1 Main Feedwater Flow Control

The level in each steam generator is controlled by two programmable indicating controllers, one primary controller and one secondary controller. Each three-element control system continuously compares the feedwater flow signal, the steam generator water level signal and the main steam flow signal (see Figure 7.2-12), which is compensated by a steam pressure signal, and regulates its associated feedwater control valve accordingly. In the unlikely event of a failure of a primary controller, steam generator level control automatically transfers to the secondary controller and initiates a control room alarm. The 1st stage turbine pressure signal, which is proportional to reactor power, changes the controller response to enhance steam generator level stability at various reactor power levels. A failure of the 1st stage steam pressure signal high or low causes the controller to switch to pre-established default values. Two selectable feedwater flow and main steam flow signals are provided for each steam generator level controller

The controllers have the ability to operate in a "single element mode." In this mode, only the steam generator level signal inputs are used to control steam generator level. The single element mode allows the MFRV control system to modulate the MFRVs to maintain steam generator levels at low power. The controllers will automatically switch to single element mode if a steam flow or feedwater flow input fails off-scale high or low. Manual override of the feedwater controllers is also provided.

The three-element control system is overridden during the following by actuation of solenoid valves in the air supply to the valve actuators:

1. The main feedwater control valves close on a reactor trip signal to minimize the plant cooldown from the reactor trip transient.

2. In order to prevent excessive moisture carryover to the turbine caused by high steam generator level, a high-high level signal will override the control system and close the feedwater control valve. The signal is derived from a two-out-of-three coincidence logic. This override is automatically removed as the water level drops below the high-high setpoint.

3. A safety injection signal trips the main feedwater pumps and closes the MFRVs to minimize feedwater addition. This prevents additional cooldown and reduces containment pressure increase for the steam line rupture analysis (see Section 14.2.5).

Each feedwater flow channel is compared with a main steam flow channel for any mismatch above or below an adjustable value. An alarm is initiated if feedwater flow is greater than main steam flow. A reactor trip is initiated if feedwater flow is less than main steam flow coincident with low steam generator level. See Section 7.2.

7.7.4.2 Bypass Feedwater Flow Control

For low power operation of less than approximately 15% power, a bypass control valve may be used to control steam generator level. The bypass control valve is closed during normal power operation. The bypass control valve is controlled by a controller, which provides either automatic or manual control of the valve. In automatic control, the valve is modulated to control a programmed level based on the difference between the measured level and the referenced programmed level ($L - L_{ref}$).

The bypass valves are closed and prevented from opening either on a safety injection signal or on high steam generator level in the associated loop.

7.7.5 AUTOMATIC TURBINE LOAD RUNBACK

Automatic turbine load runback is initiated by an approach to an overpower or overtemperature condition prior to reaching the overpower and overtemperature ΔT trip setpoints. This feature prevents high power operation which could lead to a DNBR less than 1.30.

As identified in Section 7.2.2.2.e and Section 7.2.2.2.f, an automatic turbine runback is initiated when two-out-of-four channels indicate increasing overpower ΔT or overtemperature ΔT. The turbine runback acts by reducing the load reference setpoint of the turbine Electro-Hydraulic (E-H) controller by a preset amount. This is accomplished by reducing the setpoint at a constant rate for a present time in cycles, until the runback condition clears.

7.7.6 SYSTEM EVALUATION

7.7.6.1 Plant Stability

The rod control system is designed to limit the amplitude and the frequency of continuous oscillation of the average reactor coolant temperature (T_{avg}) about the control system setpoint within acceptable values. Continuous oscillation can be induced by a feedback control loop with a loop gain, which is either too large or too small with respect to the process transient response, such that the instability is induced by the control system itself. Because stability is more difficult to maintain at lower power under automatic control, automatic control is prevented below approximately 15% of power.

The control system is designed to operate as a stable system over the full range of automatic control throughout core life.

7.7.6.2 Step Load Changes Without Condenser Steam Dump (Turbine Bypass)

A typical power control requirement is to restore equilibrium conditions, without a plant trip, following a plus or minus 10% step change in load demand, over the 15 to 100% 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 rod control system is to avoid reactor trips by maintaining the average reactor coolant temperature (T_{avg}) deviation during the transient within a given value and to restore T_{avg} to the programmed setpoint 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 nuclear flux, pressurizer pressure, T_{avg}, and temperature rise across the core.

7.7.6.3 Loading and Unloading

Ramp loading and unloading is provided over the 15% to 100% power range under automatic control. The function of the control system is to maintain T_{avg} 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.

T_{avg} increases during loading and causes a continuous insurge to the pressurizer as a result of coolant expansion. The pressurizer spray limits the resulting pressure increase. Conversely, as T_{avg} is decreasing during unloading, there is a continuous outsurge 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 of T_{avg} so that a margin is provided for the overtemperature ΔT setpoint.

7.7.6.4 Loss of Load with Condenser Steam Dump (Turbine Bypass)

The reactor control system is designed to accept a net loss of electrical load below the permissive P-9 setpoint and a 50% rapid load reduction at a rate of 200% per minute from any power level, such that no reactor trip should be actuated. The automatic condenser steam dump system is able to accommodate this abnormal load rejection and to reduce the effects of the transient imposed upon the reactor coolant system. 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% of full power. Manual control must be used when the power is below this value. The reduction of steam dump flow is limited by the rate of inserting negative reactivity via control rods.

The ability of the plant to withstand the design load rejection without a trip was verified by analysis (Reference 6). The relieving capacity of the power-operated relief valves (PORVs) is adequate to limit the system pressure to prevent actuation of high pressure reactor trip for the 50% rapid load reduction. The PORVs are not challenged for a turbine trip without a reactor trip below the P-9 Setpoint.

7.7.6.5 Turbine Generator Trip with Reactor Trip

Whenever the turbine generator trips at an operating level above the P-9 permissive setpoint, the reactor also trips (see Section 7.2). The plant is operated with a programmed average reactor coolant temperature (T_{avg}) as a function of load, with the full load T_{avg} significantly greater than the saturation temperature corresponding to the steam generator pressure at the safety valve setpoint. The thermal capacity of the reactor coolant system is greater than that of the secondary system, and because the full load T_{avg} is greater than the no-load steam temperature, a heat sink is provided by the combination of controlled release of steam to the condenser, by makeup of cold

feedwater to the steam generators, and by relief through the atmospheric relief valves as necessary.

The condenser steam dump system is controlled from T_{avg} signal whose setpoint values are reset upon trip to the no-load value. Actuation of the condenser steam dump (turbine bypass) must be rapid enough to prevent actuation of the steam generator safety valves. With the condenser steam dump valves open, T_{avg} starts to reduce quickly to the no-load setpoint. A direct feedback of temperature acts to proportionally close the valves to minimize the total amount of steam which is bypassed.

Following the turbine trip, the steam voids in the steam generators will collapse and the main feedwater regulating valves will close following the reactor trip. The MFRV bypass valves will open to control steam generator level at their setpoint and auxiliary feedwater will actuate if the steam generator low-low level setpoint is reached.

Residual heat removal is maintained by the steam generator pressure controller (manually selected) which controls the amount of steam flow to the condensers. This controller operates the same condenser dump valves to the condensers which are used during the initial transient following turbine and reactor trip.

The pressurizer pressure and level fall rapidly during the transient because of coolant contraction. 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 energized to restore pressurizer pressure to normal.

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

7.7.6.6 Rod Control System Construction

The rod control system equipment is assembled in enclosed steel cabinets. Three phase power is distributed to the equipment through a steel enclosed bus duct, bolted to the cabinets. DC power connections to the individual mechanisms are routed to the reactor head area from the solid state cabinets through insulated cables, enclosed junction boxes, enclosed reactor containment penetrations, and sealed connectors. In view of this type of construction, any accidental connection of either an AC or DC power source, either internal or external to the cabinets, is not considered credible and were evaluated in WCAP-90120L, "Topical Report, Solid State Rod Control System, Full Length," dated January 1970 (Westinghouse Proprietary, Class 2).

7.7.7 REFERENCES

1. VPNPD-93-138, “Response to Generic Letter 93-04, Rod Control System Failure and Withdrawal of Rod Cluster Control Assemblies, Point Beach Nuclear Plant, Units 1 and 2,” dated August 5, 1993.

2. NRC Letter to WEPCo, "Request for Additional Information Regarding Generic Letter 93-04, Rod Control System Failure and Withdrawal of Rod Cluster Control Assemblies, 10 CFR 50.54(f), TAC Nos. M86858 and M86859," dated December 12, 1994.

3. NPL 95-0324, "Generic Letter 93-04, Rod Control System Failure and Withdrawal of Rod Cluster Control Assemblies, Additional Information, Point Beach Nuclear Plant, Units 1 and 2," dated July 13, 1995.

4. NRC Letter to WEPCo, "Resolution of Generic Letter 93-04, Rod Control System Failure and Withdrawal of Rod Cluster Control Assemblies, 10 CFR 50.54(f), Point Beach Nuclear Plant, Units 1 and 2, (TAC Nos. M86858 and M86859)" dated August 21, 1995.

5. NRC Safety Evaluation, PBNP Units 1 and 2 - Issuance of License Amendments Regarding Extended Power Uprate, May 3, 2011.

6. Westinghouse Calculation Note CN-CPS-08-20, EC10001/257453 Plant Operabiltiy Margin to Trip and EOC Coastdown Analysis for Point Beach Units 1 and 2 Extended Power Uprate, April 26, 2011.

Table 7.7-1 ROD STOPS

Rod Stop	Actuation Signal	Rod Motion to be Blocked
1. Nuclear Overpower	l/4 high power range neutron flux or l/2 high intermediate range neutron flux	Automatic and manual withdrawal
2. High ΔT	2/4 overpower ΔT or 2/4 overtemperature ΔT	Automatic and manual withdrawal
The actuation signals for item 2 also initiate a turbine load reduction		
3. Low Power	Low turbine load signal (below l5%) from low turbine impulse pressure	Automatic withdrawal

Figure 7.7-1 SIMPLIFIED BLOCK DIAGRAM OF REACTOR CONTROL SYSTEM

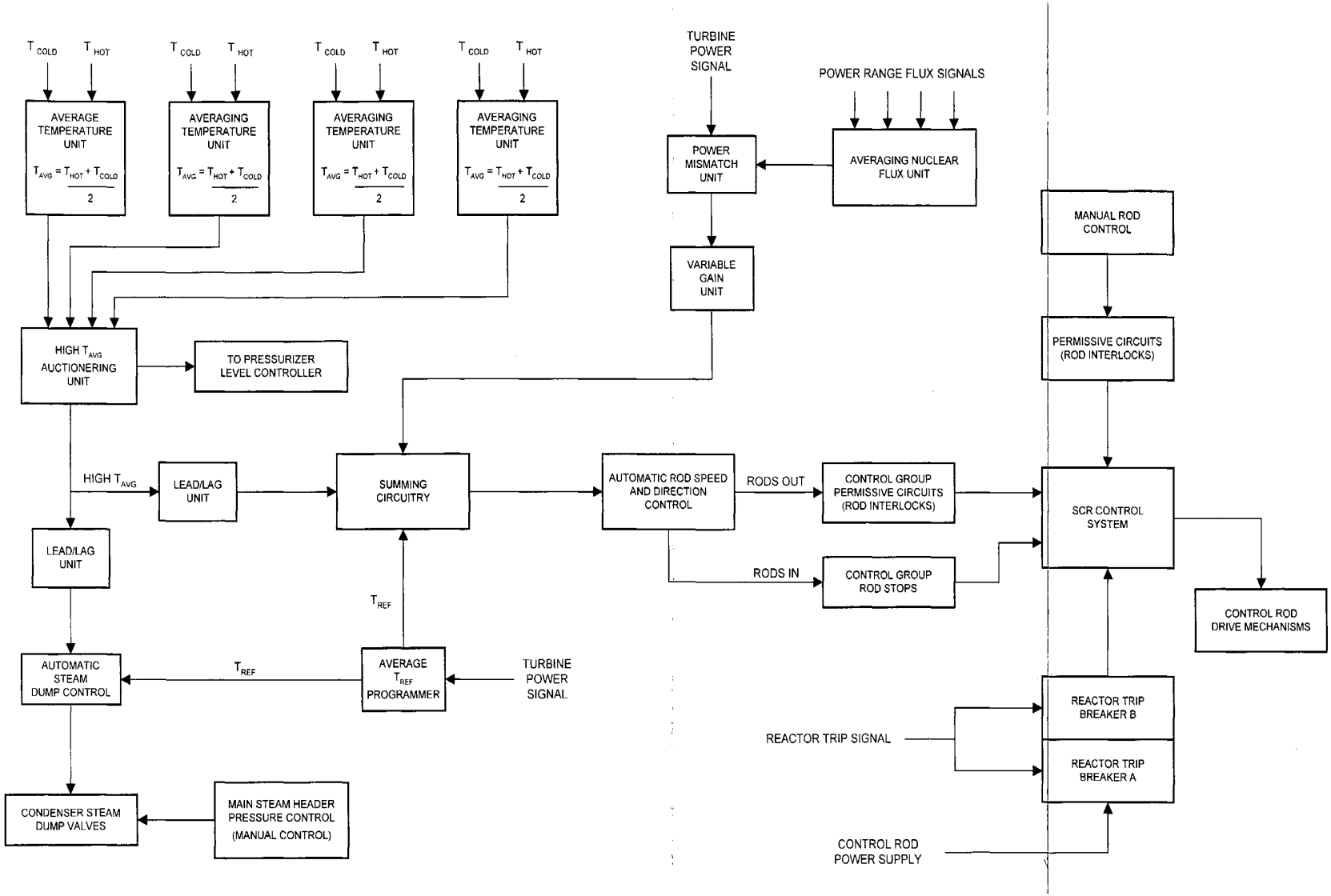


Figure 7.7-2 POWER SUPPLY TO ROD CONTROL EQUIPMENT AND CONTROL ROD DRIVE MECHANISMS