Table of Contents

List of Tables

List of Figures

THIS PAGE LEFT BLANK INTENTIONALLY.

7.0 Instrumentation and Controls

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.0.

THIS PAGE LEFT BLANK INTENTIONALLY.

7.1 Introduction

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

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

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

1. Definitions

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

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

   b. Module - Any assembly of interconnected components which constitutes an identifiable device, instrument, or piece of equipment. A module can be disconnected, removed as a unit, and replaced with a spare. It has definable performance characteristics which permit it to be tested as a unit. A module could be a card or other subassembly of a larger device, provided it meets the requirements of this definition.

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

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

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

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

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

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

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

j. Cold Shutdown Condition - When the reactor is subcritical by at least 1 percent $\Delta k/k$ and $T_{avg} \leq 200°F$.

k. Hot Shutdown Condition - When the reactor is subcritical by at least 1% $\Delta K/K$ and is at 0% Rated thermal power and $350°F > T_{avg} > 200°F$.

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

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

n. Trip Accuracy - The tolerance band containing the highest expected value of the difference between (a) the desired trip point value of a process variable and (b) the actual value at which a comparator trips (and thus actuates some desired result). This is the tolerance band within which a comparator must trip. It includes comparator accuracy, channel accuracy for each input, and environmental effects on the rack-mounted electronics. It comprises all instrumentation errors; however, it does not include any process effects such as fluid stratification.

o. Channel Accuracy - (a component of trip accuracy) includes accuracy of the primary element, transmitter and rack mounted electronics, but does not include indication accuracy.

p. Actuation Accuracy - Synonymous with trip accuracy, but used where the work “trip” may cause ambiguity.

q. Indication Accuracy - The tolerance band containing the highest expected value of the difference between (a) the value of a process variable read on an indicator or recorder and (b) the actual value of that process variable. An indication must fall within this tolerance band. It includes channel accuracy, accuracy of readout devices, and rack environmental effects, but not process effects such as fluid stratification.

r. Reproducibility - This term may be substituted for “accuracy” in the above definitions for those cases where a trip value or indicated value need not be referenced to an actual process variable value, but rather to a previously established trip or indication value; this value is determined by test.

7.1.1 Identification of Safety Related Systems

The instrumentation and control systems and supporting systems that are required to function to achieve the system responses assumed in the safety evaluation and those needed to shut down the unit safely are listed in Table 3-7.

Indicators provided for unit status are listed in Table 7-12 and Table 7-13.

7.1.1.1 Unit Comparison

The design and hardware for both protective systems for McGuire and Sequoyah Nuclear Stations supplied by Westinghouse are identical with certain exceptions.

1. Inputs to the Reactor Protection System from process sensors measuring turbine parameters are the responsibility of Duke.
2. Inputs to the Reactor Protection System from sensors detecting loss of reactor coolant pump are the responsibility of Duke.
3. Containment pressure sensors to initiate safeguards actuation from high Containment pressure are the responsibility of Duke.
4. Various safeguards final actuation device circuitry (i.e., Containment ventilation isolation, diesel generator start-up) are Duke's responsibility, where Westinghouse provides an output contact to the applicant's final actuation device.
5. The Containment Spray System is the responsibility of Duke.
6. Auxiliary Feedwater System is the responsibility of Duke.

All unit control systems on the McGuire Nuclear Station and the Sequoyah Nuclear Station within Westinghouse scope of supply are functionally identical with the exception of the steam dump system. The steam dump systems differ because Sequoyah is designed for 50 percent load rejection without trip whereas McGuire was designed for full net load rejection without trip. The difference is primarily one of system steam dump capacity with all other aspects being functionally identical between the two stations. The atmospheric dump valves were deleted at the McGuire Nuclear Station under NSM-12529 (Unit 1) and NSM-22529 (Unit 2) in 2002 and 2003, respectively. Subsequently, McGuire's design no longer supports a full net load rejection without a reactor trip.

The Non-1E portion of the Westinghouse Computer and Instrumentation Division (WCID) 7300 process control system was replaced at the McGuire Nuclear Station under EC 78241 (Unit 1) and EC 78243 (Unit 2), respectively. The replacement system is an Emerson/Westinghouse Ovation Distributed Control System (DCS).

There are other minor process control equipment supplier changes which do not affect protection or safeguards. Refer to Section 1.3 for additional comparison information.

7.1.2 Identification of Safety Criteria

7.1.2.1 Design Bases

The Westinghouse safety related systems in Chapter 7 comply with the following documents as discussed in the appropriate sections:

1. "General Design Criteria for Nuclear Power Plants," Appendix A to Title 10CFR Part 50, July 7, 1971.
2. Regulatory Guide 1.11 - "Instrument Lines Penetrating Primary Reactor Containment."
3. Regulatory Guide 1.22 - "Periodic Testing of Protection System Actuation Functions."

Periodic testing of the Reactor Trip and Engineered Safety Features Actuation Systems, as described in Sections 7.2.2 and 7.3.2, complies with NRC Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions." Under the present design, there are functions which fall under position D.4 of Regulatory Guide 1.22.

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

1. There is no practicable system design that would permit operation of the equipment without adversely affecting the safety or operability of the plant;
2. The probability that the protection system will fail to initiate the operation of the equipment is, and can be maintained, acceptably low without testing the equipment during reactor operation; and
3. The equipment can routinely be tested when the reactor is shut down.

   Where the ability of a system to respond to a bona fide accident signal is intentionally bypassed for the purpose of performing a test during reactor operation, each bypass condition is automatically indicated to the reactor operator in the main control room by a separate annunciator for the train in test. Test circuitry does not allow two trains to be tested at the same time so that extension of the bypass condition to redundant systems is prevented.
4. The Institute of Electrical and Electronic Engineers, Inc., “IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations,” IEEE Std. 279-1971.
5. The Institute of Electrical and Electronic Engineers, Inc., “IEEE Standard: Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations,” IEEE Std. 308-1971.
6. The Institute of Electrical and Electronic Engineers, Inc., “IEEE Standard for Electrical Penetration Assemblies in Containment Structures for Nuclear Fueled Power Generating Stations,” IEEE Std. 317-1971.
7. The Institute of Electrical and Electronic Engineers, Inc., “IEEE Trial-Use Standard; General Guide for Qualifying Class 1 Electric Equipment for Nuclear Power Generating Stations,” IEEE Std. 323-1971 as discussed in Section 3.11.
8. The Institute of Electrical and Electronic Engineers, Inc., “IEEE Trial-Use Guide for Type Tests of Continuous-Duty Class 1 Motors Installed Inside the Containment of Nuclear Power Generating Stations,” IEEE Std. 334-1971.
9. The Institute of Electrical and Electronic Engineers, Inc., “IEEE Standard Installation, Inspection, and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations,” IEEE Std. 336-1971.
10. The Institute of Electrical and Electronic Engineers, Inc., “IEEE Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems,” IEEE Std. 338-1971.

    The periodic testing of the Reactor Protection System and ESF Actuation System conform to the requirement of IEEE 338-1971 with the following comments:

    a. The periodic test frequency discussed in Paragraph 4.3 of IEEE 338-1971 and specified in the Technical Specifications, is conservatively selected to assure that equipment associated with protection functions has not drifted beyond its minimum performance requirements. If any protection channel appears to be marginal or requires more frequent adjustments due to plant conditions, the test frequency is increased to accommodate the situation until the marginal performance is resolved.

    b. The test interval discussed in Paragraph 5.2 is developed primarily on past operating experience and modified if necessary to assure that system and subsystem protection is

reliably provided. Analytic methods for determining reliability are not used to determine test interval.

Based on the scope definition given in IEEE 338-1971, no other systems described in Chapter 7 are required to comply with this standard.

11. The Institute of Electrical and Electronic Engineers, Inc., “IEEE Trial-Use for Seismic Qualification of Class 1 Electric Equipment for Nuclear Power Generating Stations,” IEEE Std. 344-1971. See Section 3.1.

The intent of the following documents is implemented as appropriate by Duke in the design of the control and instrumentation systems referred to in Section 7.1.1.

1. IEEE-279, “Criteria for Protection Systems for Nuclear Power Generating Stations” (1971).
2. IEEE-308, “Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations” (1971).
3. IEEE-317, “Electrical Penetration Assemblies in Containment Structures for Nuclear Generating Stations” (1971).
4. IEEE-323, “Trial-Use Guide for Qualifying Class 1 Electric Equipment for Nuclear Power Generating Stations” (1971).
5. IEEE-336, “Installation, Inspection, and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations” (1971).
6. IEEE-338, “Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems” (1971).
7. IEEE-344, “Trial-Use Guide for Seismic Qualification of Class 1 Electronic Equipment for Nuclear Power Generating Stations” (1971).
8. Regulatory Guide 1.22, “Periodic Testing of Protection System Actuation Functions.”

Duke conforms to the below listed AEC “General Design Criteria” (February 20, 1971) with the following exceptions:

1. Criterion 13, Instrumentation and Control

   Exception:

   As written, this criterion is not clear and subject to the misinterpretation that all instrumentation and control systems remain functional during and following accidents.

   Our interpretation is as follows:

   Instrumentation and control shall be provided for the systems which affect the fission process, integrity of reactor core, reactor coolant pressure boundary and Containment integrity. The instrumentation and control shall maintain the systems within acceptable ranges during normal operation and shall perform their respective safety related functions following an accident. Instrumentation shall be provided to monitor those variables required to assess reactor core integrity, safety system effectiveness and Containment environment following an accident.

2. Criteria 55 and 56

   Exception:

   Both criteria 55 and 56 contain the following paragraph:

"Isolation valves outside Containment shall be located as close to the Containment as practical and upon loss of actuating power, automatic isolation valves shall be designed to take the position that provides greater safety."

As written, this requirement cannot be interpreted since the conditions for "greater safety" is not defined. Also, since safety functions must meet the single failure requirement, the requirement to automatically assume a safe position is unnecessary, excessively limiting and unjustifiably complicating. For example, a momentary voltage dip during normal operation may be sensed as a loss of power. For some isolation valves, it is not desirable for them to assume their accident mode position, as this may cause severe perturbations to the unit operation even to the point of increasing the probability of an accident. An example is a steam line isolation valve which we do not want to close upon routine voltage transients.

Our interpretation of Criteria 55 and 56 is as follows:

"Isolation valves outside Containment shall be located as close to the containment as practical. Containment isolation provisions for lines requiring isolation shall perform the safety function assuming a single failure."

7.1.2.2 Independence of Redundant Safety Related Systems

7.1.2.2.1 Independence of Redundant Electrical Systems

The administrative responsibility for, and control over, the design and installation of these systems is as described in Chapter 17, and as applicable to other tasks. The Electrical Division of the Engineering Department has primary responsibility for the design, and design control is obtained through the implementation of departmental design control procedures. See Chapter 8 for evaluation of the physical layout of the electrical distribution system equipment. Independence concept is discussed throughout Chapter 7 where applicable.

7.1.2.2.2 Design Basis for Instrumentation Impulse Line Physical Separation

1. General Requirements

   The basic objective of impulse line separation is negation of damage to more than one redundant protection or safeguard transmitter impulse line as the result of any one incident.

   Incidents to be considered are missiles, pipe whip, high pressure jets, falling objects, etc.

   Note: The McGuire Protection Systems are separated into identified channels (I, II, III and IV). Impulse lines in the same channel can be routed together, but those of different channels must be separated.

2. Minimum Separation Requirements for Redundant Transmitter Impulse Lines

   The following precautions must be taken in routing the instrument impulse lines for the reactor protection system in order to meet the IEEE single failure criteria. It is necessary that such redundant transmitter impulse lines be physically separated at a minimum distance of eighteen inches (18") in any direction. Redundant transmitter impulse lines penetrating through walls must also be physically separated. In this case, if separate wall penetrations are not practical each redundant transmitter impulse line must be physically separated by conduit and/or other armor, when their penetration is to be made through a common opening in the wall.

   Spacing must be increased, or special shielding incorporated in areas where particular missiles or other hazards have been identified.

Safety related instrumentation impulse lines are protected from the dynamic effects of postulated piping ruptures as discussed in Section 3.6.5.

3. Requirements for Instrument Separation

   In general, if the impulse lines are properly separated in the area of the instrument, the instruments are properly separated. Caution should be exercised, however, to insure that adjacent high pressure impulse lines, test tees, instrument valves and manifolds do not constitute a hazard because of whip, valve system stem missiles or jet forces.

   Additional protection in the form of solid barriers must be provided to protect against accidental damage where a technician can be assumed to be servicing or repairing an adjacent redundant instrument.

   Strict adherence to the above minimum requirements will not necessarily produce an adequate system, however, these minimum requirements plus careful consideration of special areas will.

7.1.2.3 Physical Identification of Safety Related Equipment

There are four separate protection sets identifiable with process equipment associated with the Reactor Protection and Engineered Safety Features Actuation Systems. A protection set is comprised of more than a single process equipment rack. The color coding of each process equipment rack nameplate coincides with the color code established for the protection set of which it is a part. Redundant channels are separated by locating them in different equipment rack sets. Separation of redundant channels begins at the process sensors and is maintained in the field wiring, containment penetrations and equipment racks to the redundant trains in the logic racks. At the logic racks the protection set color coding for redundant channels is clearly maintained until the channel loses its identity in the redundant logic trains. The color coded nameplates described below provide identification of equipment associated with protective functions and their channel set association:

Protection Set	Color Coding
I	Red
II	White *
III	Blue
IV	Yellow *

* Channel II Source Range and Intermediate Range Nuclear Instrumentation (N32/N36) is color coded Yellow inside containment, through penetration E247, and up to the Channel II Amplifier Cabinet, 1/2ENBPN0002. The signal is then color coded White from the Channel II Amplifier Cabinet to the Channel II Nuclear Instrumentation.

Red is used to identify Train A and yellow is used to identify Train B.

All non-rack mounted protective equipment and components are provided with an identification tag or nameplate. Small electrical components such as relays have nameplates on the enclosure which houses them. All cables are numbered with identification tags.

For further details of the Process Control System, see Sections 7.2, 7.3, and 7.7.

For details of the Solid State Protective System, see Sections 7.2 and 7.3.

Differentiation between multi-unit safety related systems is provided by the prefix number on cable tags, nameplates, etc. The prefix number one (1) is used for Unit 1 and the number two (2) will be used for Unit 2.

7.1.2.4 Instrument Range Design Criteria

Three setpoints are specified.

1. Safety limit setpoint
2. Limiting setpoint
3. Nominal setpoint

The safety limit is the value assumed in the accident analysis and is the least conservative value.

The allowable value setpoint is the Technical Specification value and is obtained by subtracting a safety margin from the safety limit. The safety margin accounts for instrument error, process uncertainties such as flow stratification and transport factor effects, etc.

The nominal trip setpoint is the value set into the equipment and is obtained by subtracting allowances for instrument drift and calibration uncertainty from the allowable value setpoint. The nominal trip setpoint allows for the normal expected instrument setpoint drifts such that the Technical Specification limits will not be exceeded under normal operation.

Range selection for the instrumentation covers the expected range of the process variable being monitored during power operation. Limiting setpoints are at least 5% from the end of the instrument span.

Trip accuracy is defined in Section 7.1. Accuracies are given in Table 7-3 and Section 7.3.1.2.6. The trip setpoint is determined by factors other than the most accurate portion of the instrument's range. The safety limit setpoint is determined only by the accident analysis. As described above, allowance is then made for process uncertainties, instrument error, instrument drift, and calibration uncertainty to obtain the nominal setpoint value which is actually set into the equipment. The only requirement on the instrument's accuracy value is that over the instrument span, the error must always be less then or equal to the error value allowed in the accident analysis. There is no requirement that the instrument be the most accurate at the setpoint value as long as it meets the minimum accuracy requirement. The accident analysis accounts for the expected errors at the actual setpoint.

Deleted Per 2009 Update.

As Found/As Left Tolerance

RPS/ESFAS functions may have requirements stated in the Technical Specifications that operation of the channels will be gauged against the As-Found and As-Left Tolerances in accordance with TSTF-493 Rev. 4 (Ref. 5). For those specific functions, a specific methodology is used to determine the allowable calibration tolerances to further assure that the instrument channels are operating within the bounds defined in the Safety Analysis.

Deleted per 2015 update.

"As-Found" is the condition in which a channel, or portion of a channel, is found after a period of operation and before recalibration, if necessary. The As-Found Tolerance is the allowance that the channel, or portion thereof, is expected to be within based on uncertainty calculations which ensure the channel is capable of producing a trip prior to reaching the Safety Analysis Analytical Limit. Values recorded during a channel As-Found surveillance which are within the As-Found

Tolerance would clearly indicate a channel is operating as intended. Values recorded during a channel As-Found surveillance which exceed the As-Found Tolerance would be assessed to determine if the channel can continue to perform after adjustment within the bounds defined in the Safety Analysis.

Normally, the As-Found Tolerance would be equivalent to the errors verified during the surveillance. Therefore, the uncertainty terms which make up the As-Found Tolerance for the portion of the channel under surveillance would typically include the square root sum of squares combination of reference accuracy, drift and measurement and test equipment uncertainty effects (e.g. M&TE Uncertainty and M&TE Reading Resolution). Inclusion of additional uncertainty terms (e.g. normal radiation effect, tubing error effects) may be included but must be justified. Additionally, the uncertainty terms may be treated as bias if a random, independent correlation of the terms cannot be assured. As-Found Tolerances more conservative than the value calculated by this method may be used with appropriate justification.

"As-Left" is the condition in which a channel, or portion of a channel, is left after calibration or final setpoint device setpoint verification. The As-Left Tolerance is the acceptable setting variation about the setpoint that the technician may leave the setting following calibration.

Uncertainty terms which make up the As-Left Tolerance for the portion of the channel under surveillance would typically include the square root sum of squares combination of reference accuracy and measurement and test equipment uncertainty effects (e.g. M&TE Uncertainty and M&TE Reading Resolution). Inclusion of additional uncertainty terms (e.g. normal radiation effect, tubing error effects) may be included but must be justified. Additionally, the uncertainty terms may be treated as bias if a random, independent correlation of the terms cannot be assured. As-Left Tolerances more conservative than the value calculated by this method may be used without further justification.

7.1.2.5 NRC IE Bulletin 90-01 and Supplement 1

The NRC issued IE Bulletin 90-01, “Loss of Fill-Oil in Transmitters Manufactured by Rosemount,” on March 9, 1990. IE Bulletin 90-01 requested that licensees promptly identify and take appropriate corrective actions for Model 1153 Series B, Model 1153 Series D, and Model 1154 transmitters manufactured by Rosemount that may be leaking fill-oil. Duke's Bulletin response actions included identification of transmitters from the suspect lots for McGuire Nuclear Station which were in use in safety-related applications, review of applicable calibration records to inspect transmitters for loss of fill-oil behavior, and development of an enhanced surveillance program to monitor applicable transmitters for symptoms of loss of fill-oil. Additionally, the IE Bulletin 90-01 requested that upon identification of any suspect Rosemount transmitters in use in reactor protection or engineered safety features actuation systems, operability determinations be performed for this equipment until the equipment could be replaced. In its response (letter from H.B. Tucker to NRC, dated August 10, 1990) DPC found no suspect transmitters installed in the reactor protection or engineering safety features actuation systems of McGuire Nuclear Station.

The NRC issued Supplement 1 to IE Bulletin 90-01, “Loss of Fill-Oil in Transmitters Manufactured by Rosemount,” on December 22, 1992, providing further details on monitoring programs for the transmitters described in the original bulletin. Duke responded on May 24, 1993 by the letter from H.B. Tucker to the NRC. Subsequently, the NRC issued its Safety Eavluation Report (SER) on December 16, 1994 which provided approval and closeout of IE Bulletin 90-01 and Supplement 1 for the McGuire Nuclear Station.

7.1.3 References

1. Nuclear Regulatory Commission, Letter to All Holders of Operating Licenses or Construction Permits for Nuclear Power Reactors, from Charles E. Rossi, March 9, 1990, NRC Bulletin No. 90-01, “Loss of Fill-Oil in Transmitters Manufactured by Rosemount.”
2. Duke Power Company, Letter from H.B. Tucker to NRC, August 10, 1990, re: Response to NRC Bulletin No. 90-01, “Loss of Fill-Oil in Transmitters Manufactured by Rosemount.”
3. Duke Power Company, Letter from H.B. Tucker to NRC, May 24, 1993, re: Response to NRC Bulletin No. 90-01, Supplement 1, “Loss of Fill-Oil in Transmitters Manufactured by Rosemount.”
4. Nuclear Regulatory Commission, Letter from V. Nerses to T.C. McMeekin (DPC), December 16, 1994, “NRC Bulletin 90-01 Supplement 1, “Loss of Fill-Oil in Transmitters Manufactured by Rosemount.”
5. Technical Specifications Task Force (TSTF), TSTF-493, Revision 4, July 13, 2009, “Clarify Application of Setpoint Methodology for LSSS Functions.”

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.1.

7.2 Reactor Protection System

7.2.1 Description

7.2.1.1 System Description

The Reactor Protection System automatically keeps the reactor operating within a safe region by shutting down the reactor whenever the limits of the region are approached. The safe operating region is defined by several considerations such as mechanical/hydraulic limitations on equipment, and heat transfer phenomena. Therefore, the Reactor Protection System keeps surveillance on process variables which are directly related to equipment mechanical limitations, such as pressure, pressurizer water level (to prevent water discharge through safety valves, and uncovering heaters) and also on variables which directly affect the heat transfer capability of the reactor (e.g., flow, reactor coolant temperatures). Still other parameters utilized in the Reactor Protection System are calculated from various process variables. In any event, whenever a direct process or calculated variable exceeds a setpoint the reactor is shut down in order to protect against either gross damage to fuel cladding or loss of system integrity which could lead to release of radioactive fission products into the Containment.

The following subsystems make up the Reactor Protection System:

1. Process Instrumentation (Reference 1)
2. Nuclear Instrumentation System (Reference 2)
3. Solid State Logic Protection System (Reference 3)
4. Reactor Trip Switchgear (Reference 3)
5. Manual Actuation Circuit

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

Each of the two logic trains, A and B, is capable of opening a separate and independent reactor trip breaker, RTA and RTB, respectively. The two trip breakers in series connect three phase ac power from the rod drive motor generator sets to the rod drive power cabinets, as shown on Figure 7-1, Sheet 2. During unit power operation, a dc under-voltage coil on each reactor trip breaker holds a trip plunger out against its spring, allowing the power to be available at the rod control power supply cabinets. For reactor trip, a loss of dc voltage to the under-voltage coil releases the trip plunger and trips open the breaker. When either of the trip breakers opens, power is interrupted to the rod drive power supply, and the control rods fall, by gravity, into the core. The rods cannot be withdrawn until the trip breakers are manually reset. The trip breakers cannot be reset until the abnormal condition which initiated the trip is corrected. Bypass breakers BYA and BYB are provided to permit testing of the trip breakers, as discussed in Section 7.2.2.2.3.

The reactor trip breakers have been modified to further enhance the reliability of the breakers to trip on demand. The modification provides that the shunt trip device in each main reactor trip will be actuated by the automatic protection signals.

The design modification includes provisions to test the UV trip and the shunt trip device independently. The change applies only to the main trip breakers; the bypass breakers' functions are unchanged.

The modification involves adding a 48-Vdc relay in parallel with the UV trip device. An output contact of this relay is connected between the 125-Vdc supply and the shunt trip device, in parallel with the existing manual scram contact. Under normal plant conditions, the new relay is energized and its output contact is open. When plant conditions necessitate automatic protection and the 48 Vdc from the protection system is interrupted, the new relay will de-energize and its output contact will close to apply the 12 Vdc to actuate the shunt trip device.

Manual reactor scram capability is provided by two switches on the main control board in the control room. At the McGuire station, the manual scram switches are “channelized”; that is, the Train “A” manual scram switch operates the UV and the shunt trip of the reactor trip breaker “A”; the Train “B” switch, reactor trip breaker “B”. Either switch operates both the bypass breakers. Thus, diverse means (undervoltage trip attachments and shunt trip attachments) are used to open the reactor trip breakers on a manual reactor trip signal.

7.2.1.1.1 Functional Performance Requirements

The Reactor Protection System automatically initiates reactor trip:

1. Whenever necessary to prevent fuel rod damage for an anticipated operational transient (Condition II),
2. To limit core damage for infrequent faults (Condition III),
3. So that the energy generated in the core is compatible with the design provisions to protect the reactor coolant pressure boundary for limiting fault conditions (Condition IV).

The Reactor Protection System initiates a turbine trip signal whenever reactor trip is initiated. This prevents the reactivity insertion that would otherwise result from excessive reactor system cooldown and thus avoids unnecessary actuation of the Engineered Safety Features Actuation System.

The Reactor Protection System provides for manual initiation of reactor trip by operator action.

7.2.1.1.2 Reactor Trips

The various reactor trip circuits automatically open the reactor trip breakers whenever a condition monitored by the Reactor Protection System reaches a preset or calculated level. To ensure a reliable system, high quality design, components, manufacturing, quality control and testing is used. In addition to redundant channels and trains, the design approach provides a Reactor Protection System which monitors numerous system variables, therefore, providing protection system functional diversity. The extent of this diversity has been evaluated for a wide variety of postulated accidents and is detailed in References 6 and 7.

Table 7-1 provides a list of reactor trips which are described below.

1. Nuclear Overpower Trips

   The specific trip functions generated are as follows:

   a. Power range high neutron flux trip.

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

In each channel there are two independent bistables, each with its own trip setting used for a high and a low range trip setting. The high trip setting provides protection during normal power operation and the low trip setting provides protection during startup. The low trip setting can be manually bypassed when two out of the four power range channels read above approximately 10 percent power (P-10). When three out of the four channels are below 10 percent power, the low trip function automatically reinstates. Refer to Table 7-2 for a listing of all protection system interlocks.

b. Intermediate range high neutron flux trip

The intermediate range high neutron flux trip circuit trips the reactor when one out of the two intermediate range channels exceed the trip setpoint. This trip, which provides protection during reactor startup, can be manually blocked if two out of four power range channels are above approximately 10 percent power (P-10). Three out of the four power range channels below this value automatically reinstates the intermediate range high neutron flux trip. The intermediate range channels (including detectors) are separate from the power range channels. The intermediate range channels can be individually bypassed at the nuclear instrumentation racks to permit channel testing during plant shutdown or prior to startup. This bypass action is annunciated on the control board.

c. Source range high neutron flux trip

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

d. Power range high positive neutron flux rate trip

This circuit trips the reactor when an abnormal rate of increase in nuclear power occurs in two out of four power range channels. This trip provides DNB protection against rod ejection accidents of low worth from mid-power.

e. Figure 7-1, Sheet 3, shows the logic for all of the nuclear overpower and rate trips. A detailed functional description of the equipment associated with this function is given in Reference 2.

2. Core Thermal Overpower Trips

The specific trip functions generated are as follows:

a. Overtemperature ΔT trip

This trip protects the core against low DNBR and trips the reactor on coincidence as listed in Table 7-1 with one set of temperature measurements per loop. The trip (actual ΔT and setpoint) is continuously calculated by analog circuitry for each loop by solving the following equation:

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

Note: The above equation was revised in 1999 update.

Where:

ΔT is measured RCS ΔT by loop narrow range RTDs, °F.

ΔT_0 is the indicated ΔT at RTP, °F.

s is the Laplace transform operator, sec^{-1}.

T is the measured RCS average temperature, °F.

T' is the nominal T_{avg} at RTP, ≤ 585.1°F.

P is the measured pressurizer pressure, psig.

P' is the nominal RCS operating pressure, = 2235 psig

K_1 = Overtemperature ΔT reactor trip setpoint, as presented in the COLR,

K_2 = Overtemperature ΔT reactor trip heatup setpoint penalty coefficient, as presented in the COLR,

K_3 = Overtemperature ΔT reactor trip depressurization setpoint penalty coefficient, as presented in the COLR,

τ_1, τ_2 = Time constants utilized in the lead-lag controller for ΔT, as presented in the COLR,

τ_3 = Time constants utilized in the lag compensator for ΔT, as presented in the COLR,

τ_4, τ_5 = Time constants utilized in the lead-lag controller for T_{avg}, as presented in the COLR,

τ_6 = Time constants utilized in the measured T_{avg} lag compensator, as presented in the COLR, and,

$f_1(\Delta I)$ = a function of the indicated difference between top and bottom detectors of the power-range nuclear ion chambers; refer to Figure 7-1; with gains to be selected based on measured instrument response during plant startup tests such that:

(i) for $q_t - q_b$ between the "positive" and "negative" $f_1(\Delta I)$ breakpoints as presented in the COLR; $f_1(\Delta I) = 0$, where q_t and q_b are precent RATED THERMAL POWER in the top and bottom halves of the core respectively, and $q_t + q_b$ is total THERMAL POWER in percent of RATED THERMAL POWER;

(ii) for each percent imbalance that the magnitude of $q_t - q_b$ is more negative than the $f_1(\Delta I)$ "negative" breakpoint presented in the COLR, the ΔT Trip Setpoint shall be automatically reduced by the $f_1(\Delta I)$ "negative" slope presented in the COLR; and

(iii) for each percent imbalance that the magnitude of $q_t - q_b$ is more positive than the $f_1(\Delta I)$ "positive" breakpoint presented in the COLR, the ΔT Trip Setpoint shall be automatically reduced by the $f_1(\Delta I)$ "positive" slope presented in the COLR.

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

Increases in ΔI beyond a pre-defined deadband result in a decrease in trip setpoint. Refer to Figure 7-1.

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

Figure 7-1, Sheet 5, shows the logic for overtemperature ΔT trip function. A detailed functional description of the process equipment associated with this function is contained in Reference 1.

b. Overpower ΔT trip

This trip protects against excessive power (fuel rod rating protection) and trips the reactor on coincidence as listed in Table 7-1, with one set of temperature measurements per loop. The trip (actual ΔT and setpoint) for each channel is continuously calculated using the following equation:

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

Note: The above equation was revised in 1999 update.

Where:

ΔT is measured RCS ΔT by loop narrow range RTDs, °F.

ΔT_0 is the indicated ΔT at RTP, °F.

s is the Laplace transform operator, sec^{-1}.

T is the measured RCS average temperature, °F.

T" is the nominal T_{avg} at RTP, ≤ 585.1°F.

K_4= Overpower ΔT reactor trip setpoint as presented in the COLR,

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

K_6 = Overpower ΔT reactor trip heatup setpoint penalty coefficient as presented in the COLR for T > T' and K_6 = 0 for T ≤ T",

τ_1, τ_2 = Time constants utilized in the lead-lag controller for ΔT, as presented in the COLR,

τ_3 = Time constants utilized in the lag compensator for ΔT, as presented in the COLR,

τ_6 = Time constants utilized in the measured T_{avg} lag compensator, as presented in the COLR,

τ_7 = Time constant utilized in the rate-lag controller for T_{avg}, as presented in the COLR, and

f_2 (ΔI) = a function of the indicated difference between top and bottom detectors of the power-range nuclear ion chambers; with gains to be selected based on measured instrument response during plant startup tests such that:

(i) for $q_t - q_b$ between the "positive" and "negative" $f_2(\Delta I)$ breakpoints as presented in the COLR; $f_2(\Delta I) = 0$, where q_t and q_b are precent RATED THERMAL POWER in the top and bottom halves of the core respectively, and $q_t + q_b$ is total THERMAL POWER in percent of RATED THERMAL POWER;

(ii) for each percent imbalance that the magnitude of $q_t - q_b$ is more negative than the $f_2(\Delta I)$ "negative" breakpoint presented in the COLR, the ΔT Trip Setpoint shall be automatically reduced by the $f_2(\Delta I)$ "negative" slope presented in the COLR; and

(iii) for each percent imbalance that the magnitude of $q_t - q_b$ is more positive than the $f_2(\Delta I)$ "positive" breakpoint presented in the COLR, the ΔT Trip Setpoint shall be automatically reduced by the $f_2(\Delta I)$ "positive" slope presented in the COLR.

The source of temperature and flux information is identical to that of the overtemperature ΔT trip and the resultant ΔT setpoint is compared to the same ΔT. Figure 7-1, Sheet 5, shows the logic for this trip function. The detailed functional description of the process equipment associated with this function is contained in Reference 1.

3. Reactor Coolant System Pressurizer Pressure and Water Level Trips

The specific trip functions generated are as follows:

a. Pressurizer low pressure trip

The purpose of this trip is to protect against low pressure which could lead to DNB. The parameter being sensed is reactor coolant pressure as measured in the pressurizer. Above P-7 the reactor is tripped when the pressurizer pressure measurements (compensated for rate of change) fall below preset limits. The trip logic is automatically enabled above P-7. This signal is compensated to account for the fact that the measurement is in the pressurizer rather than in the core proper. This trip is blocked below P-7 because at low power levels the trip is not required. The trip logic and interlocks are given in Table 7-1.

The trip logic is shown on Figure 7-1, Sheet 6. A detailed functional description of the process equipment associated with the function is contained in Reference 1.

b. Pressurizer high pressure trip

The purpose of this trip is to protect the Reactor Coolant System against system overpressure.

The same sensors and transmitters that are used for the pressurizer low pressure trip are also used for the high pressure trip except that separate bistables are used for high pressure trip. These bistables trip when uncompensated pressurizer pressure signals exceed preset limits on coincidence as listed in Table 7-1. There are no interlocks or permissives associated with this trip function. This trip protests against overstressing the reactor coolant pressure boundary.

The logic for this trip is shown on Figure 7-1, Sheet 6. The detailed functional description of the process equipment associated with this trip is provided in Reference 1.

c. Pressurizer high water level trip

The purpose of this trip is to prevent water relief through the pressurizer safety valves and therefore provide for equipment protection. This trip is automatically blocked below

P-7 to permit startup. The coincidence logic and interlocks of pressurizer high water level signals are given in Table 7-1.

The trip logic for this function is shown on Figure 7-1, Sheet 6. A detailed description of the process equipment associated with this function is contained in Reference 1.

4. Reactor Coolant System Low Flow Trips

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

a. Low reactor coolant flow

The parameter sensed is reactor coolant flow. Four elbow taps in each coolant loop are used as a flow sensing device that indicates the status of reactor coolant flow. The basic function of this device is to provide information on flow reduction. An output signal from two out of the three bistables in a loop indicates a low flow in that loop.

Above P-7 two-out-of-four loop low flow trips the reactor; above P-8 low flow in any one loop causes a reactor trip.

The coincidence logic and interlocks are given in Table 7-1.

The detailed functional description of the process equipment associated with the trip function is contained in Reference 1.

b. Reactor coolant pump bus under-voltage trip

This trip is required in order to protect against low flow which can result from loss of voltage to the reactor coolant pumps (e.g., from plant blackout).

There is one under-voltage sensing monitor connected to the motor side of each reactor coolant pump breaker. (These reactor coolant pump breakers are located in the Category 1 Auxiliary Building.) These adjustable monitors provide an output signal when the voltage goes below approximately 60-80 percent of normal operating voltage. Signals from monitors connected to any two of the pumps (time delayed up to approximately 0.7 seconds to prevent spurious trips caused by short term voltage perturbations) trip the reactor if the power level is above P-7. The coincidence logic and interlocks are given in Table 7-1.

c. Reactor coolant pump bus underfrequency trip

This trip is required for the protection of the reactor from low flow resulting from bus underfrequency (e.g., major power grid frequency disturbance). This trip trips the reactor for an underfrequency condition. The setpoint of the underfrequency monitors is adjustable between 54 and 59 Hz.

One underfrequency sensing monitor is connected to each reactor coolant pump bus. (The reactor coolant pump bus is located in the Category 1 Auxiliary Building.) Signals from monitors connected to any two of the buses (time delayed up to approximately 0.2 seconds to prevent spurious trips caused by short term frequency perturbations) will cause a direct trip of the reactor if the power level is above P-7. An underfrequency condition will trip the reactor coolant pump breakers at any power level. Figure 7-1, Sheet 5, shows the logic for the Reactor Coolant System low flow trips.

5. Steam Generator Trip

The specific trip function generated is as follows:

a. Low-low steam generator water level trip

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

The logic is shown on Figure 7-1, Sheet 7. A detailed functional description of the process equipment associated with this trip is provided in Reference 1.

6. Safety Injection Signal Actuation Trip

A reactor trip occurs when the Safety Injection System is actuated. The means of actuating the Safety Injection System are described in Section 7.3. This trip protects the core against a loss of reactor coolant or steam.

Figure 7-1, Sheet 8, shows the logic for this trip. A detailed functional description of the process equipment associated with this trip function is provided in Reference 1.

7. Manual Trip

The manual trip consists of two switches with one output on each switch. One switch is used to actuate the train A trip breaker; the other switch actuates the train B trip breaker. Operating either manual trip switch removes the voltage from the under-voltage trip coil, energizes the shunt trip coil, and trips the reactor.

There are no interlocks which can block this trip. Figure 7-1, Sheet 3, shows the manual trip logic.

8. Turbine Trips

A direct reactor trip on turbine trip provides additional protection against PORV challenges initiated by a narrow range of events, that is, turbine trips not initiated by a reactor trip or a safety injection and occurring at or near full power.

The reactor trip on turbine trip will be generated by either of the following signals, provided reactor power is greater than the P-8 setpoint:

a. Four-out-of-four turbine stop valves closed.

b. Two-out-of-three turbine auto-stop oil pressure low, which indicates loss of turbine control oil.

The trip logic is shown on Figure 7-1, Sheet 16.

7.2.1.1.3 Reactor Protection System Interlocks

1. Power Escalation Permissives

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

A one-of-two intermediate-range permissive signal (P-6) is required prior to source range level trip blocking. A source-range manual block is provided for each logic train and the blocks must be in effect on both trains in order to proceed in the intermediate range. Source range level trips are automatically reactivated when both intermediate range channels are below the permissive (P-6) level. There is a manual reset switch for administratively reactivating the source range level trip when between the permissive P-6 and P-10 level, if required. Source range level trip block is always maintained when power is above the permissive P-10 level.

The intermediate-range level trip and power-range (low setpoint) trip can only be blocked after satisfactory operation and permissive information are obtained from two-of-four power-range channels. Individual blocking switches are provided so that the low setpoint power range trip and intermediate-range trip can be independently blocked. These trips are automatically reactivated when any three of the four power range channels are below the permissive (P-10) level, thus ensuring automatic activation to more restrictive trip protection.

The development of permissives P-6 and P-10 is shown on Figure 7-1, Sheet 4. All of the permissives are digital; they are derived from analog signals in the nuclear power range and intermediate-range channels.

See Table 7-2 for the list of protective system interlocks.

2. Blocks of Reactor Trips at Low Power

Interlock P-7 blocks a reactor trip at low power (below approximately 10 percent of full power) from low reactor coolant flow, reactor coolant pump under voltage, reactor coolant pump underfrequency, pressurizer low pressure, or, pressurizer high water level. See Figure 7-1, Sheets 5, 6 and 16, for permissive applications. The block action (absence of P-7 interlock signal) occurs when three-out-of-four power range neutron flux signals are below the setpoint in coincidence with two-out-of-two turbine inlet pressure signals below the setpoint (low unit load).

The P-8 interlock blocks a reactor trip from a turbine trip or low reactor coolant flow reactor trip when the unit is below approximately 47 percent of full power. The block action (absence of the P-8 interlock signal) occurs when three-out-of-four neutron flux power range signals are below the setpoint. Thus, below the P-8 setpoint, the reactor is allowed to operate with one inactive loop and trip does not occur until two loops are indicating low flow.

See Figure 7-1, Sheet 4, for derivation of P-8, and Sheet 5 for applicable logic. See Table 7-2 for the list of protection system blocks.

7.2.1.1.4 Reactor Coolant Temperature Sensor Arrangement

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

The hot leg temperature measurement on each loop is accomplished with three fast response narrow range RTDs mounted in thermowells, spatially located at intervals of 120° around the hot leg. A wide range RTD is installed in each hot leg. One fast response narrow range RTD is located in each cold leg at the discharge of the reactor coolant pump (replacements for the cold leg RTDs located in the bypass manifold). A wide range RTD is installed in each cold leg. Temperature streaming in the cold leg is not a concern due to the mixing action of the RCP, hence, only one cold leg RTD is required.

This cold leg temperature measurement, together with the average T_H obtained for the three hot leg temperatures, is used to calculate reactor coolant loop delta-t and T-average. A new penetration in each cold leg houses an additional well mounted narrow range RTD for use as an installed spare.

In the event of a single hot leg RTD faiure, the remaining two hot leg RTDs can be averaged to obtain the Thot Average of the loop. This can be accomplished by modifying the gain and/or bias of the circuitry based on historical data. The new two-RTD Thot Average shall be equivalent to the three-RTD Thot Average prior to failure of the one RTD.

7.2.1.1.5 Analog System

The process analog system is described in Reference 1.

7.2.1.1.6 Solid State Logic Protection System

The solid state logic protection system takes digital inputs (voltage/no voltage) from the process and nuclear instrument channels corresponding to conditions (normal/abnormal) of unit parameters. The system combines these signals in the required logic combination and generates a trip signal (no voltage) to the under-voltage coils of the reactor trip circuit breakers when the necessary combination of signals occur. The system also provides annunciator, status light and computer input signals which indicate the condition of bistable input signals, partial trip and full trip functions and the status of the various blocking, permissive and actuation functions. In addition, the system includes means for semi-automatic testing of the logic circuits. A detailed description of this system is given in Reference 3.

7.2.1.1.7 Isolation Amplifiers

In certain applications, it is considered advantageous to employ control signals derived from individual protection channels through isolation amplifiers contained in the protection channel, in accordance with IEEE-279.

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

Isolation amplifier qualification type tests are described in References 4 and 5

7.2.1.1.8 Energy Supply and Environmental Variations

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

7.2.1.1.9 Setpoints

The setpoints that require trip action, when reached, are given in the Technical Specifications, or in the Core Operating Limits Report.

7.2.1.1.10 Seismic Design

The seismic design considerations for the Reactor Protection System are given in Section 3.1. This design meets the requirements of Criterion 2 of the 1971 GDC.

7.2.1.2 Design Bases Information

The information given below and in Section 7.2.1.1.8 presents the design bases information requested by Section 3 of IEEE 279, 1971, Reference 8. Functional logic diagrams are presented in Figure 7-1.

7.2.1.2.1 Unit Conditions

The following are the generating station conditions requiring reactor trip.

1. DNBR approaching DNBR limit for Condition II faults (See Chapter 4 for fuel design limits).
2. Power density (kilowatts per foot) approaching rated value for Condition II faults (See Chapter 4 for fuel design limits).
3. Reactor Coolant System overpressure creating stresses approaching the limits specified in Chapter 5.

7.2.1.2.2 Unit Variables

The following are the variables required to be monitored in order to provide reactor trips (See Table 7-1).

1. Neutron flux
2. Reactor coolant temperature
3. Reactor Coolant System pressure (pressurizer pressure)
4. Pressurizer water level
5. Reactor coolant flow
6. Reactor coolant pump operational status (bus voltage and frequency)
7. Steam generator water level
8. Turbine-generator operational status (autostop oil pressure and stop valve position)

7.2.1.2.3 Spatially Dependent Variables

The following variable is spatially dependent: Reactor coolant temperature - see Section 7.3.1.2 for a discussion of this variable spatial dependence.

7.2.1.2.4 Limits, Margins and Levels

The parameter values that require reactor trip are given in Technical Specifications or in the Core Operating Limits Report. The Accident Analysis proves that the setpoints used in the Technical Specifications are conservative.

The setpoints for the various functions in the Reactor Protection System have been analytically determined such that the operational limits so prescribed prevent fuel rod clad damage and loss of integrity of the Reactor Coolant System as a result of any Condition II incident (anticipated malfunction). For those incidents the Reactor Protection System limits the following parameters to:

1. Minimum DNBR greater than the statistical design limit for the DNB correlation
2. Maximum System Pressure less than 110% of the design pressure
3. Fuel rod maximum linear power less than the rate which would cause centerline melting

The accident analyses described in Chapter 15.0 demonstrates that the functional requirements as specified for the Reactor Protection System are adequate to meet the above considerations, even assuming, for conservatism and adverse combinations of instrument errors. A discussion of the safety limits associated with the reactor core and Reactor Coolant System, plus the limiting safety system setpoints, are presented in the Technical Specifications.

7.2.1.2.5 Abnormal Events

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

1. Earthquakes (refer to Chapter 3 and Chapter 2).
2. Fire (refer to Section 9.5).
3. Explosion (Hydrogen Buildup inside Containment). (Refer to Section 6.2).
4. Missiles (refer to Section 3.5).
5. Flood (refer to Chapter 2 and Chapter 3).
6. Wind and Tornadoes (refer to Section 3.3).

7.2.1.2.6 Minimum Performance Requirements

The performance requirements are as follows:

1. System response times:

   The time delays are defined as the time required for the reactor trip (i.e., the time the rods are free and beginning to fall) to be initiated following a step change in the variable being monitored from 5 percent below to 5 percent above the trip setpoint. During preliminary startup tests, it was demonstrated that actual time delays of installed equipment are equal to or less than the values assumed in the accident analyses. Maximum allowable time delays in generating the reactor trip signal are given in Table 7-19.

2. Reactor trip accuracies are calculated for the various trip functions by approved, conservative methodologies.

7.2.1.3 Final System Drawings

Functional block diagrams, electrical elementaries and other drawings required to assure electrical separation and perform a safety review are provided in the McGuire Electrical Drawings.

7.2.2 Analyses

7.2.2.1 Failure Mode and Effects Analyses

A failure mode and effects analyses of the Reactor Protection System has been performed. Results of this study and a fault tree analysis are presented in Reference 6.

7.2.2.2 Evaluation of Design Limits

While most setpoints used in the Reactor Protection System are fixed, there are variable setpoints, most notably the overtemperature ΔT and overpower ΔT setpoints. All setpoints in the Reactor Protection System have been selected on the basis of engineering design and safety studies. The capability of the Reactor Protection System to prevent loss of integrity of the fuel cladding and/or Reactor Coolant System pressure boundary during Condition II and III transients is demonstrated in the Accident Analysis, Chapter 15. These safety analyses are carried out using those setpoints determined from results of the engineering design studies. Setpoint limits are presented in the Technical Specifications and Core Operating Limits Report. A discussion of the intent for each of the various reactor trips and the accident analysis (where

appropriate) which utilizes this trip is presented below. It should be noted that the selected trip setpoints all provide for margin before protective action is actually required to allow for uncertainties and instrument errors. The design meets the requirements of Criteria 10 and 20 of the 1971 GDC.

7.2.2.2.1 Trip Setpoint Discussion

It has been pointed out previously that below the DNBR limit there may be a potential for local fuel cladding failure. The DNB ratio existing at any point in the core for the core design has been determined as a function of the core inlet temperature, power output, operating pressure and flow. Consequently, core safety limits in terms of a DNBR equal to the DNBR limit for the hot channel have been developed as a function of core ΔT, T_{avg} and pressure for a specified flow as illustrated by the solid lines in Figure 7-3. Also shown as solid lines in Figure 7-3 are the loci of conditions equivalent to 118 percent reactor power as a function of ΔT and T_{avg} representing the overpower (KW/ft) limit on the fuel. The dashed lines indicate the maximum permissible setpoint (ΔT) as a function of T_{avg} and pressure for the overtemperature and overpower reactor trip. Actual setpoint constants in the equation representing the dashed lines are as given in the Core Operating Limits Report. These values are conservative to allow for instrument errors. The design meets the requirements of Criteria 10, 15, 20 and 29 of the 1971 GDC.

DNBR is not a directly measurable quantity; however, the process variables that determine DNBR are sensed and evaluated. Small isolated changes in various process variables may not individually result in violation of a core safety limit. The design concept of the Reactor Protection System takes cognizance of this situation by providing reactor trips associated with individual process variables in addition to the overpower/overtemperature safety limit trips. Process variable trips prevent reactor operation whenever a change in the monitored value is such that a core or system safety limit is in danger of being exceeded should operation continue. Basically, the high pressure, low pressure and overpower/overtemperature ΔT trips provide sufficient protection for slow transients as opposed to such trips as reactor coolant pump under-voltage, high flux, or rate, which trip the reactor for faster changes in flow or flux, respectively, that would result in fuel damage before actuation of the slower responding ΔT trips could be effected.

Therefore, the Reactor Protection System is designed to provide protection for fuel cladding and Reactor Coolant System pressure boundary integrity where: (1) a rapid change in a single variable or factor could potentially result in exceeding a core or a system safety limit, and (2) a slow change in one or more variables will have an integrated effect which potentially could cause safety limits to be exceeded. Overall, the Reactor Protection System offers diverse and comprehensive protection against fuel cladding failure and/or loss of Reactor Coolant System integrity for Condition II and III accidents.

The Reactor Protection System design was evaluated in detail with respect to common mode failure and is presented in References 6 and 7. The design meets the requirements of Criterion 21 of the 1971 GDC.

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

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

7.2.2.2.2 Reactor Coolant Flow Measurement

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

$$\frac{\Delta P}{\Delta P_o} = \left(\frac{w}{w_o}\right)^2$$

where ΔP_o is the pressure differential at the reference flow w_o, and ΔP is the pressure differential at the corresponding flow, w. The full flow reference point is established by extrapolating along the correlation curve. The expected absolute accuracy of the channel is within ± 10 percent of full flow and field results have shown the repeatability of the trip point to be within ± 1 percent.

7.2.2.2.3 Evaluation of Compliance to Applicable Codes and Standards

The Reactor Protection System meets the criteria of the NRC General Design Criteria as indicated. The Reactor Protection System meets the criteria of IEEE-Standard 279, Reference 8.

1. Single Failure Criterion

   The protection system is designed to provide two, three, or four instrumentation channels for each protective function and two logic train circuits. These redundant channels and trains are electrically isolated and physically separated. Thus, any single failure within a channel or train does not prevent protective action at the system level when required. Loss of input power to a channel or logic train results in a signal calling for a trip. This design meets the requirements of Criterion 23 of the 1971 GDC.

   To prevent the occurrence of common mode failures, such additional measures as functional diversity, physical separation, and testing as well as administrative control during design, production, installation and operation are employed, as discussed in Reference 6. The design meets the requirements of Criteria 21 and 22 of the 1971 GDC.

2. Quality of Components and Modules

   For a discussion of the quality of the components and modules used in the Reactor Protection System, refer to Chapter 17. The quality assurance applied conforms to Criterion 1 of the 1971 GDC.

3. Equipment Qualification

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

4. Independence

   Channel independence is maintained throughout the system, extending from the sensor through to the devices actuating the protective function. Physical separation is used to achieve separation of redundant transmitters. Separation of wiring is achieved by using separate wireways, cable trays, conduit runs and Containment penetrations for each redundant channel. Redundant analog equipment is separated by locating modules in separate protection cabinets. Each redundant channel is energized from a separate ac power feed. This design meets the requirements of Criterion 21 of the 1971 GDC.

Independence of the logic trains is discussed in Reference 3. Two reactor trip breakers, actuated by separate logic matrices, interrupt power to the control rod drive mechanisms. The breaker main contacts are connected in series with the power supply so that opening either breaker interrupts power to all full length control rod drive mechanisms, permitting the rods to free fall into the core. See Figure 7-4.

The design philosophy is to make maximum use of a wide variety of measurements. The protection system continuously monitors numerous diverse system variables. The extent of this diversity has been evaluated for a wide variety of postulated accidents and is discussed in Reference 7. Generally, two or more diverse protection functions would terminate an accident before intolerable consequences could occur. The design meets the requirements of Criterion 22 of the 1971 GDC.

5. Control and Protection System Interaction

The protection system is designed to be independent of the control system. In certain applications the control signals and other non-protective functions are derived from individual protection channels through isolation amplifiers. The isolation amplifiers are classified as part of the protection system and are located in the analog protection racks. Non-protective functions include those signals used for control, remote process indication, and computer monitoring. The isolation amplifiers are designed such that a short circuit, open circuit, or the application of 118VAC or 140VDC on the isolated portion of the circuit (i.e., the non-protective side of the circuit) will not affect the input (protective) side of the circuit. The signals obtained through the isolation amplifiers are never returned to the protection racks. This design meets the requirements of Criterion 24 of the GDC and Section 4.7 of IEEE 279, 1971, Reference 8.

A detailed discussion of the design and testing of the isolation amplifiers is given in References 4 and 5. These reports include the results of applying various malfunction conditions on the output portion of the isolation amplifiers. The results show that no significant disturbance to the isolation amplifier input signal occurred.

The redundant, isolated control signal cables leaving the protection racks come into close proximity at locations such as the control board. It would be postulated that electrical faults, or interference, at these locations might be propagated into all redundant racks and degrade protection circuits because of the close proximity of protection and control wiring within each rack.

Westinghouse test programs have demonstrated that Class 1E protection systems Nuclear Instrumentation System (NIS), Solid State Protection System (SSPS) and 7300 Process Control System (7300 PCS) are not degraded by non-Class 1E circuits, sharing the same enclosure, which could be postulated to carry electrical faults or interference into the enclosures.

Tests conducted on the as-built designs of the NIS and SSPS were reported and accepted by the NRC in support of the Diablo Canyon application (Docket No's 50-275 and 50-323). Westinghouse considers these programs as applicable to all plants, including McGuire. Westinghouse tests on the 7300 PCS were covered in a report entitled “7300 Series Process Control System Noise Tests” subsequently reissued as WCAP-8892-A (Reference 10). In a letter dated April 20, 1977, R. Tedesco to C. Eicheldinger, the NRC accepted the report in which the applicability to the McGuire plant is established.

The Westinghouse 7300 Process Instrumentation and Control System controls portion has been replaced with a digital Distributed Control System (DCS), specifically, the Emerson-

Westinghouse Ovation platform. The Ovation DCS is capable of performing the same control and monitoring functions as the previous W7300 system.

The use of auctioneered high or low inputs from the protection sets for control inputs has been replaced in favor of using validated signal selection (median, 2nd highest, etc.) This design approach reduces problems caused by the failure of an input sensor.

6. Capability for Testing

The Reactor Protection System is capable of being tested during power operation. Where only parts of the system are tested at any one time, the testing sequence provides the necessary overlap between the parts to assure complete system operation. The testing capabilities are in conformance with Regulatory Guide 1.22 as discussed in Section 7.1.2.1.

The protection system is designed to permit periodic testing of the analog channel portion of the Reactor Protection System during reactor power operation without initiating a protective action unless a trip condition actually exists. This is because of the coincidence logic required for reactor trip. Note, however, that the source and intermediate range high neutron flux trips must be bypassed during testing.

The following types of sensors provide input to the protection sets of Process Control System and Solid State Protection System for Engineered Safety Features Actuation and Reactor Protection System:

a. Differential Pressure Transmitters (Level)
b. Differential Pressure Transmitters (Flow)
c. Pressure Transmitters
d. Frequency Transmitters
e. Voltage Transmitters
f. Circuit Breaker Auxiliary Contacts
g. Pressure Switches
h. Valve Limit Switches
i. Resistance Temperature Detectors

The response time of differential pressure transmitters (level), differential pressure transmitters (flow), pressure transmitters, frequency transmitters, and voltage transmitters are tested by one of the following methods:

a. Test sensor in place by perturbing the process being monitored using existing equipment used for normal plant operation.
b. Test sensor in place by perturbing the process input using additional equipment provided for response time testing.
c. Remove the sensor from service and bench test the device.

Westinghouse WCAP-13632-P-A, 'Elimination of Pressure Sensor Response Time Testing Requirements' and WCAP-14036-P-A, 'Elimination of Periodic Protection Channel Response Time Tests' provide both the technical basis and the methodology for verifying the total channel response time using an allocated time. WCAP-13632-P-A and WCAP-14036-P-A specify 'allocated response time' values for specific sensor and electronic components. This methodology may be used in conjunction with or in lieu of response time measurement testing.

Circuit breaker auxiliary contacts, pressure switches, and valve limit switches are tested for operation only. Since these are bistable devices, no significant change in response time is anticipated when compared to the overall response time of the system.

No significant deterioration in response time of resistance temperature detector elements is anticipated. However, RTD elements are tested on a refueling outage frequency.

The operability of the process sensors is ascertained by comparison with redundant channels monitoring the same process variables or those with a fixed known relationship to the parameter being checked. The incontainment process sensors can be calibrated during unit shutdown if required.

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

The power range channels of the Nuclear Instrumentation System are tested by superimposing a test signal on the actual detector signal being received by the channel at the time of testing. The positive flux rate trip is tested by applying an appropriate step change to the input of each power range channel. This is accomplished in the test mode by alternating between 2 test signals where one test signal is adjusted to be the required percent of full power above the second test signal. Turning the Test Signal Selector from the lower value signal to the higher value signal introduces the positive step change. Bistable action is verified by control board annunciator and trip status lights. The test signals are introduced at a point equivalent to the detector signal inputs on each power range drawer assembly.

Figure 7-1 (Sheet 3) of the FSAR shows the output of the “rate trip.” The power range channel showing test injection points is shown in Figure 2-3 of WCAP-8255, Reference 2. A description of the test circuit operation for each channel is also included on Page 3-13 in Section 3.6 of WCAP-8255. The output of the bistable is placed in a tripped condition and bypassed prior to testing. The power range channel logic is two-out-of-four, and bypassing of this reactor trip function during testing is not required, however bypass of this reactor trip function is routinely done as a precaution.

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

It should be noted that a valid trip signal causes the channel under test to trip at a lower actual reactor power level. A reactor trip occurs when a second bistable trips. No provision is made in the channel test circuit for reducing the channel signal level below that signal being received from the Nuclear Instrumentation System detector.

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

For a detailed description of the Nuclear Instrumentation System see Reference 2.

The design of the Reactor Coolant Pump Monitor Panel provides a high degree of flexibility for testing of the trip logic circuits. Each of the under-voltage and underfrequency trip signals is generated by an individual two-out-of-four logic system. Use of the two-out-of-four SSPS logic permits calibration and/or testing of one channel at a time during reactor operation without jeopardizing overall system performance. Key lock test switches are provided to break the potential inputs to the voltage sensing circuits to functionally test each channel. The under-frequency channels can be tested in the same manner. The RCP under-voltage and underfrequency monitors comply with the requirements of IEEE 279-1971.

The reactor logic trains of the Reactor Protection System are designed to be capable of complete testing at power. Annunciation is provided in the Control Room to indicate when a train is in test (train output bypassed) and when a reactor trip breaker is bypassed. Details of the logic system testing are given in Reference 3.

The reactor coolant pump breakers cannot be tripped at full power without causing a unit upset by loss of power to a coolant pump.

Manual trip cannot be tested at power without causing a reactor trip since operation of either manual trip switch actuates its associated train. Note, however, that manual trip could also be initiated from outside the Control Room by manually tripping one of the reactor trip breakers.

The reactor trip function that is derived from the automatic safety injection signal is tested at power as follows:

1. The analog signals, from which the automatic safety injection signal is derived, are tested at power in the same manner as the other analog signals and as described in Section 7.2.2.2.3. The processing of these signals in the Solid State Protection System (SSPS) wherein their channel orientation converts to a logic train orientation is tested at power by the built-in semi-automatic test provisions of the SSPS as described in Reference 3. The reactor trip breakers are tested at power as discussed in Section 7.2.2.2.3. The testing of reactor trip from safety injection during refueling refers only to the manual safety injection actuation function.

   The generation of reactor trip from turbine trip on the Westinghouse turbine is a testable function at power (similar to the other reactor trips) generated from analog channels developing a bistable (on-off output), as follows:

   a. The signal derived from the auto stop oil pressure switch is tested by exercising the switches one at a time before entering mode 1 and the logic combinations are tested at power.

   b. The position signal derived from the turbine steam stop valves is testable at any load when the functional tests of the steam inlet valve are performed on a one-valve-at-a-time basis.

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

1. Check of input relays

   During testing of the Process Instrumentation System and Nuclear Instrumentation System channels, each channel bistable is placed in a trip mode causing one input relay in train A and one in train B to de-energize. A contact of each relay is connected to a universal logic printed circuit card. This card performs both the reactor trip and monitoring functions. The contact that creates the reactor trip also causes a status lamp and an annunciator on the

control board to operate. Either the train A or train B input relay operation lights the status lamp and annunciator.

Each train contains a multiplexing test switch. At the start of a Process or Nuclear Instrumentation System test, this switch (in either train) is placed in the A + B position. The A + B position alternately allows information to be transmitted from the two trains to the control board. A steady status lamp and annunciator indicates that input relays in both trains have been de-energized. A flashing lamp means that the input relays in the two trains did not both de-energize. Contact inputs to the logic protection system such as reactor coolant pump bus underfrequency relays operate input relays which are tested by operating the remote contacts as described above and using the same type of indications as those provided for bistable input relays.

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

2. Check of Logic Matrices

   Logic matrices are checked one train at a time. Input relays are not operated during this portion of the test. Reactor trips from the train being tested are inhibited with the use of the input error inhibit switch on the semi-automatic test panel in the train. Details of semi-automatic tester operation are given in Reference 3. At the completion of the logic matrix tests, one bistable in each channel of process instrumentation or nuclear instrumentation is tripped to check closure of the input error inhibit switch contacts.

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

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

   The general design features and details of the testability of the logic system are described in Reference 3. The testing capability meets the requirements of Criterion 21 of the 1971 GDC.

3. Testing of Reactor Trip Breakers

   Normally, reactor trip breakers 52/RTA and 52/RTB are in service, and bypass breakers 52/BYA and 52/BYB are withdrawn (out of service). In testing the protection logic, pulse techniques are used to avoid tripping the reactor trip breakers thereby eliminating the need to bypass them during this testing. The following procedure describes the method used for testing the trip breakers:

   a. With bypass breaker 52/BYA racked out, manually close and trip it to verify its operation.

b. Rack in and close 52/BYA. Manually trip 52/RTA through a protection system logic matrix.

c. Reset 52/RTA.

d. Trip and rack out 52/BYA.

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

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

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

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

The complete Reactor Protection System is normally required to be in service. However, to permit online testing of the various protection channels or to permit continued operation in the event of a subsystem instrumentation channel failure, Technical Specifications 3.3.1 and 3.3.2 define the required restrictions for bypassing a channel and for operation due to a channel failure.

The Reactor Protection System is designed in such a way that response time tests are only to be performed during shutdown. However, the safety analyses utilize conservative numbers for trip channel response time. The measured channel response times are compared with those used in the safety evaluations. On the basis of startup tests conducted on several units, the actual response times measured are less than the time used in the safety analyses.

4. Bypasses

Where operating requirements necessitate automatic or manual bypass of a protective function, the design is such that the bypass is removed automatically whenever permissive conditions are not met. Devices used to achieve automatic removal of the bypass of a protective function are considered part of the protective system and are designed in accordance with the criteria of this section. Indication is provided in the Control Room if some part of the system has been administratively bypassed or taken out of service. A discussion of the design and implementation of the bypass system per Regulatory Guide 1.47 is provided in Section 7.8.2.

5. Multiple Setpoints

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

6. Completion of Protective Action

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

7. Manual Initiation

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

8. Access

   The design provides for administrative control of access to all setpoint adjustments, module calibration adjustments, test points, and the means for manually bypassing channels or protective functions. For details refer to Reference 1.

9. Information Read Out

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

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

   Annunciators are also used to alert the operator of deviations from normal operating conditions so that he may take appropriate corrective action to avoid a reactor trip. Actuation of any rod stop or trip of any reactor trip channel actuates a visual and audible alarm.

10. Identification

    The protection system equipment is identified distinctively as being in the protection system. This identification distinguishes between redundant portions of the protection system. The identification described in Section 7.1 provides immediate and unambiguous identification of the protection equipment.

7.2.2.3 Specific Control and Protection Interactions

7.2.2.3.1 Neutron Flux

Four power range nuclear instrumentation channels are provided for overpower protection. An additional signal for automatic rod control is derived by comparing the four NIS channels and selecting the "2nd highest". If any channel fails in such a way as to produce a high or low output, that channel does not cause control rod movement because of the "2nd highest" algorithm. Two out of four overpower trip logic ensure an overpower trip if needed even with an independent failure in another channel.

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

7.2.2.3.2 Reactor Coolant Temperature

The accuracy of the narrow range resistance temperature detector loop temperature measurements is demonstrated during plant startup tests by comparing temperature measurements from the loop narrow range resistance temperature detectors with one another as well as with the temperature measurements obtained from the wide range resistance temperature detector located in the hot leg and cold leg piping of each loop. The comparisons are done with the Reactor Coolant System in an isothermal condition. The linearity of the ΔT measurements obtained from the hot leg and cold leg loop narrow range resistance temperature detectors as a function of plant power is also checked during plant startup tests. The absolute value of ΔT versus plant power is not important, per se, as far as reactor protection is concerned. Reactor Trip System setpoints are based upon percentages of the indicated ΔT at nominal full power rather than on absolute values of ΔT. This is done to account for loop differences which are inherent and therefore provides better protective action without the expense of accuracy. For this reason, the linearity of the ΔT signals as a function of power is of importance rather than the absolute values of the ΔT. As part of the plant startup tests, the loop narrow range resistance temperature detector signals are compared with the core exit thermo-couple signals.

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

Since control is based on the average temperature of the loop with the 2nd highest temperature, the control rods are always moved based upon a conservative temperature measurement with respect to DNB. A spurious low or high average temperature measurement from any loop will cause no control action and will alert the operator of the abnormal condition.

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

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

7.2.2.3.3 Pressurizer Pressure

The pressurizer pressure protection channel signals are used for high and low pressure protection and as inputs to the overtemperature ΔT trip protection function. Isolated output signals from these channels are used by the Ovation PCS to control pressurizer spray and heaters and power operated relief valves. Pressurizer pressure is sensed by fast response pressure transmitters.

The control scheme utilizes the 2nd highest value signaled from protection Channels I, II, III, and IV. The control scheme eliminates spurious transmitter signals from impacting the pressure control function.

Additional redundancy is provided in the low pressurizer pressure reactor trip logic and in the logic for safety injection to ensure low pressure protection.

In the unlikely event that the Control Room must be evacuated, the Reactor Coolant System pressure can be maintained by use of the auxiliary spray supply valves and the pressurizer heaters. Controls for these valves and heaters are located on the auxiliary shutdown panel.

The pressurizer heaters are incapable of overpressurizing the Reactor Coolant System. Overpressure protection is based upon the maximum positive surge of the reactor coolant produced as a result of turbine trip under full load, assuming the core continues to produce full power with normal feed flow maintained. The self-actuated safety valves are sized on the basis of steam flow from the pressurizer to accommodate this surge at a setpoint of 2500 psia and an accumulation of 3 percent. Note that no credit is taken for the relief capability provided by the power operated relief valves, or the steam dump system.

In addition, operation of any one of the power operated relief valves maintains pressure below the high pressure trip point for most transients. The rate of pressure rise achievable with heaters is slow, and ample time and pressure alarms are available to alert the operator of the need for appropriate action.

Redundancy is not compromised by having a shared tap since the logic for this trip is two out of four. If the shared tap is plugged, the affected channels remain static. If the impulse line bursts, the indicated pressure drops to zero. In either case the fault is easily detectable, and the protective function remains operable.

7.2.2.3.4 Pressurizer Water Level

Three pressurizer water level channels are used for high pressurizer water level reactor trip. Isolated signals from these channels are processed with a median select algorithm and then used by the Ovation PCS for pressurizer water level control. A failure in the level control system could fill or empty the pressurizer at a slow rate (on the order of half an hour or more), which allows ample time for corrective action by the operator.

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

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

7.2.2.3.5 Steam Generator Water Level

The basic function of the reactor protection circuits associated with low-low steam generator water level is to preserve the steam generator heat sink for removal of long-term residual heat. Should a complete loss of feedwater occur, the reactor would be tripped on low-low steam generator water level. In addition, redundant auxiliary feedwater pumps are provided to supply feedwater in order to maintain residual heat removal after trip. This reactor trip acts before the steam generators are dry. This reduces the required capacity and increases the time interval before auxiliary feedwater pumps are required, and minimizes the thermal transient on the Reactor Coolant System and steam generators. Therefore, a low-low steam generator water level reactor trip circuit is provided for each steam generator to ensure that sufficient initial thermal capacity is available in the steam generator at the start of the transient.

Three channels of main feedwater flow instrumentation and two channels of main steam flow instrumentation are provided for each steam generator level controller. The Ovation PCS uses signal validation logic to exclude failed signals. Therefore, a spurious high or low signal from the feedwater or steam flow channel will not cause a significant change in feedwater flow. The mismatch between steam flow and feedwater flow s signals would actuate alarms to alert the operator of the situation in time for manual correction. If the condition continues, a two-out-of-three high-high steam generator water level signal in any loop, independent of the indicated feedwater flow, will cause feedwater isolation and trip the turbine. The high-high steam generator water level trip is an equipment protective trip preventing excessive moisture carryover which could damage the turbine blading.

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

Four steam generator water level signals from the protection channel are used for level control for each steam generator. The Ovation PCS selects the 2nd highest of the four signals, which will avoid control system reaction to a spurious low steam generator water level signal which would otherwise tend to open the feedwater valve. Before a reactor trip would occur, two-out-of-four channels in a loop would have to indicate a low-low water level. Any slow drift in the water level signal will permit the operator to respond to the level alarms and take corrective action.

Deleted Per 2011 Update.

7.2.2.4 Additional Postulated Accidents

Loss of station instrument air or loss of component cooling water is discussed in Section 7.3.2.3. Load rejection and turbine trip are discussed in further detail in Section 7.7.

The control interlocks, called rod stops, that are provided to prevent abnormal power conditions which could result from excessive control rod withdrawal are discussed in Section 7.7.1.4.1 and listed on Table 7-18. Excessively high power operation (which is prevented by blocking of automatic rod withdrawal), if allowed to continue, might lead to a safety limit (as given in Technical Specifications) being reached. Before such a limit is reached, protection is available from the Reactor Protection System. At the power levels of the rod block setpoints, safety limits have not been reached, and therefore these rod withdrawal stops do not come under the scope of safety related systems, and are considered as control systems.

7.2.3 Tests and Inspections

The Reactor Protection System meets the testing requirements of IEEE 338, 1971, Reference 9, as discussed in Section 7.1.2.1. The testability of the system is discussed in Section 7.2.2.2.3. The initial test intervals are specified in Chapter 16. Written test procedures and documentation, conforming to the requirements of Reference 9, will be available for audit by responsible personnel. Periodic testing complies with Regulatory Guide 1.22 as discussed in Sections 7.1.2.1, and 7.2.2.2.3.

7.2.3.1 In-Service Tests and Inspections

Periodic surveillance of the Reactor Protection System is performed to ensure proper protective action. This surveillance consists of checks, calibrations, and channel functional testing which are summarized as follows:

1. Checks

   A check consists of a qualitative determination of acceptability by observation of channel behavior during operation. It includes comparison of the channel with other independent channels measuring the same variable. Failures such as blown instrument fuses, defective indicators, or faulted amplifiers which result in “upscale” or “downscale” indication can be easily recognized by simple observation of the functioning of the instrument or system. Furthermore, in many cases such failures are revealed by alarm or annunciator action, and a check supplements this type of surveillance.

2. Calibration

   A channel calibration consists of adjustment of channel output such that it responds, within acceptable range and accuracy, to known values of the parameter which the channel measures. Calibration encompasses the entire channel including alarm and/or trip, and includes the channel functional test discussed below. Thus, the calibration ensures the acquisition and presentation of accurate information.

3. Channel functional test

   A channel functional test consists of injecting a simulated signal into the signal conditioning portion of the channel to verify its operability, including alarm and/or trip initiating action.

   The minimum frequency for checks, calibration and testing are defined in Technical Specifications. Based on experience with both conventional and nuclear systems, when the unit is in operation the minimum checking frequencies set forth therein are considered adequate.

7.2.3.2 Periodic Testing of the Nuclear Instrumentation System

The following periodic tests of the Nuclear Instrumentation System can be performed, but may not be required by Technical Specifications:

1. Testing at unit shutdown
   a. Source range testing
   b. Intermediate range testing
   c. Power range testing
2. Testing between P-6 and P-10 permissive power levels
   a. Source range testing
   b. Intermediate range testing
   c. Power range testing
3. Testing above P-10 permissive power level
   a. Source range testing
   b. Intermediate range testing
   c. Power range testing

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

7.2.3.3 Periodic Testing of the Process Analog Channels of the Protection Circuits

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

1. T_{avg} and ΔT protection channels
2. Pressurizer pressure protection channels
3. Pressurizer water level protection channels
4. (Deleted)
5. Steam generator water level protection channels
6. Reactor coolant low flow protection channels
7. Turbine inlet pressure channels
8. Containment pressure
9. Steam pressure protection channels

The following conditions are required for these tests:

1. These tests may be performed at any unit power from cold shutdown to full power.
2. Before starting any of these tests with the unit at power, all redundant reactor trip channels associated with the function to be tested must be in the normal (untripped) mode in order to avoid spurious trips.
3. Refer to the applicable plant test procedures for setpoints.
4. The Suppliers' Systems Manuals which contain systems description, static and dynamic testing, are referenced in the plant test procedures.
5. The Westinghouse or Supplier's Block Diagrams which identify the functions provided in the instrument channels, are referenced in the plant test procedures.

7.2.4 References

1. Reid, J. B., Process Instrumentation for Westinghouse Nuclear Steam Supply Systems, Westinghouse Electric Corporation, *WCAP 7913*, January, 1973. (Non-proprietary.)
2. Lipchak, J. B., Nuclear Instrumentation System, Westinghouse Electric Corporation, *WCAP 8255*, January, 1974.
3. Katz, D. N., Solid State Logic Protection System Description, Westinghouse Electric Corporation, *WCAP 7488-L*, March, 1971 (Westinghouse NES Proprietary); and *WCAP 7672*, May, 1971 (Non-proprietary).
4. Garber, I., Isolation Tests Process Instrumentation Isolation Amplifier Westinghouse Computer and Instrumentation Division Nucana 7300 Series, Westinghouse Electric Corporation, *WCAP 7862*, September, 1972 (Non-proprietary).
5. Lipchak, J. B., and Bartholomew, R. R., Test Report Nuclear Instrumentation System Isolation Amplifier, Westinghouse Electric Corporation, *WCAP 7506L*, October, 1970 (Westinghouse NES Proprietary); and *WCAP 7819* Rev. 1, January, 1972 (Non-proprietary).
6. Gangloff, W. C., and Loftus, W. D., An Evaluation of Solid State Logic Reactor Protection In Anticipated Transients, Westinghouse Electric Corporation, *WCAP 7706-L*, (Westinghouse NES Proprietary) and *WCAP 7706* (Non-proprietary), July, 1971.

7. Burnett, T. W. T., Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors, Westinghouse Electric Corporation, *WCAP 7306*, April, 1969.

8. The Institute of Electrical and Electronic Engineers, Inc., IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations, *IEEE Std. 279-1971*.

9. The Institute of Electrical and Electronic Engineers, Inc., IEEE Trial Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems, *IEEE Std. 338-1971*.

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

11. Safety Evaluation Report, McGuire Nuclear Station, Units 1 and 2, Supp. No. 7, NUREG-0422, May, 1983.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.2.

THIS PAGE LEFT BLANK INTENTIONALLY.

7.3 Engineered Safety Features Actuation System

In addition to the requirements for a reactor trip for anticipated abnormal transients, the facility is provided with adequate instrumentation and controls to sense accident situations and initiate the operation of necessary Engineered Safety Features. The occurrence of a limiting fault, such as a loss of coolant accident or a steam break, requires a reactor trip plus actuation of one or more of the Engineered Safety Features in order to prevent or mitigate damage to the core and Reactor Coolant System components, and insure Containment integrity.

In order to accomplish these design objectives the Engineered Safety Features system has proper and timely initiating signals which are supplied by the sensors, transmitters and logic components making up the various instrumentation channels of the Engineered Safety Features Actuation System.

7.3.1 Description

The Engineered Safety Features Actuation System senses selected unit parameters, determines whether or not predetermined safety limits are being exceeded and, if they are, combines the signals into logic matrices sensitive to combinations indicative of primary or secondary system boundary ruptures (Class III or IV faults). Once the required logic combination is completed, the system sends actuation signals to those engineered safety features components whose aggregate function best serves the requirements of the accident. The Engineered Safety Features Actuation System meets the requirements of Criteria 13 and 20 of the 1971 GDC.

7.3.1.1 System Description

The Engineered Safety Features Actuation System is a functionally defined system described in this section. The equipment which provides the actuation functions identified in Section 7.3.1.1.1 is listed below and discussed in this section and the referenced WCAPs.

1. Process Instrumentation (Reference 1)
2. Solid State Logic Protection System (Reference 3)
3. Engineered Safety Features Test Cabinet (Reference 4)
4. Manual Actuation Circuits

The Engineered Safety Features Actuation System consists of two discrete portions of circuitry: 1) An analog portion consisting of three to four redundant channels per parameter or variable to monitor various unit parameters such as the Reactor Coolant System and steam system pressures, temperatures and flows and Containment pressures; and 2) a digital portion consisting of two redundant logic trains which receive inputs from the analog protection channels and perform the needed logic to actuate the engineered safety features. Each digital train is capable of actuating the engineered safety features equipment required. The intent is that any single failure within the Engineered Safety Features Actuation System does not prevent system action when required.

The redundant concept is applied to both the analog and logic portions of the system. Separation of redundant analog channels begins at the process sensors and is maintained in the field wiring, Containment vessel penetrations and analog protection racks, terminating at the redundant groups of safeguards logic racks. The design meets the requirements of Criterion 20, 21, 22, 23 and 24 of the 1971 GDC.

The variables are sensed by the analog circuitry as discussed in Reference 1 and in Section 7.2. The outputs from the analog channels are combined into actuation logic as shown on Figure 7-1, Sheets 5, 6, 7 and 8. Table 7-5 and Table 7-6 give additional information pertaining to logic and function.

The interlocks associated with the Engineered Safety Features Actuation System are outlined in Table 7-7.

The overriding or resetting of the ESF actuation signal does not cause any equipment to change position. Deliberate manual operator action is required to reposition the equipment (Reference 7).

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

Deleted paragraph(s) per 2002 revision.

The NRC issued Generic Letter 89-19, "Request for Action Related to the Resolution of Unresolved Issue A-47, 'Safety Implication of Control Systems in LWR Plants' Pursuant to 10 CFR 50.54(f)," on September 20, 1989. This generic letter required PWR licensees to provide a description of their steam generator overfill protection systems, which was responded to in the letter from H.B. Tucker to NRC dated March 19, 1990. As described in that response to the NRC, the McGuire overfill protection system is initiated on high water level in any one steam generator based on a safety grade 2-out-of-3 initiating logic. The system isolates main feedwater (MFW) by closing the MFW isolation valves and tripping the MFW pumps. In accordance with the Generic Letter 89-19 guidance, the overfill protection channels are electrically isolated from the control channels through isolator cards in the Westinghouse 7300 PCS. Section 3.3.2 of the MNS Technical Specifications includes requirements to periodically verify operability of the overfill protection system.

A description of the Ice Condenser System and its associated instrumentation is given in Chapter 6.

7.3.1.1.1 Function Initiation

The specific functions which rely on the Engineered Safety Features Actuation System for initiation are:

1. A reactor trip, provided one has not already been generated by the Reactor Protection System.
2. A “Safety Injection” or “S” signal which in turn actuates the following items:
   a. Cold leg injection isolation valves which are opened for injection of borated water by safety injection pumps into the cold legs of the Reactor Coolant System.
   b. Charging pumps, safety injection pumps, residual heat removal pumps and associated valving which provide emergency makeup water to the cold leg of the Reactor Coolant System following a loss of coolant accident.
   c. Service water pumps which provide cooling water to the Component Cooling System heat exchangers and is thus the heat sink for Containment cooling.
   d. Motor driven auxiliary feedwater pumps.
   e. Emergency diesels to assure backup supply of power to emergency and supporting systems components. (Required if preferred offsite power is not available.)

3. Phase A containment isolation, whose function is to prevent fission product release to the site boundary by isolating all nonessential lines.
4. Steam line isolation to prevent the continuous, uncontrolled blowdown of more than one steam generator and thereby uncontrolled Reactor Coolant System cooldown.
5. Main feedwater line isolation as required to prevent or mitigate the effect of excessive cooldown.
6. High-high containment pressure signal which performs the following functions:
   a. Initiates containment spray air return fans (after time delay) to reduce containment pressure and temperature following a loss of coolant or steamline break accident inside containment.
   b. Initiates phase B Containment isolation which isolates the Containment following a loss of reactor coolant accident, or a steam or feedwater line break within Containment to limit radioactive releases. (Isolation of all but safety injection and spray lines penetrating the Containment).

7.3.1.1.2 Analog Circuitry

The process analog sensors and racks for the Engineered Safety Features Actuation System are covered in Reference 1. Discussed in this report are the parameters to be measured including pressures, flows, tank and vessel water levels, and temperatures as well as the measurement and signal transmission considerations. These latter considerations include the basic current transmission system, transmitters, orifices and flow elements, resistance temperature detectors, and pneumatics. Other considerations covered are automatic calculations, signal condition and location and mounting of the devices.

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

Containment pressure is sensed by four physically separated differential pressure transmitters mounted by strong supports outside of the Containment, which are connected to the Containment atmosphere by stainless steel impulse tubing. The impulse lines are separated and protected and provided with isolation valving which conforms to Regulatory Guide 1.11 and GDC 56 with the exceptions stated in Reference 8.

The following is a description of those process channels not included in the Reactor Protection or Engineered Safety Features Actuation Systems which enable additional monitoring of in-containment conditions in the post loss of coolant accident recovery period. These channels are located outside of the Containment (with the exception of sump instrumentation) and are not affected by the accidents.

1. Refueling water storage tank level

   Three channels of level instrumentation are provided for the refueling water storage tank. Each channel has level indication on the main control board with one channel recorded. At RWST low level, two-out-of-three logic from all three channels initiates the automatic portion of switchover from injection to recirculation. In addition, redundant pre-low, low, and low-low level alarms are provided on the main control board through two-out-of-three logic from all three channels. These alarms alert the operator that the various necessary manual actions for completing the transfer to cold leg recirculation must be started. High level and make-up level alarms are also provided by separate instrumentation.

2. High head safety injection pumps discharge pressure

   These channels clearly show that the safety injection pumps are operating. The transmitters are outside the Containment.

3. Pump energization

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

4. Valve position

   All engineered safety features remote operated valves have position indication on the control board in two places to show proper positioning of the valves. Red and green indicator lights are located next to the manual control station showing open and closed positions. The engineered safety features positions of these valves are displayed on the monitor light panels, which consist of an array of white lights which are dark when the valves are in their required positions for normal power operations. The monitor lights for automatically actuated valves are energized when the valve is in the automatically actuated position. These monitor lights thus enable the operator to quickly assess the status of the Engineered Safety Features Systems. These indications are derived from contacts integral to the valve operators. In the cases of the accumulator isolation valves, redundancy of position indication is provided by valve stem mounted limit switches which actuate annunciators on the control board when the valves are not correctly positioned for engineered safety features actuation. The stem mounted switches are independent of the limit switches in the motor operators.

   In addition, the following local instrumentation is available:

   a. Residual heat removal pumps discharge pressure (indication provided in the Control Room).

   b. Residual heat exchanger exit temperatures (indication also provided in the Control Room).

   c. Containment spray test lines total flow.

   d. Safety injection test line pressure and flow.

5. Sump Instrumentation

   The Containment sump instrumentation consists of two trains of level devices designed to operate in a post accident environment.

   The transmitter housings are submergence qualified. The indicators and alarm system are located in the Control Room.

7.3.1.1.3 Digital Circuitry

The engineered safety features logic racks are discussed in detail in Reference 3. The description includes the considerations and provisions for physical and electrical separation as well as details of the circuitry. Reference 3 also covers certain aspects of on-line test provisions, provisions for test points, considerations for the instrument power source, considerations for accomplishing physical separation, and provisions for assuring instrument qualification. The outputs from the analog channels are combined into actuation logic as shown on Figure 7-1, Sheets 5 (T_{avg}), 6 (Pressurizer pressure), 7 (low steam pressure), 8 (engineered safety features actuation) and 14 (auxiliary feedwater).

To facilitate engineered safety features actuation testing, two cabinets (one per train) are provided which enable operation, to the maximum practical extent, of safety features loads on a group by group basis until actuation of all devices has been checked (See Reference 4). Final actuation testing is discussed in detail in Section 7.3.2.

7.3.1.1.4 Final Actuation Circuitry

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

1. Safety Injection System pump and valve actuators. See Chapter 6 for flow diagrams and additional information.
2. Containment Isolation [Phase A - "T" signal isolates all nonessential process lines on receipt of safety injection signal; Phase B - "P" signal isolates remaining process lines (which do not include safety injection lines) on receipt of 2/4 high-high Containment pressure signal]. For further information, see Section 6.2.4.
3. Service water pump and valve actuators (See Chapter 9).
4. Auxiliary feed pumps start (See Chapter 10).
5. Diesel start (See Chapter 8).
6. Feedwater isolation (See Chapter 10).
7. Ventilation isolation valve and damper actuators (See Chapter 6).
8. Steam line isolation valve actuators (See Chapter 10).

Deleted per 2012 Update.

If an accident is assumed to occur coincident with a blackout, the engineered safety features loads are sequenced, if necessary, onto the diesel generators to prevent overloading of the emergency power supply. This sequence is discussed in Chapter 8. The design meets the requirements of Criterion 35 of the 1971 GDC.

7.3.1.1.5 Support Systems

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

1. Nuclear Service Water System - Heat Removal (See Chapter 9).
2. Component Cooling Water System - Heat Removal (See Chapter 9).
3. Electrical Power Distribution Systems (See Chapter 8).

7.3.1.2 Design Bases Information

The functional diagrams presented in Figure 7-1, Sheets 5, 6, 7 and 8 provide a graphic outline of the functional logic associated with requirements for the Engineered Safety Features Actuation System. Requirements for the engineered safety features are given in Chapter 6. Given below is the design bases information requested in IEEE-279, 1971, Reference 2.

7.3.1.2.1 Unit Conditions

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

1. Primary System:
   a. Rupture in small pipes or cracks in large pipes
   b. Rupture of a reactor coolant pipe
   c. Steam generator tube rupture
2. Secondary System:
   a. Minor secondary system pipe breaks resulting in steam release rates equivalent to a single dump, relief or safety valve
   b. Rupture of a major steam pipe

7.3.1.2.2 Unit Variables

The following list summarizes the unit variables required to be monitored during each accident identified in the preceding section. Post accident monitoring requirements are given on Table 7-12 and Table 7-13.

1. Primary System Accidents
   a. Pressurizer pressure
   b. Containment pressure (not required for steam generator tube rupture)
2. Secondary System Accidents
   a. Pressurizer pressure
   b. Steam line pressures
   c. Reactor coolant average temperature (T_{avg})
   d. Containment pressure

7.3.1.2.3 Spatially Dependent Variables

The only variable sensed by the Engineered Safety Features Actuation System which has spatial dependence is reactor coolant temperature. The effect on the measurement is negated by multiple RTD measurements as described in Section 7.2.1.1.4 and Section 5.6.

7.3.1.2.4 Limits, Margins and Levels

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

7.3.1.2.5 Abnormal Events

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

1. Loss of coolant accident (See Section 15.6.5)
2. Steam breaks (See Section 15.1.5)
3. Earthquakes (See Chapter 2 and Chapter 3)
4. Fire (See Section 9.5.1)
5. Explosion (Hydrogen buildup inside Containment) (See Section 15.6.5)

6. Missiles (See Section 3.5)
7. Flood (See Chapter 2 and Chapter 3)

7.3.1.2.6 Minimum Performance Requirements

Minimum performance requirements are as follows:

1. System Response Times

   The ESF RESPONSE TIME shall be that time interval from when the monitored parameter exceeds its ESF actuation setpoint at the channel sensor until the ESF equipment is capable of performing its safety function (i.e., the valves travel to their required positions, pump discharge pressures reach their required values, etc.). Times shall include diesel generator starting and sequence loading delays, where applicable. The response time may be measured by means of any series of sequential, overlapping, or total steps so that the entire response time is measured. Refer to Section 7.2.2.2.3, "Evaluation of Compliance to Applicable Codes and Standards" regarding sensor response time testing. The response times to initiate engineered safety features are conservative. The values listed in Table 7-20 are maximum allowable times consistent with the accident analysis, and are systematically verified during unit start-up tests. These maximum delay times thus include all compensation and therefore require that any such network be aligned and operating during verification testing.

   Engineered Safety Features Actuation accuracies are calculated for various initiative functions by approved, conservative methodologies.

7.3.1.3 Final System Drawings

Functional block diagrams, electrical elementaries and other drawings as required to assure electrical separation and to perform a safety review are provided in Reference 6.

7.3.2 Analysis

7.3.2.1 Failure Mode and Effects Analyses

A failure mode and effects analyses is in progress for equipment in the scope of Westinghouse. Due to similarities between the Reactor Protection System and Engineered Safety Features Actuation System, it is expected that the results of this study will be comparable to the results presented in WCAP-7706, Reference 5. Also several of the logic functions discussed in WCAP-7706 are shared by the Reactor Protection System and the Engineered Safety Features Actuation System.

7.3.2.2 Compliance with Standards and Design Criteria

Discussion of the NRC General Design Criteria is provided in various sections of Chapter 7, "Instrumentation and Controls" where a particular GDC is applicable. Applicable GDC's include Criteria 13, 20, 21, 22, 23, 24, 35, 37, 40, 43 of the 1971 General Design Criteria. Compliance with certain IEEE Standards is presented in Section 7.1.2.1. Compliance with Regulatory Guide 1.22 is discussed in Section 7.1.2.1. Compliance with Regulatory Guide 1.47 is discussed in Section 7.8.2. The discussion given below shows that the Engineered Safety Features Actuation System complies with IEEE 279, 1971, Reference 2.

7.3.2.2.1 Single Failure Criteria

For manually controlled electrically operated valves used in an engineered safety feature system or essential auxiliary system, for which removal of power to the valve is necessary to meet the single failure criterion, the following requirements apply:

1. Technical Specifications include a list of all valves that have power removed and the required positions of these valves.
2. Redundant indication is provided in the Control Room.
3. Power to active valves can be re-applied consistent with the time allowed for the valve to be operational.

Refer to Section 6.3.2.16 for discussion on valves requiring removal of power.

The discussion presented in Section 7.2.2.2.3 is applicable to the Engineered Safety Features Actuation System, with the following exception. In the Engineered Safety Features Actuation System, a loss of instrument power calls for actuation of engineered safety features equipment controlled by the specific bistable that lost power (Phase B excepted). The actuated equipment must have power to comply. The power supply for the protection systems is discussed in Section 7.6 and Chapter 8. For Phase B, the final bistables are energized to trip to avoid spurious actuation.

This is considered acceptable because Phase B on high-high Containment pressure signal provides automatic initiation of the system via protection channels meeting the criteria in Reference 2. Moreover, all engineered safety features equipment (valves, pumps, etc.) can be individually manually actuated from the control board. Hence, a secondary means of Phase B is available. The design meets the requirements of Criteria 21 and 23 of the 1971 GDC.

7.3.2.2.2 Equipment Qualification

Equipment qualifications are discussed in Section 3.11.

7.3.2.2.3 Channel Independence

The discussion presented in Section 7.2.2.2.3 is applicable. The engineered safety features outputs from the solid state logic protection cabinets are redundant, and the actuations associated with each train are energized up to and including the final actuators by the separate a.c. power supplies which power the logic trains.

7.3.2.2.4 Control and Protection System Interaction

The discussions presented in Section 7.2.2.2.3 are applicable.

7.3.2.2.5 Capability for Sensor Checks and Equipment Test and Calibration

The discussions of system testability in Section 7.2.2.2.3 are applicable to the sensors, analog circuitry, and logic trains of the Engineered Safety Features Actuation System.

The following discussions cover those areas in which the testing provisions differ from those for the Reactor Protection System:

1. Testing of Engineered Safety Features Actuation System

   The Engineered Safety Features Systems are tested to provide assurance that the systems operate as designed and are available to function properly in the unlikely event of an accident. Engineered safety features test cabinets are discussed in WCAP-7705, Reference

4. The testing program meets the requirements of Criteria 21, 37, 40 and 43 of the 1971 GDC and Regulatory Guide 1.22 as discussed in Section 7.1.2.1. The program is as follows:

   a. Prior to initial unit operations, Engineered Safety Features System tests are conducted.

   b. Subsequent to initial startup, Engineered Safety Features System tests are conducted during each regularly scheduled refueling outage.

   c. During on-line operation of the reactor, all of the engineered safety features analog and logic circuitry are fully tested. In addition, most of the engineered safety features final actuators are fully tested. The remaining few final actuators whose operation is not compatible with continued on-line unit operation are checked by means of continuity testing.

   d. During normal operation, the operability of testable final actuation devices of the engineered safety features are tested by manual initiation from the Control Room.

2. Performance Test Acceptability Standard for the “S” (Safety Injection Signal) and for the “P” (the Automatic Demand Signal for Phase B Actuation Signals Generation.

   During reactor operation the basis for Engineered Safety Features Actuation Systems acceptability is the successful completion of the overlapping tests performed on the initiating system and the Engineered Safety Features Actuation Systems. Checks of process indications verify operability of the sensors. Analog checks and tests verify the operability of the analog circuitry from the input of these circuits through to and including the logic input relays. Solid state logic testing checks the digital signal path from and including logic input relay contacts through the logic matrices and master relays and perform continuity tests on the coils of the output slave relays; final actuator testing operates the output slave relays and verifies operability of those devices which require safeguards actuation and which can be tested without causing unit upset. A continuity check is performed on the actuators of the untestable devices. Operation of the final devices is confirmed by control board indication and visual observation that the appropriate pump breakers close and automatic valves shall have completed their travel.

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

   Maintenance checks (performed during regularly scheduled refueling outages), such as resistance to ground of signal cables in radiation environments are based on qualification test data which identifies what constitutes acceptable radiation, thermal, etc. degradation.

3. Frequency of Performance of Engineered Safety Features Actuation Tests

   During reactor operation, complete system testing (excluding sensors or those devices whose operation would cause unit upset) is performed. Testing, including the sensors, is also performed during scheduled unit shutdown for refueling.

4. Engineered Safety Features Actuation Test Description

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

   a. The test procedures must not involve the potential for damage to any unit equipment.

   b. The test procedures must minimize the potential for accidental tripping.

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

5. Description of Initiation Circuitry

   Several systems comprise the total Engineered Safety Features System, the majority of which may be initiated by difference process conditions and be reset independently of each other.

   The remaining functions (listed in Section 7.3.1.1.1) are initiated by a common signal (safety injection) which in turn may be generated by different process conditions.

   In addition, operation of all other vital auxiliary support systems, such as Auxiliary Feedwater, Component Cooling and Nuclear Service Water, is initiated by the safety injection signal.

   Each function is actuated by a logic circuit which is duplicated for each of the two redundant trains of engineered safety features initiation circuits.

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

6. Analog Testing

   Analog testing is identical to that used for reactor trip circuitry and is described in Section 7.2.3.3. Briefly, in the analog racks, proving lamps and analog test switches are provided. Administrative control requires, during bistable testing, that the bistable output be put in a trip condition by placing the test switch in the test position. This action connects the proving lamp to the bistable and disconnects and thus de-energizes (operates) the bistable output relays in Train A and Train B cabinets and allows injection of a test signal to the channel. Relay logic in the process cabinets automatically blocks the test signal unless the bistable amplifier is tripped. This is only done on one channel at a time. Status lights and single channel trip alarms in the main Control Room confirm that the bistable relays have been de-energized and the bistable outputs are in the trip mode. An exception to this is Phase B, which is energized to actuate 2/4 and reverts to 2/3 when one channel is in test.

   A signal is then inserted through a test jack. Verification of the bistable trip setting is now confirmed by the proving lamp.

7. Solid State Logic Testing

   After the individual channel analog testing is complete, the logic matrices are tested from the Train A and Train B logic rack test panels. This step provides overlap between the analog and logic portions of the test program.

   During this test, each of the logic inputs is actuated automatically in all combinations of trip and non-trip logic. Trip logic is not maintained sufficiently long enough to permit master relay actuation -- master relays are “pulsed” in order to check continuity. Following the logic testing, the individual master relays are actuated electrically to test their mechanical operation. Actuation of the master relays during this test applies low voltage to the slave relay coil circuits to allow continuity checking, but not slave relay actuation. During logic testing of one Train, the other Train can initiate the required engineered safety features function. For additional details, see Reference 3.

8. Actuator Testing

At this point, testing of the initiation circuits through operation of the master relay and its contacts to the coils of the slave relays has been accomplished. Slave relays do not operate because of reduced voltage.

In the next step, operation of the slave relays and the devices controlled by their contacts is checked. For this procedure, control switches mounted on a safeguards test cabinet panel in the logic rack area are provided for each slave relay. These controls are of the type that require two deliberate actions on the part of the operator to actuate a slave relay. By operation of these relays one at a time through the control switches, all devices that can be operated on line are tested. Devices are assigned to the slave relays such that no undesired effect on unit operation occurs. This procedure minimizes upset to the unit and again assures that overlap in the testing is continuous, since the normal power supply for the slave relays is utilized.

During this last procedure, close communication between the Control Room operator and Personnel at the test panel is required. Prior to the energizing of a slave relay, the operator in the main Control Room assures that unit conditions permit operation of the equipment that is actuated by the relay. After the tester has energized the slave relay, the Control Room operator observes that all equipment has operated as indicated by appropriate indicating lamps, monitor lamps and annunciators on the control board, and, using a prepared check list, records all operations. For equipment whose operation is undesired, the circuit can be placed in a condition where the relay contact operation can be verified by continuity without operation of the equipment. The operator then resets all devices and prepares for operation of the next slave relay actuated equipment.

The following tests cannot be completely initiated on line due to operation restraints.

CLOSING THE MAIN STEAM LINE ISOLATION VALVES

Main steam isolation valves are routinely tested during refueling outages. Testing of the main steam isolation valves to closure at power is not practical. As the plant power is increased, the core average temperature is programmed to increase. If the valves are closed under these elevated temperature conditions, the steam pressure transient would unnecessarily operate the steam generator relief valves and possibly the steam generator safety valves. The steam pressure transient produced would cause shrinkage in the steam generator level, which would cause the reactor to trip on low-low steam generator water level. Testing during operation will decrease the operating life of the valve.

Based on the above identified problems incurred with periodic testing of the main steam line isolation valves at power and since 1) no practical system design will permit operation of the valves without adversely affecting the safety or operability of the plant, 2) the probability that the protection system will fail to initiate the actuated equipment is acceptably low due to test up to final actuation, and 3) these valves will be routinely tested during refueling outages, the proposed resolution meets the requirements of the exceptions of Section D.4 of Regulatory Guide 1.22.

CLOSING THE FEEDWATER CONTROL VALVES

These valves are routinely tested during refueling outages. To close them at power would adversely affect the operability of the plant. The verification of operability of feedwater control valves at power is assured by confirmation of proper operation of the steam generator water level system. The actual actuation function of the solenoids, which provides the closing function is periodically tested at power as discussed in Section 7.3.2.2.5, 9. The operability of the slave relay which actuates the solenoid, which is the actuating device, is verified during this test. Although the actual closing of these control valves is blocked when

the slave relay is tested, all functions are tested to assure that no electrical malfunctions have occurred which could defeat the protective function. It is noted that the solenoids work on the de-energize to actuate principle, so that the feedwater control valves will fail closed upon either the loss of electrical power to the solenoids or loss of air pressure.

Based on the above, the testing of the isolation function of feedwater control valves meets the requirements of the exceptions of Section D.4 of Regulatory Guide 1.22.

CLOSING THE FEEDWATER ISOLATION VALVES

The feedwater isolation valves are routinely tested during refueling outages. Periodic testing of these feedwater isolation valves, closing them completely or partially, at power would induce steam generator water level transients and oscillations which would trip the reactor.

These transient conditions would be caused by perturbing the feedwater flow and pressure conditions necessary for proper operation of the variable-speed feedwater pump control system and the steam generator water level control system. Any operation which induces perturbations in the main feedwater flow, whether deliberate or otherwise, generally leads to a reactor trip and should be avoided. It is noted that these valves will fail closed upon the loss of DC power to either Train A or Train B solenoids.

Based on these identified problems incurred with periodic testing of the backup feedwater valves at power and since 1) no practical system design will permit operation of these valves without adversely affecting the safety or operability of the plant, 2) the probability that the protection system will fail to initiate the activated equipment is acceptably low due to testing up to final actuation, and 3) these valves will be routinely tested during refueling outages, the proposed resolution meets the requirements of the exceptions of Section D.4 of Regulatory Guide 1.22.

TRIPPING THE FEEDWATER PUMP TRIP SOLENOIDS

These functions are not directly related to safety, but are provided for precautionary and economical reasons and are not subject to the same testability guidelines as the protection system. Nevertheless, these functions are routinely tested during refueling outages.

9. Actuator Blocking and Continuity Test Circuits

For the limited number of components that cannot be operated on line as discussed in the preceding paragraph, additional blocking relays are provided which allow operation of the slave relays without actuation of the associated engineered safety features devices. Interlocking prevents blocking the output of more than one slave relay at a time. The circuits provide for monitoring of the slave relay contacts, the devices' control circuit cabling, control voltage and the devices' actuating solenoids.

For circuits with contact closure for protection function actuation, the slave relay contact, in series with device, is normally open, the blocking relay is normally closed, and the test lamp is normally energized. To check: open the blocking relay contact in series with lamp connections - the test lamp should be de-energized; close the blocking relay contact in series with the lamp connections - the test lamp should now be energized. The circuit is now in its “normal” i.e., operable condition.

For circuits with contact opening for protection function actuation, the slave relay contact in series with device is normally closed, the blocking relay contact in series with the green lamp is normally open, the white test lamp is normally energized, and the green test lamp is normally de-energized. To check: close the blocking relay - the green test lamp should not be energized also; open this blocking relay contact - the green test lamp should be de-energized. The circuit is now in its “normal” i.e., operable conditions.

The continuity test circuits for these components that cannot be actuated on line are discussed as follows in Appendix B of Reference 6 (WCAP-7705). The typical schemes for blocking operation of selected[1] protection function actuator circuits are shown in Figure 7-5 as details A and B. The schemes operate as explained below and are duplicated for each safeguards train.

Detail A shows the circuit for contact closure for protection function actuation. Under normal plant operation, and equipment not under test, the test lamps “DS*” for the various circuits will be energized. Typical circuit path will be through the normally closed test relay contact “K8*” and through test lamp connections 1 to 3. Coil “X2” will be capable of being energized for protection function actuation upon closure of solid state logic output relay contacts “K*”. Coil “X2” is typical for a breaker closing auxiliary coil, motor starter master coil, coil of a solenoid valve, auxiliary relay, etc. When the contacts “K8*” are opened to block energizing of coil “X2”, the white lamp is de-energized.

Detail B shows the circuit for contact opening for protection function actuation. Under normal plant operation, and equipment not under test, the white test lamps “DS*” for the various circuits will be energized, and green test lamp “DS*” will be de-energized. Typical circuit path for white lamp “DS*” will be through the normally closed solid state logic output relay contact “K*” and through test lamp connections 1 to 3. Coil “Y2” will be capable of being de-energized for protection function actuation upon opening of solid state logic output relay contact “K*”. Coil “Y2” is typical for a solenoid valve coil, auxiliary relay, etc. When the contacts “K8*” are closed to block de-energizing of coil “Y2”, the green test lamp is energized.

10. Time Required for Testing

    The analog testing can be performed at a rate of several channels per hour. Logic testing can be performed in less than 30 minutes. Testing of actuated components (including those which can only be partially tested) is a function of Control Room operator availability. It requires several shifts to accomplish these tests. During this procedure automatic actuation circuitry will override testing, except for those few devices associated with a single slave relay whose outputs must be blocked and then only while blocked. Continuity testing associated with a blocked slave relay will take several minutes. During this time the redundant devices in the other trains would be functional.

11. Summary

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

    The procedures require testing at various locations.

    a. Analog testing and verification of bistable setpoint are accomplished at process analog racks. Verification of bistable relay operation is done at the main Control Room status lights.

[1] Circuits that cannot be actuated without causing a plant upset or equipment damage.

b. Logic testing through operation of the master relays and low voltage application to slave relays is done at the logic rack test panel.

c. Testing of pumps, fans and valves is done at a test panel located in the vicinity of the logic racks in combination with the Control Room Operator.

d. Continuity testing for those circuits that cannot be operated is done at the same test panel mentioned in 11c.

12. Testing During Shutdown

Emergency Core Cooling System tests are performed at each major fuel reloading. With the Reactor Coolant System pressure less than or equal to 350 psig and temperature less than or equal to 350°F, a test safety injection signal is applied to initiate operation of the system. This test is discussed further in Section 6.3.4.

7.3.2.2.6 Deleted Per 2008 Update

7.3.2.3 Further Considerations

In addition to the considerations given above, a loss of instrument air or loss of component cooling water to vital equipment has been considered. Neither the loss of instrument air nor the loss of cooling water (assuming no other accident conditions) can cause safety limits as given in Technical Specifications to be exceeded. Likewise, loss of either one of the two does not adversely affect the core or the Reactor Coolant System nor does it prevent an orderly shutdown if this is necessary. Furthermore, all pneumatically operated valves and controls assume a preferred operating position upon loss of instrument air. It is also noted that, for conservatism during the accident analyses (Chapter 15), credit is not taken for the instrument air systems nor for any control system benefit.

7.3.2.4 Summary

The effectiveness of the Engineered Safety Features Actuation System is evaluated in Chapter 15, based on the ability of the system to contain the effects of Condition III and IV faults, including loss of coolant and steam break accidents. The Engineered Safety Features Actuation System parameters are based upon the component performance specifications which are given by the manufacturer or verified by test for each component. Appropriate factors to account for uncertainties in the data are factored into the constants characterizing the system.

The Engineered Safety Features Actuation System must detect Condition III and IV faults and generate signals which actuate the engineered safety features. The system must sense the accident condition and generate the signal actuating the protection function reliably and within a time determined by and consistent with the accident analyses on Chapter 15.

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

Operating procedures require that the complete Engineered Safety Features Actuation System normally be operable. However, redundancy of system components is such that the system operability assumed for the safety analyses can still be met with certain instrumentation channels out of service. Channels that are out of service are to be placed in the tripped mode or bypass mode in the case of Phase B.

7.3.2.4.1 Loss of Coolant Protection

By analysis of loss of coolant accident and in system tests it has been verified that except for very small coolant system breaks which can be protected against by the charging pumps followed by an orderly shutdown, the effects of various loss of coolant accidents are reliably detected by the low pressurizer pressure signal; the Emergency Core Cooling System (Safety Injection System) is actuated in time to prevent or limit core damage.

For large coolant system breaks the passive accumulators inject first, because of the rapid pressure drop. This protects the reactor during the unavoidable delay associated with actuating the active Emergency Core Cooling System phase.

High Containment pressure also actuates the Safety Injection System. Therefore, emergency core cooling actuation can be brought about by sensing this other direct consequence of a primary system break; that is, the Engineered Safety Features Actuation System detects the leakage of the coolant into the Containment. The generation time of the actuation signal of about 1.0 second, after detection of the consequences of the accident, is adequate.

Containment spray provides additional emergency cooling of Containment and also limits fission product release upon manual actuation once recirculation mode has initiated to mitigate the effects of a loss of coolant accident.

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

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

7.3.2.4.2 Steam Break Protection

The Safety Injection System is also actuated in order to protect against a steam line break. About 2.0 seconds elapses between sensing low pressurizer pressure and generation of the actuation signal. Analysis of steam break accidents assuming this delay for signal generation shows that the Safety Injection System is actuated for a steam break in time to limit or prevent further core damage for steam break cases. There is a reactor trip but the core reactivity is further reduced by the highly borated water injected by the Safety Injection System.

Additional protection against the effects of steam break is provided by feedwater isolation which occurs upon actuation of the Safety Injection System. Feedwater line isolation is initiated in order to prevent excessive cooldown of the reactor vessel and thus protect the Reactor Coolant System boundary.

Additional protection against a steam break accident is provided by closure of all steam line isolation valves in order to prevent uncontrolled blowdown of all steam generators. The generation of the protective system signal (about 2.0 seconds) is again short compared to the time to trip the fast acting steam line isolation valves which are designed to close in less than approximately eight seconds.

In addition to actuation of the engineered safety features, the effect of a steam break accident also generates a signal resulting in a reactor trip on overpower or following Safety Injection System actuation. However, the core reactivity is further reduced by the high borated water injection by the Safety Injection System.

When pressurizer pressure is below the P-11 setpoint, the operator can manually block the low steamline pressure signal to prevent steamline isolation during a normal shutdown. Blocking the low steamline pressure signal automatically activates steamline pressure rate instrumentation for steam break protection during normal plant cooldown. A high rate of change in steamline pressure initiates the steamline isolation. When pressurizer pressure increases above the P-11 setpoint, low steamline pressure protection is automatically reinstated and steam pressure rate protection is removed. Provisions are made to manually reinstate low steamline pressure protection at any time.

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

7.3.3 References

1. Reid, J. B., Process Instrumentation for Westinghouse Nuclear Steam Supply System (4 Loop Plant using *WC*ID 7300 Series Process Instrumentation, Westinghouse Electric Corporation, *WCAP-7913*, (Non-Proprietary).
2. The Institute of Electrical and Electronics Engineers, Inc., IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations, IEEE Std. 279-1971.
3. Katz, D. N., Solid State Logic Protection System Description, Westinghouse Electric Corporation, *WCAP-7488-L*, January, 1971, (Westinghouse NES Proprietary); and *WCAP-7672*, June, 1971, (Non-proprietary).
4. Haller, J. T., Engineered Safeguards Final Device or Actuator Testing, *WCAP-7705*, March 1973.
5. Gangloff, W. C., and Lofus, W. D., An Evaluation of Solid State Reactor Protection in Anticipated Transients, Westinghouse Electric Corporation, *WCAP-7706L* (Westinghouse NES Proprietary) and *WCAP-7706* (Non-Proprietary) July, 1971.
6. McGuire Drawing System
7. Letter from W. O. Parker, Jr. (Duke) to H. R. Denton (NRC) dated October 14, 1980. Subject: Override, Bypass or Reset of ESF Actuation Signal.
8. MC-1210.05, Memo to file, dated 8/19/1982, Instrument Line Containment Vessel Penetrations and Isolation Devices.
9. Deleted Per 2002 Update.
10. Deleted Per 2002 Update.
11. Nuclear Regulatory Commission, Letter to All Licensees of Operating Reactors, Applicants for Operating Licenses and Holders of Construction Permits for Light Water Reactor Power Plants, from James G. Partlow, September 20, 1989, "Request for Action Related to the Resolution of Unresolved Issue A-47, 'Safety Implication of Control Systems in LWR Plants' Pursuant to 10 CFR 50.54(f) (Generic Letter 89-19)."
12. Duke Power Company, Letter from H.B. Tucker to NRC, March 19, 1990, re: Response to Generic Letter 89-19, "Request for Action Related to the Resolution of Unresolved Issue A-47, 'Safety Implication of Control Systems in LWR Plants' Pursuant to 10 CFR 50.54(f)."

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.3.

THIS PAGE LEFT BLANK INTENTIONALLY.

7.4 Systems Required for Safe Shutdown

The functions necessary for safe shutdown are available from instrumentation channels that are associated with the major systems in both the primary and secondary of the Nuclear Steam Supply System. These channels are normally aligned to serve a variety of operational functions. There are not identifiable safe shutdown systems per se. However, prescribed procedures for securing and maintaining the unit in a safe condition can be instituted by appropriate alignment of selected systems. The discussion of these systems together with the applicable codes, criteria and guidelines is found in other sections of the Safety Analysis Report. The alignment of shutdown functions associated with the engineered safety features actuation which are invoked under postulated limiting fault situations is discussed in Chapter 6, and Section 7.3.

The instrumentation and control functions which are identified as being required for maintaining safe shutdown of the reactor are by definition the minimum number under non-accident conditions. These functions permit the necessary operations that:

1. Prevent the reactor from achieving criticality in violation of the Technical Specifications and
2. Provide an adequate heat sink such that design and safety limits are not exceeded.

7.4.1 Description

The designation of systems that can be used for obtaining and maintaining a normally safe shutdown depends on identifying those systems which provide the following capabilities:

1. Boration with related charging and letdown capability
2. Adequate supply for auxiliary feedwater
3. Residual heat removal.

7.4.1.1 Auxiliary Feedwater System

The Auxiliary Feedwater System (AFS) design is described in Section 10.4.10, and Figure 10-47 and Table 10-9, Table 10-10, Table 10-12, and Table 10-13. The instrumentation and controls for this system are presented below.

7.4.1.1.1 System Description

7.4.1.1.1.1 Initiating Circuits and Logic

The AFS is designed for operation during plant startup, a plant shutdown and emergency conditions where normal feedwater is not available. The AFS can be started and controlled from either the Control Room or control panels local to the pumps. During normal plant operation the AFS valves are positioned in such a manner that on an automatic start, auxiliary feedwater is available with no safety signal needed to align the valves.

The motor driver auxiliary feedwater pumps start automatically and provide flow on any one of the following conditions:

1. Two out of four low-low level alarms in any steam generator.
2. Loss of all main feedwater pumps.
3. Initiation of the Safety Injection Signal.
4. Loss of off-site and station normal auxiliary power (blackout).

The turbine driven auxiliary feedwater pump starts automatically and provides flow on either one of the following conditions:

1. Two out of four low-low level alarms in any two (2) steam generators.
2. Loss of offsite and station normal auxiliary power (blackout).

The controls of this pump have been modified so that automatic start of the pump due to above signals is sealed in thus requiring manual shutdown of the pump after an automatic start (Ref. 2, Section 7.4.3).

An automatic start due to a low-low steam generator level or a safety injection signal is initiated by the Engineered Safety Features Systems as described in Section 7.3 and shown in logic form on Figure 7-1. The automatic start of the motor driven pumps due to a blackout is initiated by the sequencer as described in Section 8.3.1.1.4 and Table 8-1.

Safety grade indication of the AFS flow to each steam generator is provided in the control room persuent to requirements of NUREG-0694. This instrumentation meets the emergency power diversity requirements as for AFS system so setforth in the standard Review Plan 10.4.9 (Ref. 3, Section 7.4.3).

An automatic start of the auxiliary feedwater motor driven pumps due to either a low-low level in a steam generator or loss of both main feedwater pumps is blocked by either a Safety Injection Signal or a blackout signal. The pumps are then started by the sequencing system.

7.4.1.1.1.2 Redundancy

The motor driven pumps (each 100 percent capacity) are redundant in that each receives power from a different safety train of the Essential Auxiliary Power System. The 200 percent capacity turbine driven pump can be started by means of a signal from either safety train.

7.4.1.1.1.3 Sequencing

The auxiliary feedwater motor driven pumps are sequentially loaded on the Essential Auxiliary Power System during a blackout.

7.4.1.1.1.4 Diversity

Because the Auxiliary Feedwater System uses both motor driven and steam turbine driven pumps, this system has power diversity.

The AFS has various sources for pump suction supply. The AFS is normally aligned to the AFS storage tank and the AFS condensate storage tanks. During a blackout or low AFS normal suction pressure, both trains of Nuclear Service Water System are automatically accessible for auxiliary feedwater supply.

Control diversity exists because the AFS can be completely controlled from panels local to the pumps or from the Control Room.

7.4.1.1.1.5 Actuated Devices

The only devices in the AFS which are activated during an automatic start are the pumps, as described in Section 7.4.1.1.1.1.

An automatic start of the auxiliary feedwater motor driven pumps due to either a low-low level in a steam generator or trip of both main feed pumps can be manually defeated in the Control

Room. This allows the operator to stop the auxiliary feedwater pumps during plant shutdown. Whenever the automatic start mode is defeated an alarm is present in the Control Room.

7.4.1.1.1.6 Supporting Systems

The Essential Auxiliary Power System supplies power for pump motors, various valves and control power as described in Sections 8.3.1.1.1, 8.3.1.1.6 and 8.3.2.1.4.

The Nuclear Service Water System is described in Section 7.4.1.2.

7.4.1.1.1.7 Logic Diagrams

See Figure 7-1.

7.4.1.1.1.8 P & I Diagrams

See Figure 10-47

7.4.1.1.1.9 Electrical Schematics

See series of drawing MCEE 147-00 found in the McGuire Nuclear Station Electrical Schematics.

7.4.1.1.1.10 Location and Layout

See Figure 1-3

7.4.1.1.1.11 Controls and Instrumentation Outside of Control Room

The following controls and instrumentation are needed to operate the AFS and are located at the pumps:

1. Instrumentation
   a. Each steam generator level
   b. Each steam generator pressure
   c. Auxiliary feedwater flow to each steam generator
   d. Suction pressure for each pump
   e. Discharge pressure for each pump
   f. Auxiliary feedwater turbine steam pressure
   g. Auxiliary feedwater turbine speed
   h. Position (0-100% open) for all pneumatic control valves
   i. Position (open/close) for all motor operated valves
   j. Auxiliary feedwater control valve reset status
2. Controls
   a. Control (0-100% Open) of all pneumatic control valves
   b. Control (Open/Close) of all motor operated valves
   c. Start/Stop control for each pump

d. Auxiliary feedwater control valve reset switches

7.4.1.1.2 Design Basis Information

The design basis for the Auxiliary Feedwater System instrumentation is to provide a system to deliver feedwater to the steam generators during normal startup, shutdown, and hot standby. This system also provides feedwater to the steam generators during emergency conditions such as main steam line break, loss of normal feedwater and blackout.

Other information required by Section 3 of IEEE 279-1971 is contained in Sections 7.4.1.1.1 and 10.4.7.2.

7.4.1.1.3 Analysis

There are no specific NRC Regulatory Guides or General Design Criteria applicable to this instrumentation.

The requirements of IEEE 279-1971 are written for protection systems as defined in the scope of that standard, and as such, are not directly applicable to this instrumentation. A discussion of the extent to which the design of this sytem's instrumentation meets the applicable portions of IEE 279-1971 is provided below in compliance with the NRC Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants.

The following refers to the requirements set forth in Section 4 of IEEE 279-1971:

7.4.1.1.3.1 General Functional Requirements

The Auxiliary Feedwater System instrumentation essential to the system safety function is designed for operation under the environmental conditions specified in Section 3.11.

7.4.1.1.3.2 Single Failure Criterion

Any single failure of the Auxiliary Feedwater System instrumentation affects only the Auxiliary Feedwater line to which it is associated, and will in no way affect the operation of the parallel line to the same steam generator or the redundant lines feeding the other steam generator.

7.4.1.1.3.3 Quality of Components and Modules

Components of the Auxiliary Feedwater System instrumentation are of a quality consistent with the requirements of 10CFR50.65, "Maintenance Rule Program."

7.4.1.1.3.4 Channel Integrity

The instrumentation associated with the Auxiliary Feedwater System which is essential to the system's function, is designed to maintain the necessary functional capability under the environmental conditions specified in Section 3.11.

7.4.1.1.3.5 Channel Independence

The Auxiliary Feedwater System instrumentation for one train is physically and electrically isolated from that of the redundant train.

7.4.1.1.3.6 Control and Protection System Interaction

The Auxiliary Feedwater System instrumentation meets the requirements of Section 4.7 of IEEE 279-1971, as stated in Section 7.4.1.1.1.

7.4.1.1.3.7 Derivation of System Inputs

Steam generator pressure, steam generator level and auxiliary feedwater flow are the signals used for this instrumentation.

7.4.1.1.3.8 Operating Bypasses

Refer to Section 7.4.1.1.1 for bypasses and interlocks.

7.4.1.2 Nuclear Service Water System

The Nuclear Service Water (NSW) System design is described in Section 9.2.2 and Figure 9-31. The instrumentation and controls for these systems are presented below.

7.4.1.2.1.1 Initiating Circuits

The NSW system normally operates under manual control by the plant operator. Safety mode operation is initiated by actuation of the Safety Injection Signal, Containment Isolation Signal, or loss of offsite power. The realignment process is fully automatic. The initiation signals override the normal manual control.

7.4.1.2.1.2 Logic

In the normal manual control mode of operation, only one of the redundant NSW trains is in operation per unit. The suction and discharge is shared by both units. On receipt of a Safety Injection Signal both trains of the affected unit align automatically. Train A suction and discharge align to Lake Norman. Train B suction and discharge align to the Standby Nuclear Service Water Pond (SNSWP). Isolation valves supplying various safety related heat exchangers are opened, the crossover valves between trains are closed and the Auxiliary Building non-essential isolation valves are closed. Both NSW pumps of the affected unit receive a signal to start. A Containment isolation signal closes the Reactor Building nonessential isolation valves. The realignment process does not require operator action. The remaining unit is unaffected by the safety mode actuation in the other, with the exception of the common valve alignment. Water level and temperature of the SNSWP is monitored in the Control Room. The SNSWP instrumentation is not required to perform safety related functions.

7.4.1.2.1.3 Bypasses

There are no bypasses capable of preventing the Safety Injection Signal from performing its intended function. However, the non-essential equipment supply and isolation valves are blocked from closing during test. Testing of the remainder of the initiation circuits results in a functional test of the actuated device. Access to test switches is administratively controlled.

7.4.1.2.1.4 Interlocks

There are no interlocks capable of blocking the safety injection signal. The NSW strainer motors and backwash pump motors are interlocked with their respective NSW pumps so that the strainer and backwash pump motors will run while in automatic control when the NSW pump is running. The component cooling water heat exchanger isolation valves are interlocked with their

respective NSW pumps so that the valve will open when the NSW pump starts. Since the intake and discharge is shared by both units, the valves used in safety mode alignment may receive safety injection signals from either unit. These signals are interlocked using isolation relays to maintain unit separation. The NSW pumps are interlocked with their respective Motor Driven Auxiliary Feedwater (MDCA) pumps such that the NSW pump will automatically start when the MDCA pump starts. This interlock provides assurance that the NSW suction source is available for the Auxiliary Feedwater System.

7.4.1.2.1.5 Sequencing

Nuclear Service Water System equipment is sequentially loaded on the Essential Auxiliary Power System following safety mode initiation under the conditions described in Section 8.3.1.1.7 and in the order shown in Table 8-1.

7.4.1.2.1.6 Redundancy

The two trains of NSW equipment per unit are completely redundant. In the event of Control Room evacuation, start/stop controls for the NSW pumps have been provided on the auxiliary shutdown control panel.

7.4.1.2.1.7 Diversity

Operating conditions requiring safety mode actuation of the Nuclear Service Water System are detected by diverse means.

7.4.1.2.1.8 Actuated Devices

Devices in the Nuclear Service Water System actuated by the Safety Injection and Containment Isolation Signals are shown in Figure 7-6 and include the nuclear service water pumps, air and motor operated valves.

7.4.1.2.1.9 Supporting Systems

The NSW System receives electrical power from the Essential Auxiliary Power System which is described in Section 8.3.

7.4.1.2.1.10 Design Bases

The control and instrumentation for the Nuclear Service Water System is designed to provide reliable and continuous control of system equipment under all plant operating conditions. The controls provide for manual operation of the system under normal conditions with overriding automatic controls to realign equipment to a safety mode of operation at the onset of abnormal plant conditions. Control and instrumentation is designed to maintain the separation and redundancy provided by the mechanical design of the system, which provides two isolated full capacity trains of equipment. Section 3 of IEEE 279-1971 addresses the monitoring and detection of plant operating conditions requiring protective action. The required monitoring and detection capability is not provided directly in the NSW instrumentation and control systems. Instead, these functions are performed externally in the Solid State Protection System (SSPS) and safety mode actuation is accomplished through control interfaces, implemented as control outputs provided in the SSPS rather than the Nuclear Service Water System. The SSPS is discussed in Section 7.3. The Essential Auxiliary Power System is discussed in Section 8.3.

7.4.1.2.1.11 Logic Diagrams

See Figure 7-6.

7.4.1.2.1.12 P & I Diagrams

See Figure 9-31.

7.4.1.2.2 Analysis

7.4.1.2.2.1 Conformance to IEEE-279

IEEE 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations”, establishes minimum requirements for the reactor protective and engineered safety features instrumentation and control systems. The instrumentation and controls associated with the safe shutdown systems are not defined as a protective system in IEEE-279; however, many criteria of IEEE-279 have been incorporated in the design of the instrumentation and controls for safe shutdown systems. The instrumentation and controls required for safe shutdown are designed and arranged such that no single failure can prevent a safe shutdown, even in the event of loss of off-site power. Single failures considered include electrical faults (e.g., fires, missiles) resulting in mechanical damage. Compliance with single failure criterion is accomplished by providing redundancy of power supplies, actuation circuits, and by separating the redundant elements electrically and physically to achieve the required independence.

7.4.1.2.2.2 Consideration of Selected Plant Contingencies

1. Loss of Instrument Air Systems - The pneumatic valves which are essential during safety injection fail in the safe mode upon loss of instrument air or otherwise have a backup safety related air source. All other control is electrical and powered from the emergency power system.
2. Plant Load Rejection, Turbine Trip and loss of offsite power - In the event of loss of offsite power associated with plant load rejection or turbine trip, power for safe shutdown is provided by the on-site emergency power system. The description and analysis of the emergency power system are discussed fully in Section 8.3. The emergency diesel generators provide power for operation of pumps and valves. The station batteries provide dc power for operation of control and instrumentation systems required to actuate and control essential components.
3. Loss of Cooling Water to Vital Equipment - None of the Instrumentation and controls required for safe shutdown rely on cooling water for operation.

7.4.1.3 Component Cooling Water System

The Component Cooling Water System is described in Section 9.2.2 and Figure 9-57. The instrumentation and controls are presented below.

7.4.1.3.1 Description

7.4.1.3.1.1 Initiating Circuits

The system normally operates under manual control by the plant operator. Safety mode operation is initiated by Safety Injection Signal and Containment Isolation Signal. The realignment process is fully automatic. The initiation signals override the normal manual control.

7.4.1.3.1.2 Logic

In normal operation the system is manually controlled by the plant operator. On receipt of a safety injection signal, all component cooling water pumps start, the residual heat removal heat exchanger isolation valves open, and the Auxiliary Building non-essential isolation valves close. A Containment isolation signal automatically closes the Reactor Building non-essential isolation valves. The realignment process does not require operator action. The normal system control log is bypassed by the safety signals.

7.4.1.3.1.3 Bypasses

There are no bypasses capable of preventing the Safety Injection and Containment Isolation Signals from performing their intended functions. Testing of the safety injection and Containment isolation initiation circuits results in a functional test of the actuated device. Access to the test switches is administratively controlled.

7.4.1.3.1.4 Interlocks

There are no interlocks capable of blocking the safety injection or Containment isolation initiation signals. There are no interlocks between units which would result in actuation of a component cooling water train of one unit in response to operating conditions in the other unit. The component cooling water pump recirculation line valves are interlocked to protect the pump on low flow. The reactor coolant thermal barrier discharge valves are interlocked to close on high flow.

7.4.1.3.1.5 Sequencing

Component Cooling Water System equipment is sequentially loaded on the Essential Auxiliary Power System following safety mode initiation under the conditions described in Section 8.3.1.1.7 and in the order shown in Table 8-1.

7.4.1.3.1.6 Redundancy

The two trains of component cooling water equipment per unit are completely redundant. On loss of offsite power, all component cooling water pumps are started automatically. In the event of Control Room evacuation, start/stop controls for the component cooling water pumps have been provided on the auxiliary shutdown panel.

7.4.1.3.1.7 Diversity

Operating conditions requiring safety mode actuation of the Component Cooling Water System are detected by diverse means.

7.4.1.3.1.8 Actuated Devices

Devices in the Component Cooling Water System actuated by the Safety Injection and Containment Isolation Signals are shown in Figure 9-57, and include the component cooling water pumps and motor operated valves.

7.4.1.3.1.9 Supporting Systems

The Component Cooling Water System receives electrical power from the Essential Auxiliary Power System which is described in Section 8.3, cooling water and an assured source of makeup water from the Nuclear Service Water System which is described in Sections 7.4.1.2

and 9.2.1, and normal makeup water from the Demineralized Water System which is described in Section 9.2.3.

7.4.1.3.1.10 Design Bases

The control and instrumentation for the Component Cooling Water System is designed to provide reliable and continuous control of system equipment under all plant operating conditions. The controls provide for manual operation of the system under normal conditions with overriding automatic controls to realign equipment to a safety mode of operation at the onset of abnormal plant conditions. Control and instrumentation is designed to maintain the separation and redundancy provided by the mechanical design of the system, which provides two isolated full capacity trains of equipment.

Section 3 of IEEE 279-1971 addresses the monitoring and detection of plant operating conditions requiring protective action. The required monitoring and detection capability is not provided directly in the component cooling instrumentation and control systems. Instead, these functions are performed externally in the Solid State Protection System (SSPS) and safety mode actuation is accomplished through control interfaces, implemented as control outputs provided in the SSPS hardware, and hard wired into component cooling control circuits. A discussion of the required monitoring and detection functions, therefore concerns the SSPS rather than the Component Cooling Water System. The SSPS is discussed in Section 7.3. The Essential Auxiliary Power System is discussed in Sections 8.1.4 and 8.3.

7.4.1.3.1.11 Logic Diagrams

See Figure 9-57.

7.4.1.3.1.12 P & I Diagrams

See Figure 9-57.

7.4.1.3.2 Analysis

7.4.1.3.2.1 Conformance to IEEE-279.

IEEE-279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations”, establishes minimum requirements for the reactor protective and engineered safety features instrumentation and control systems. The instrumentation and controls associated with the safe shutdown systems are not defined as a protective system in IEEE-279; however, many criteria of IEEE-279 have been incorporated in the design of the instrumentation and controls for safe shutdown systems. The instrumentation and controls required for safe shutdown are designed and arranged such that no single failure can prevent a safe shutdown, even in the event of loss of off-site power. Single failures considered include electrical faults (e.g., open, shorted or grounded circuits) and physical events (e.g., fires, missiles) resulting in mechanical damage. Compliance with single failure criterion is accomplished by providing redundancy of power supplies, actuation circuits, and by separating the redundant elements electrically and physically to achieve the required independence.

7.4.1.3.2.2 Consideration of Selected Plant Contingency

1. Loss of Instrument Air Systems - The pneumatic valves which are essential during safety injection fail in the safe mode upon loss of instrument air. All other control is electrical and powered from the emergency power system.

2. Plant Load Rejection, Turbine Trip and Loss of Offsite Power - In the event of loss of offsite power associated with plant load rejection or turbine trip, power for safe shutdown is provided by the on-site emergency power system. The description and analysis of the emergency power system are discussed fully in Section 8.3. The emergency diesel generators provide power for operation of pumps and valves. The station batteries provide dc power for operation of control and instrumentation systems require to actuate and control essential components.
3. Loss of Cooling Water to Vital Equipment - None of the instrumentation and controls required for safe shutdown rely on cooling water for operation.

7.4.1.4 Chemical and Volume Control System

7.4.1.4.1 Description

7.4.1.4.1.1 Initiating Circuits

The system normally operates under automatic and/or manual control by the plant operator. Safety mode operation is initiated by actuation of the unit Safety Injection Signal and Containment Isolation Signal. The realignment process does not require operator action.

7.4.1.4.1.2 Logic

In normal operation the system maintains a predetermined water level in the pressurizer, maintains seal-water flow to the reactor coolant pumps, and controls the water chemistry of the reactor coolant. Other than the centrifugal charging pumps (CCP) and associated piping and valves, the CVCS is not required to function during a loss of coolant accident. Upon receipt of a safety injection signal, the centrifugal charging pumps start, the volume control tank and charging line isolation valves close, and the suction valves from the refueling water storage tank open. On Containment isolation, the letdown isolation and seal water isolation valves are closed. The realignment process does not require operator action. Control board process indication and status instrumentation is provided to enable the operator to evaluate system performance and control system operation.

7.4.1.4.1.3 Bypasses

There are no bypasses capable of preventing the Safety Injection or Containment Isolation Signals from performing their intended functions. The boric acid transfer and makeup water pumps are bypassed automatically during safety injection. The sealwater containment isolation valves are blocked from actuation during test but testing the initiating circuits for the remainder of the CVCS results in a functional test of the actuated devices. Access to the test switches is administratively controlled.

7.4.1.4.1.4 Interlocks

There are no interlocks capable of keeping the Safety Injection or Containment Isolation signals from performing their intended functions. There are no interlocks between units which would result in safety mode alignment of one unit in response to operating conditions in the other unit.

7.4.1.4.1.5 Sequencing

CVCS equipment is sequentially loaded on the Essential Auxiliary Power System following safety mode initiation under the conditions described in Section 8.3.1.1.7, and in the order shown in Table 8-1.

7.4.1.4.1.6 Redundancy

Three separate charging pumps are provided. Normally a centrifugal charging pump operates supplying charging and makeup capability to the Reactor Coolant System. On blackout, or safety mode alignment both CCPs are automatically started. In event of Control Room evacuation, the following equipment is provided on the auxiliary shutdown panel:

1. Start/stop control switches and indication for all three charging pumps.
2. Start/stop control switches and indication for the boric acid transfer and make up water pumps.
3. Open/Close control switches and indication for the letdown orifice isolation valves.
4. Open/Close control switch and indication for the boric acid to charging pumps supply valve.

7.4.1.4.1.7 Diversity

Operating conditions requiring safety mode actuation of the CVCS are detected by diverse means.

7.4.1.4.1.8 Actuated Devices

Devices in the CVCS actuated by Safety Injection and Containment Isolation Signals (shown in Figures 9-96 and 9-98) include the centrifugal charging pumps and air and motor operated valves.

7.4.1.4.1.9 Supporting Systems

The CVCS receives electrical power from the Essential Auxiliary Power System which is described in Section 8.3 and cooling water from the Component Cooling Water and Nuclear Service Water Systems described in Sections 7.4.1.3 and 7.4.1.2.

7.4.1.4.1.10 Design Bases

The control and instrumentation for the CVCS is designed to provide reliable and continuous control of system equipment under all plant operating conditions. The controls provide for manual and/or automatic operation of the system under normal conditions with overriding automatic controls to realign equipment to a safety mode of operation at the onset of abnormal plant conditions. Control and instrumentation is designed to maintain the separation and redundancy provided by the mechanical design of the system. Section 3 of IEEE 279-1971 addresses the monitoring and detection of plant operating conditions requiring protection action. The required monitoring and detection capability is not provided directly in the CVCS instrumentation and control systems. Instead, these functions are performed externally in the Solid State Protection System (SSPS) and safety mode actuation is accomplished through control interfaces implemented as control outputs provided in the SSPS hardware, and hard wired into CVCS control circuits. A discussion of the required monitoring and detection functions, therefore concerns the SSPS rather than the CVCS. The SSPS is discussed in

Section 7.3. The Essential Auxiliary Power System is discussed in Section 8.1.4 and Section 8.3.

7.4.1.4.1.11 Logic Diagrams

See Figure 7-8.

7.4.1.4.1.12 P & I Diagrams

See Figures 9-96 and 9-98.

7.4.1.4.2 Analysis

7.4.1.4.2.1 Conformance to IEEE-279.

IEEE 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations,” establishes minimum requirements for the reactor protective and engineered safety features instrumentation and control systems. The instrumentation and controls associated with the safe shutdown systems are not defined as a protective system in IEEE-279; however, many criteria of IEEE-279 have been incorporated in the design of the instrumentation and controls of safe shutdown systems. The instrumentation and controls required for safe shutdown are designed and arranged such that no single failure can prevent a safe shutdown, even in the event of loss of off-site power. Single failures considered include electrical faults (e.g., open, shorted or grounded circuits) and physical events (e.g., fires, missiles) resulting in mechanical damage. Compliance with single failure criterion is accomplished by providing redundancy of power supplies, actuation circuits, and by separating the redundant elements electrically and physically to achieve the required independence.

7.4.1.4.2.2 Consideration of Selected Plant Contingency

1. Loss of Instrument Air Systems - The pneumatic valves which are essential during safety injection fail in the safe mode upon loss of instrument air. All other control is electrical and powered from the emergency power system.
2. Plant Load Rejection, Turbine Trip and Loss of Offsite Power - In the event of loss of offsite power associated with plant load rejection or turbine trip, power for safe shutdown is provided by the on-site emergency power system. The description and analysis of the emergency power system are discussed fully in Section 8.3. The emergency diesel generators provide power for operation of pumps and valves. The station batteries provide dc power for operation of control and instrumentation systems required to actuate and control essential components.
3. Loss of Cooling Water to Vital Equipment - None of the instrumentation and controls required for safe shutdown rely on cooling water for operation.

7.4.1.5 Residual Heat Removal System

The Residual Heat Removal (RHR) System design is described in Section 5.5.7 and Figure 5-28.

7.4.1.5.1 Description

7.4.1.5.1.1 Initiating Circuits

During normal plant operation the system does not operate but is aligned for operation as part of the Emergency Core Cooling System. Safety mode operation is initiated by actuation of the unit Safety Injection Signal.

7.4.1.5.1.2 Logic

During power generation and hot standby operation, the RHR System is not in service but is aligned for operation as part of the Emergency Core Cooling System. During Reactor Startup the RHR system helps control reactor coolant pressure. During reactor shutdown, the RHR system transfers heat from the Reactor Coolant System to the Component Cooling System to reduce the temperature of the reactor coolant to the cold shutdown temperature. The RHR system is also used to transfer refueling water between the refueling water storage tank and the refueling cavity before and after the refueling operations. The reactor shutdown return lines are arranged in parallel redundant circuits and are utilized also as the low head safety injection lines to the reactor coolant system. Utilization of the same return circuits for safeguards as well as for normal cooldown lends assurance to the proper functioning of those lines for safeguards purposes. Upon receipt of a Safety Injection Signal, the RHR pumps start automatically, supplying low head injection water. Control board process indication and status instrumentation is provided to enable the operator to evaluate system performance and control system operation.

7.4.1.5.1.3 Bypasses

There are no bypasses capable of preventing the safety mode initiation signal from performing its intended function.

7.4.1.5.1.4 Interlocks

There are two motor operated gate valves in series in the inlet line from the Reactor Coolant System to the Residual Heat Removal System (1ND1B and 1ND2A). They are normally closed and are only opened for residual heat removal after system pressure is reduced below approximately 385.5 psig and system temperature has been reduced to approximately 350°F. These are the same type of valve and motor operators as those used for accumulator isolation, but they differ in their controls and indications in the following respect:

1. The isolation valve adjoining the Reactor Coolant System is interlocked with a pressure signal to prevent it from being opened whenever the system pressure is greater than 385.5 psig or the isolation valve from the refueling water storage tank is open or the Containment sump line is open or the discharge line to the Containment spray nozzles is open or the supply to the safety injection pumps is open. The valve is manually closed by the operator. An annunciator will alarm in the control room whenever Reactor Coolant System Pressure is greater than 440 psig concurrent with the isolation valve being in the open or intermediate position. The alarm will notify the operator that double barrier isolation between the Reactor Coolant System and the Residual Heat Removal System is not being maintained. This interlock and alarm function is derived from one process control channel.
2. The other valve adjoining the Residual Heat Removal System is similarly interlocked and alarms with the actions being derived from a second process control channel. This second

process control channel utilizes a diverse pressure sensor (one manufactured by a different vendor).

Where the inlet line from the Reactor Coolant System joins the redundant RHR system, there are two isolation valves, one for each train of equipment (1ND4B and 1ND19A). These valves are interlocked with Safety Injection and Containment Spray System valves, so that they cannot be opened when the Emergency Core Cooling System is aligned to take suction from the Containment sump. They are also interlocked with their associated Containment sump valve to close when the sump valve opens.

7.4.1.5.1.5 Sequencing

The RHR pumps are sequentially loaded on the Essential Auxiliary Power System following safety mode initiation under the conditions described in Section 8.3.1.1.7 and in the order shown in Figure 8-1.

7.4.1.5.1.6 Redundancy

The two trains of RHR equipment are completely redundant. In the event of Control Room evacuation, the following equipment is provided on the Auxiliary Shutdown Panel:

1. Start/Stop control switches for the RHR pumps.
2. Open/Close control switches for the inlet line isolation valves from the Reactor Coolant System (1ND1B and 1ND2A).
3. Manual loaders for the RHR heat exchanger flow control valves and heat exchanger bypass flow control valve.

7.4.1.5.1.7 Diversity

Operating conditions requiring safety mode actuation of the RHR system are detected by diverse means.

7.4.1.5.1.8 Actuated Devices

The only devices which receive Safety Injection Signals are the RHR pumps.

7.4.1.5.1.9 Supporting Systems

The RHR system receives electrical power from the Essential Auxiliary Power System which is described in Section 8.3 and cooling water from the Component Cooling Water System which is described in Section 7.4.1.3.

7.4.1.5.1.10 Design Bases

The control and instrumentation for the RHR System is designed to provide reliable and continuous control of system equipment under all plant operating conditions. Control and instrumentation is designed to maintain the separation and redundancy provided by the mechanical design of the system, which provides two isolated full capacity trains of equipment. Section 3 of IEEE 279-1971 addresses the monitoring and detection of plant operating conditions requiring protective action. The required monitoring and detection capability is not provided directly in the RHR instrumentation and control systems. Instead, these functions are performed externally in the Solid State Protection System (SSPS) and safety mode actuation is accomplished through control interfaces, implemented as control outputs provided in the SSPS hardware, and hard wired into RHR control circuits. A discussion of the required monitoring and

detection functions, therefore concerns the SSPS rather than the Residual Heat Removal System. The SSPS is discussed in Section 7.3. The Essential Auxiliary Power System is discussed in Section 8.1.4 and Section 8.3.

Information required by Section 3(8) and 3(9) of IEEE 279-1971 is discussed in Section 5.5.7.

7.4.1.5.1.11 Logic Diagrams

See Figure 7-9.

7.4.1.5.1.12 P & I Diagrams

See Figure 5-28.

7.4.1.5.2 Analysis

7.4.1.5.2.1 Conformance to IEEE-279

IEEE 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations”, establishes minimum requirements for the reactor protective and engineered safety features instrumentation and control systems. The instrumentation and controls associated with the safe shutdown systems are not defined as a protective system in IEEE-279; however, many criteria of IEEE-279 have been incorporated in the design of the instrumentation and controls for safe shutdown systems. The instrumentation and controls required for safe shutdown are designed and arranged such that no single failure can prevent a safe shutdown, even in the event of loss of off-site power. Single failures considered include electrical faults (e.g., open, shorted or grounded circuits) and physical events (e.g., fires, missiles) resulting in mechanical damage. Compliance with single failure criterion is accomplished by providing redundancy of power supplies, actuation circuits, and by separating the redundant elements electrically and physically to achieve the required independence.

7.4.1.5.2.2 Consideration of Selected Plant Contingency

1. Loss of Instrument Air Systems - The pneumatic valves which are needed during safety injection fail in the safe mode upon loss of instrument air. All other control is electrical and powered from the emergency power system.
2. Plant Load Rejection, Turbine Trip and Loss of Offsite Power - In the event of loss of offsite power associated with plant load rejection or turbine trip, power for safe shutdown is provided by the on-site emergency power system. The description and analysis of the emergency power system are discussed fully in Section 8.3. The emergency diesel generators provide power for operation of pumps and valves. The station batteries provide dc power for operation of control and instrumentation systems required to actuate and control essential components.
3. Loss of Cooling Water to Vital Equipment - None of the instrumentation and controls required for safe shutdown rely on cooling water for operation.

7.4.1.6 Emergency Core Cooling System

7.4.1.6.1 Safety Injection System

7.4.1.6.1.1 Description

The Safety Injection System is designed to provide Emergency Core Cooling in order to prevent fuel clad melting to assure that the core remains in place and substantially intact in case of a LOCA or steam break accident. See Section 6.3 for a description of major components in this system. P & I diagrams for safety injection system are presented in Figure 6-176 and Figure 6-177. The system is composed of redundant trains, Train A and Train B. The instrumentation and controls of the components and equipment in Train A are physically and electrically separate and independent of the instrumentation and controls of the components and equipment in Train B. Thus, the system is designed to tolerate a single failure without the loss of its core protective functions. This failure is limited to an active failure during the short term (injection) phase following a LOCA, or to an active or passive failure during the long-term (recirculation) phase. Definitions for active and passive failures are provided in Section 3.0.

The Safety Injection System is automatically actuated by a Safety Injection Signal as a consequence of one of the following events:

1. Low pressurizer pressure.
2. High containment pressure.
3. Manual actuation.

The SIS is electrically interlocked to start the injection mode on a Safety Injection Signal as follows:

1. The centrifugal charging pumps start. Simultaneously, pump suction valves from the RWST (1NV221A and 1NV222B) and discharge valves (1NI9A, 1NI10B) open to provide a clear flow path from RWST to RCS. Simultaneously, normal charging path valves 1NV244A and 1NV245B close. The mini-flow line valves (1NV150B, 1NV151A) are closed by manual operator action. (See Section 6.3.2.17.) Valves 1NV141A and 1NV142B close when valves 1NV221A and 1NV222B leave their seats.
2. The Safety Injection pumps and Residual Heat Removal pumps start.
3. The normally open accumulator isolation valves (1NI54A, 1NI65B, 1NI76A, and 1NI88B) open if any have been closed.

The injection mode continues until the low level is reached in the refueling water storage tank (RWST). The water level in the RWST is measured by three separate channels of instrumentation each with read-outs on the main control board. Two-out-of-three logic from all three automatically switches the safety injection system from the injection phase to the cold-leg recirculation phase of operation when the low level is reached in the RWST. An alarm is actuated at RWST low level. Additional two-out-of-three logic provides an alarm when the pre-low and low-low level is reached in the RWST. The switchover sequence (outlined in Table 6-125) is followed regardless of which power supply is available (offsite or emergency onsite). Controls for the Safety Injection System are grouped together on the main control board. Component position indication lights are also provided to verify that the function of a given switch have been completed.

When the automatic switchover level is reached in the RWST, two-out-of-three logic from all three channels automatically opens the Containment sump valves (1N1184B and 1N1185A).

The Containment sump valves are interlocked with the RWST isolation valves to the RHR pumps (1ND4B and 1ND19A) such that these isolation valves will close when the Containment sump valves reach their full open position. This automatic switchover provides an uninterrupted flow of water to the RHR pumps.

There are four accumulator tanks in SIS. Each tank contains dilute boric acid with a pressurized non-reactive cover gas (nitrogen) over it. Contents of the tanks are used to flood the core following Reactor Coolant System depressurization as a result of a LOCA. Water from only three tanks need to be injected in order to partially cover the core. During normal plant operation each accumulator tank is isolated from the Reactor Coolant System by two check valves in series. There is one motor operated valve in each accumulator tank discharge line which may be used to isolate the accumulator from the rest of the system. Each of these valves is interlocked to open completely within ten seconds after either (a) the primary coolant system pressure exceeds a preselected value (refer to the Technical Specifications) or (b) a safety injection signal has been initiated. Both signals are provided to the valves. Diverse position indication is provided in the Control Room by means of two diverse sensors mounted on each valve. An audible alarm is actuated by a sensor on the valve when the valve is not in the fully open position. The position and audible alarm are independent of the motor control center power. Due to this diverse interlock and indication scheme, no local controls have been provided in the control scheme to close these isolation valves from outside the Control Room. However, means are available in the Control Room to reconnect power to and close these valves under extremely critical circumstances.

7.4.1.6.1.2 Analysis

IEEE 279-1971 “Criteria for Protection Systems for Nuclear Power Generating Stations”, establishes minimum requirements for the reactor protective and engineered safety features instrumentation and control systems. Conformance with the applicable positions of IEEE 279, Section 4 is discussed in the following sections.

7.4.1.6.1.2.1 General Functional Requirements

The instrumentation and controls provided for the Safety Injection System enable the operator to evaluate the system performance and detect malfunctions. The Safety Injection System instrumentation essential to the system safety function is designed for operation under the environmental conditions specified in Section 3.11.

7.4.1.6.1.2.2 Single Failure Criterion

The instrumentation and controls required for Safety Injection System are designed such that no single failure can prevent proper action at the system level. Single failures considered include electrical faults (e.g., open, shorted or grounded circuits) and physical events (e.g., fires, missiles) resulting in mechanical damage. Compliance with single failure criterion is accomplished by providing separation of the redundant elements electrically and physically to achieve the required independence. Electrical separation is assured through the provision of independent power supplies and the elimination of electrical interconnection between redundant elements. A failure analysis for this system is present in Table 6-133.

7.4.1.6.1.2.3 Quality of Components and Modules

The components of the Emergency Core Cooling System are of a quality consistent with the requirements of 10CFR50.65, "Maintenance Rule Program".

7.4.1.6.1.2.4 Equipment Qualification

The Safety Injection System instrumentation and control equipment is designed to operate in the design ambient conditions in the area in which they are located. Environmental design and qualification of electrical and instrumentation equipment is discussed in Section 3.11. Seismic qualifications and testing are discussed in Section 3.1.

7.4.1.6.1.2.5 Channel Integrity

Pre-operational testing and inspection is performed to verify that all components, automatic and manual controls provided for the Safety Injection System accomplish the intended design function and maintain their necessary functional capability.

7.4.1.6.1.2.6 Channel Independence

The Safety Injection System channel independence is achieved by electrical and physical separation as described in Section 7.4.1.6.1.2.2.

7.4.1.6.1.2.7 Derivation of System Inputs

The Safety Injection System inputs are derived from signals that are direct measures of the desired variables.

7.4.1.6.1.2.8 Capability for Test and Calibration

The instrumentation and control components required for safety injection which are not normally in operation are periodically tested. All automatic and manual activating and control devices are tested to verify their operability. Periodic testing is described in the Technical Specifications.

7.4.1.7 Auxiliary Shut-Down Control

7.4.1.7.1 General Considerations

In the unlikely event the control room must be evacuated, sufficient instrumentation and control is provided to bring the plant safely to a hot standby condition (mode 3). The following general considerations are applied to the shutdown system:

1. The turbine is tripped (note that this can be accomplished at the turbine as well as in the Control Room).
2. The reactor is tripped (note that this can be accomplished at the reactor trip switchgear as well as in the Control Room).
3. All automatic systems continue functioning (discussed in Sections 7.2 and 7.7).
4. For equipment having motor controls outside the Control Room (which duplicate the functions inside the Control Room) the controls are provided with a selector switch which transfers control of the switchgear from the Control Room to an auxiliary control panel. (Refer to Figure 1-3 for the location of the auxiliary shutdown panel and the auxiliary feedwater control panels.) Placing the local selector switch in the local operating position gives an annunciating alarm in the Control Room. The auxiliary shutdown control panel and auxiliary feedwater control panels have doors which are alarmed in the Control Room when opened.
5. Jumpers can be installed in the appropriate area termination cabinets to bypass the Safety Injection Signals when pressurizer pressure has decreased to the P-11 setpoint.

6. Jumpers can be installed in the appropriate area termination cabinets or penetrations to close the accumulator isolation valves when pressurizer pressure has decreased to the P-11 setpoint and the Safety Injection Signal, if present, has been reset.

A tabulation of the controls on the auxiliary shutdown control panel and auxiliary feedwater control panels necessary for hot standby from outside the control room are shown in Table 7-8 through Table 7-11.

If the Control Room is inaccessible on a long term basis, the plant can be brought to cold shutdown.

The systems previously discussed in Section 7.4, in addition to the equipment and services identified in Section 7.4.1.7.1, "General Considerations" and Section 7.4.1.7.2 below are sufficient to achieve and maintain hot standby and cold shutdown of the unit as required in GDC 19 1971.

7.4.1.7.2 Equipment, Services, and Approximate Time Required After Incident that Required Hot Standby

1. Auxiliary feedwater pumps - required if main feedwater pumps are not operated. For blackout condition the auxiliary feedwater pumps start automatically within one minute. (See Chapter 10 for discussion of pumps.)
2. Reactor Containment fan cooler units - automatic (See Section 9.4.5 for discussion of fan coolers.)
3. Diesel generators - loaded within one minute (See Chapter 8 for discussion of diesels.)
4. Emergency lighting in the areas of station required during this condition. Immediately (See Chapter 9 for discussion of lighting).
5. Pressurizer heaters - within four hours (see Section 5.5.10 for discussion of heaters.)
6. A communication network is available for prompt use between the following areas:
   a. Outside telephone exchange
   b. Auxiliary Shutdown Control Panel
   c. Auxiliary Feedwater Control Panel
   d. Diesel generator
   e. Switchgear room
7. Monitoring Indicators

   The characteristics of these indicators, which are provided outside as well as inside the Control Room, are described in Section 7.5. The necessary indicators are as follows:

   a. Water level indicator for each steam generator
   b. Pressure indicator for each steam generator
   c. Pressurizer water level indicator
   d. Pressurizer pressure indicator

7.4.1.7.3 Equipment and Systems Available for Cold Shutdown

1. Reactor coolant pump (See Section 5.5.1)

2. Auxiliary feedwater pumps (See Section 10.4.10)
3. Boric acid transfer pump (See Section 9.3.4)
4. Charging pumps (See Section 9.3.4)
5. Service water pumps (See Section 9.2.1)
6. Containment fans (See Section 9.4.5)
7. Control Room Ventilation (See Section 9.4.1)
8. Component Cooling pumps (See Section 9.2.2)
9. Residual heat removal pumps (See Section 5.5.7)
10. Certain motor control center and switchgear sections (See Chapter 8)
11. Controlled steam release and feedwater supply (See Section 7.7 and Chapter 10).
12. Boration capability (See Section 9.3.4, "Chemical and Volume Control System").
13. Nuclear Instrumentation System (source range and intermediate range) (See Sections 7.2 and 7.7).
14. Reactor coolant inventory control (charging and letdown) (See Section 9.3.4).
15. Pressurizer pressure control including opening control for pressurizer relief valves, heaters, and spray (See Section 5.5.10).

Note that the reactor design does not preclude attaining the cold shutdown condition from outside the Control Room. An assessment of unit conditions can be made on a long term basis (a week or more) to establish procedures for making the necessary physical modifications to instrumentation and control equipment in order to attain cold shutdown. During such time the unit can be safely maintained in the hot standby condition. Even though both units use a common Control Room the mechanical and electrical systems are separate for each unit. Therefore, each unit can achieve hot standby or cold shutdown independent of the other unit using the systems and equipment previously discussed in Section 7.4.

7.4.1.7.4 Further Considerations

In addition to the considerations given above, a loss of instrument air or loss of component cooling water to vital equipment has been considered. Neither the loss of instrument air nor the loss of cooling water (assuming no other accident conditions) can cause safety limits as given in Technical Specifications to be exceeded. Likewise, loss of either one of the two does not adversely affect the core or the Reactor Coolant System nor does it prevent an orderly shutdown if this is necessary. Furthermore, all pneumatically operated valves and controls assume a preferred operating position upon loss of instrument air. It is also noted that, for conservatism during the accident analyses (Chapter 15), credit is not taken for the instrument air systems nor for any control system benefit.

7.4.1.7.5 Final System Drawings

Functional block diagrams, electrical elementaries and other drawings required to assure electrical separation and perform a safety review are provided in the McGuire Electrical Schematics.

7.4.2 Analysis

Hot standby is a stable condition, automatically reached following a unit shutdown. The hot standby condition can be maintained safely for an extended period of time. In the unlikely event that access to the Control Room is restricted, the unit can be safely kept in hot standby until the Control Room can be re-entered.

The safety evaluation of the maintenance of a shutdown with these systems and associated instrumentation and controls has included consideration of the accident consequences that might jeopardize safe shutdown conditions. The accident consequences that are germane are those that would tend to degrade the capabilities for boration, adequate supply for auxiliary feedwater, and residual heat removal.

The results of the accident analyses are presented in Chapter 15. Of these the following produce the most severe consequences that are pertinent:

1. Uncontrolled Boron Dilution
2. Loss of Normal Feedwater
3. Loss of External Electrical Load and/or Turbine Trip
4. Loss of all A.C. Power to the Station Auxiliaries

It is shown by these analyses that safety is not adversely affected by these incidents with the associated assumptions being that the instrumentation and controls indicated in Section 7.4 are available to control and/or monitor shutdown. These available systems allow a maintenance of hot shutdown even under the accident conditions listed above which would tend toward a return to criticality or a loss of heat sink.

A review of the IE instrumentation and control systems was conducted in response to IE Bull. 79-27. This review determined that McGuire design meets all requirements of this Bulletin (Ref. 4).

7.4.3 References

1. McGuire Electrical Schematics
2. Letter from W. O. Parker, Jr. to H. R. Denton (NRC) dated October 14, 1980. Subject: Bypass, Override and Reset Circuits of ESF.
3. Letter from W. O. Parker, Jr. to H. R. Denton (NRC) dated September 18, 1980. Subject: Auxiliary Feedwater System.
4. Letter from W. O. Parker, Jr. (Duke) to J. P. O'Reilly (NRC) dated February 29, 1980

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.4.

THIS PAGE LEFT BLANK INTENTIONALLY.

7.5 Safety Related Display Instrumentation

7.5.1 Description

Table 7-12 and Table 7-13 lists the information readouts provided to the operators to enable them to perform required manual safety functions, and to determine the effect of manual actions taken following a reactor trip due to a Condition II, III, or IV event, as defined in Chapter 15. A more detailed listing is provided in McGuire Updated Final Safety Analysis Report (UFSAR) Table 1-6.

Table 7-14 lists information available to the operator for monitoring conditions in the reactor, the Reactor Coolant System, the Containment and process systems throughout all normal operating conditions of the unit, including anticipated operational occurrences.

7.5.2 Analyses

Post accident monitoring is not covered by the scope of IEEE 279-1971. Specific post accident monitoring design requirements for the McGuire Nuclear Station are addressed in McGuire Updated Final Safety Analysis Report (UFSAR) Section 1.11, "Regulatory Guide 1.97, Revision 2 - Review for McGuire Nuclear Station".

The post accident monitoring system requires three instrumentation cables to be run underground. These cables are routed from the Auxiliary Building to the refueling water storage tank through a seismically designed pipe trench. The circuits are designed to operate during flood conditions by utilizing a continuous, unspliced circuit of waterproof armored cable. Separation is maintained by 18" physical distance or by use of barriers.

7.5.3 Relief and Safety Valve Position Indication

(Ref. 3, Section 7.5.5) or Section 1.8.24.

This system provides the position indication for the pressurizer power operated relief valves and safety valves on the main control room board.

System Description

Power Operated Relief Valves

The position of PORVs is detected by seismically and environmentally qualified stem-mounted limit switches. The limit switches actuate indicator lights on the main control board. The entire circuit including the power supply is safety grade. A control room computer alarm is also provided to alarm opening of a PORV.

Safety Valves

Flow through the safety valves is detected by an acoustic flow detection system. This system senses the vibrations caused by flow through the valve when valve is not fully closed. Two accelerometers are strapped to the discharge piping of each safety valve to sense the flow vibrations. The alarm output of this system is used to provide indication and annunciator alarm in the control room. The system with the exception of the annunciator alarms is safety grade and meets the appropriate seismic and environmental qualifications.

7.5.4 Inadequate Core Cooling Instrumentation

Ref. Section 1.8.27, 1.11, Tables 1-3 and 1-6.

7.5.4.1 Core Exit Thermocouples (CET)

The present incore thermocouple system has 65 thermocouples (T/C's) positioned to sense exit coolant temperature of selected fuel assemblies. The output of the thermocouples is routed via 5 instrument ports located in the reactor vessel head. Each instrument port is provided with an electrical connector for 13 thermocouples. The thermocouple output is cabled to the backup display and the plant computer.

The primary display for the Incore Thermocouple System consists of a graphic which can be displayed on monitors located on control boards. This display is generated through the plant Operator Aid Computer. The graphics provide a spatially oriented core map available on demand indicating temperature at each of the 65 core exit thermocouple locations. The readout range extends from 200°F to 2300°F. Trending of selected thermcouple readings and hard copy printouts are available on demand. This display is non class 1E.

Class 1E backup displays (one for each of two trains) are provided on the control board with the capability of reading the upgraded thermocouples within a time interval of no greater than six minutes. The range of display extends from 32°F to 2300°F.

7.5.4.2 Subcooling Monitor

The margin to saturation is calculated from Reactor Coolant System (RCS) pressure and temperature measurements using the Plant Computer and the Subcooling Margin Monitor (SMM) which is part of the Inadequate Core Cooling Monitoring (ICCM) System.

For the Plant Computer the margin to saturation is calculated from Reactor Coolant System (RCS) pressure and temperature measurements (dynamic and low-range pressures, dynamic-range hot leg temperatures, and temperatures from in-core thermocouples). When RCS pressure is sufficiently less than 800 PSIG to ensure the low range pressure sensor is within its measurement span, the low range input is used. The wide range pressure inputs are used for the remaining conditions. The average of the five highest value incore thermocouples (from 40 EQ T/C's) are used to represent core exit conditions. The wide range hot leg RTD's are used to measure the loop hot leg temperatures. The highest of these temperatures and the appropriate pressure are then used to calculate a conservative margin to saturation. Averaging of the thermocouple readings and calculation of margin to saturation are performed by the plant computer.

There are two Class 1E channels of SMM which are provided by the ICCM (one SMM channel per train of ICCM). For each channel of the SMM, the average of the five highest value incore thermocouples for that channel (20 Class 1E T/C's are installed per channel) are used to represent core exit conditions. Each channel also uses wide range hot leg RTD's to measure the hot leg temperatures for two of the RCS loops.

The SMM performs calculations and a comparison to adjusted saturation curves (adjusted for possible measurement uncertainties) to compute margins.

Indication and Alarms

The Plant computer output consists of a graphic display which plots plant pressure and temperature in relation to the computer generated adjusted saturation curve. In addition, numerical values are provided for parameters of interest such as pressure (Reactor Coolant System), temperatures (hot leg), and subcooling margins. Program logic variables such as source for pressure value (wide or low range sensor) and containment conditions (normal or accident) are also provided. Alarm status is indicated by messages on the graphic display and Alarm workstation. Alarms are provided at a selected margin from the adjusted saturation curve to warn of the approach to loss of adequate subcooling and again upon reaching the adjusted

saturation curve to warn of the loss of adequate subcooling. The Plant Computer also displays computed numerical values sent from the SMM.

The SMM output consists of a main control board plasma display (one per channel) which plots plant pressure and temperature in relation to the SMM generated adjusted saturation curve. In addition, numerical values are provided for parameters of interest such as pressure (Reactor Coolant System), temperatures (hot leg), and subcooling margins. Alarm status is indicated by messages on the display. Annunciator alarms are provided at a selected margin from the adjusted saturation curve to warn of the approach to loss of adequate subcooling and again upon reaching the adjusted saturation curve to warn of the loss of adequate subcooling.

Analysis

The McGuire subcooling monitor meets the requirements of Category 2 equipment as called for in Regulatory Guide 1.97 Rev. 2. (Ref. 4, Section 7.5.5) The subcooling margin is continuously monitored. The SMM which is part of the ICCM is a fully qualified, redundant, Class 1E processor and display. Inputs to the SMM are provided from QA Condition 1 instruments. The Plant Computer is powered by highly reliable battery backed control power. The Plant Computer processing and display are located in a mild environment. Primary inputs to the Plant Computer graphic display are provided from QA Condition 1 instruments, which have been isolated for input to the Plant Computer. Additional inputs of lesser qualification are used by the Plant Computer, when available and within valid ranges, to provide additional accuracy.

7.5.4.3 Reactor Vessel Level System (RVLIS)

This system is designed to monitor the water level in the reactor vessel, or the approximate void content under forced circulation conditions, during certain postulated accident conditions. Included is equipment to monitor both the upper plenum (head) level, as well as the entire height of the reactor vessel.

The system instrumentation permits vessel level measurement from the bottom to the top of the reactor vessel, utilizing taps off an existing spare head penetration and a tap off a thimble tube at the seal table. Two sets of differential pressure transmitters are provided which have differing measurement ranges to cover different flow behavior with and without pump operations. The lower range cells indicate water level when no reactor coolant pumps are operating. Under natural circulation or no-circulation conditions, these pressure drops will provide indication of the collapsed liquid level or relative void content in the reactor vessel above and below the hot legs. The dynamic range cells indicate the combined core and internals pressure drop for any combination of operating reactor coolant pumps. Under forced-flow conditions, the pressure drops will provide indication of the relative void content of the circulating primary coolant system fluid. The upper range measurement is taken by two differential pressure transmitters between the same spare head penetration, and taps off two hot legs.

To minimize containment post-accident environment effects in measurement accuracy, the system design is based upon locating the transmitters outside the containment. Hydraulic isolators in the impulse lines provide the required double barrier protection between the RCS and outside containment. Reference leg temperature measurements, together with the existing RCS temperature and pressure, are utilized to automatically compensate for difference in coolant and reference leg temperature effects.

Installation of the system is complete. The emergency procedures which reference RVLIS have been written using the Westinghouse Owners Group emergency response guidelines (Ref. 5).

7.5.5 References

1. Vogeding, E. L., Seismic Testing of Electrical and Control Equipment, *WCAP-7817*, December, 1971.

   Vogeding, E. L., Seismic Testing of Electrical and Control Equipment, (WCID Process Control Equipment), *WCAP-7817*, Supplemental, December, 1971. Potochnik, L. M., Seismic Testing of Electrical and Control Equipment (Westinghouse Solid-State Protection System), (Low Seismic Plants), *WCAP-7817*, Supplement 3, December, 1971.

2. Fischer, D. G., Qualification of Westinghouse Seismic Testing Procedure for Electrical Equipment Tested Prior to May, 1974, *WCAP-8373*, August 1974.

3. McGuire Nuclear Station, Responses To TMI Concerns, Item II.D.3.

4. Letter from T.M. Novak (NRC) to H.B. Tucker (Duke) dated September 17, 1984. Subject: Inadequate Core Cooling Instrumentation (McGuire Nuclear Station, Units 1 and 2).

5. Letter from H. B. Tucker (Duke) to H. R. Denton (NRC) dated May 16, 1984. Subject: Inadequate Core Cooling Instrumentation.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.5.

7.6 All Other Systems Required for Safety

7.6.1 Instrumentation and Control Power Supply System

7.6.1.1 Description

The following is a description of the Instrumentation and Control Power Systems:

1. Refer to McGuire One-Line Diagram MC-1705-01 (up to date) or Figures 8-35 and 8-36 (typical) for a single line diagram of 125 VDC and 120 VAC Vital Instrumentation and Control Power Systems.
2. There are four inverters and four distribution panels per unit. Each inverter is connected independently to one distribution panel.
3. The inverters provide a source of 120 Volt 60 Hz power for the operation of the safety related Nuclear Steam Supply System instrumentation. This power is derived from the station batteries, thus assuring continued operation of instrumentation systems in the event of a station blackout.
4. Each of the four distribution panels may be connected to a common backup source of 120 VAC regulated power. The tie is through a local, manually operated "make before break" transfer switch which connects the inverter to the regulated power panelboard such that the distribution panel will not lose power as the transfer switch is operated, but cannot be aligned to both sources at the same time.

7.6.1.2 Analysis

There are four independent batteries and battery chargers. There is also a spare battery charger which can be aligned to replace a charger which is out of service for preventive maintenance or repair. Each battery is attached to a bus serving one inverter.

Since not more than one inverter is connected to the same bus, a loss of a single bus can only affect one of the four inverters for the affected unit. Each inverter is independently connected to only one instrument distribution panel in a single unit so that the loss of an inverter cannot affect more than one of the four distribution panels in the affected unit.

In addition, each of the four distribution panels for a given unit is connected to the same source of backup 120 VAC regulated power. Each distribution panel can receive power from the 120 VAC regulated backup source under operator control.

Therefore, no single failure in the instrumentation and control power systems can cause a loss of power to more than one of the redundant loads. The design is in compliance with paragraph 5.4 of Reference 1 (IEEE-308, 1971).

7.6.2 Annulus Ventilation System

The Annulus Ventilation System collects and filters gaseous leakage during accident conditions. The system also maintains post-accident negative pressure in the annulus area, between the Containment and the Reactor Building.

The Annulus Ventilation System receives the Containment high-high pressure signal (Sp) and actuates automatically. Annulus pressure is maintained between minus 1/2 and minus 3 1/2 inches of water gauge. The recirculation and exhaust dampers are repositioned automatically by the annulus pressure sensing System to regulate pressure to the design basis.

The Annulus Ventilation System has two 100% capacity trains. Both trains are physically and electrically separated and independent of each other.

Instrumentation, controls, alarms and read-out gauges are provided in the Control Room for each section. (Refer to Section 6.2.3 for additional discussion.)

See Figure 7-12 for the logic diagram of the system.

7.6.2.1 Instrumentation Application

The following subdivision describes the instrumentation for the Annulus Ventilation System. This system does not operate during normal plant operation.

7.6.2.1.1 Containment Pressure

Two out of four Containment pressure transmitters through bistables are used to actuate the Annulus Ventilation System on high-high pressure. High pressure alarm indications are located in the Control Room.

7.6.2.1.2 Annulus Pressure

There are four annulus pressure sensors located on the annulus wall. One sensor is used for Train A and one for Train B. The sensors are used to automatically position the recirculation and exhaust dampers to regulate annulus pressure. The other two pressure sensors, one for Train A and one for Train B, monitor low and low-low pressure in the annulus. Indication is provided for both setpoints, and the train related annulus ventilation fan is tripped upon a low-low pressure only if it is in the exhaust mode.

7.6.2.1.3 Filter Train Differential Pressure

Pressure transmitters are provided to measure the differential pressure across the filter train. Remote read-outs are provided in the Control Room.

7.6.2.1.4 Annulus Ventilation Fans Inlet Header Flow

Flow transmitters are provided to measure inlet header flow to the annulus ventilation fans. If flow is <80%, a low flow indicator is initiated the Control Room.

7.6.2.1.5 Charcoal Filter Temperature

One high temperature alarm and one filter fire alarm are provided for filter temperature monitoring. Both temperature set-points are alarmed in the Control Room. The filter fire alarm may require operator action to actuate the deluge system to extinguish the fire. A crossover network is provided to cool the filter train associated with the redundant ventilation fan.

7.6.2.1.6 Annulus Ventilation Exhaust Header Flow

Flow transmitters are provided to measure exhaust flows. Remote read-outs are provided in the Control Room.

7.6.2.1.7 Supporting Systems

The Annulus Ventilation System receives electrical power from the Essential Auxiliary Power System which is described in Section 8.3.

7.6.2.1.8 Design Basis Information

7.6.2.1.8.1 Design Bases

The control and instrumentation for the Annulus Ventilation System is designed to provide reliable and continuous manual control of system equipment under LOCA conditions. Automatic controls are provided to realign the equipment to a safety mode of operation upon receipt of a safety actuation signal.

7.6.2.1.8.2 Conformance to IEEE 279-1971

Section 3 of IEEE 279-1971 (Reference 2, Section 7.6.20) addresses the monitoring and detection of plant operating conditions requiring protective action. The required monitoring and detection capability is not provided directly in the Annulus Ventilation System instrumentation and control system. Instead, these functions are performed externally in the Solid-State Protection System (SSPS). Safety mode actuation is accomplished through control interfaces, implemented as control outputs provided in the SSPS. A discussion of the required monitoring and detection functions therefore concerns the SSPS, and is discussed in Section 7.3. Other design basis considerations are discussed in Sections 3.1, 3.11, 9.4 and Table 3-7.

7.6.2.2 Analysis

7.6.2.2.1 NRC General Design Criteria

Implementation of the requirements of the NRC General Design Criteria is described in Section 3.1.

7.6.2.2.2 Conformance to IEEE 279-1971

IEEE 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations,” establishes minimum requirements for the reactor protective and engineered safety features instrumentation and control systems. The instrumentation and controls associated with the Annulus Ventilation System are not defined as a protective system in IEEE 279-1971; however, many criteria of IEEE 279-1971 have been incorporated in the design of the instrumentation and controls for this system.

7.6.2.2.3 General Functional Requirements

The instrumentation and controls associated with the Annulus Ventilation System are designed to enable the operator to manually control the exhaust and recirculation dampers, determine system performance with read-outs and indicator lights, and detect system malfunctions.

The Annulus Ventilation System instrumentation and controls are designed to operate automatically under the environmental conditions specified in Section 3.11.

7.6.2.2.4 Single Failure Criterion

The Annulus Ventilation System instrumentation and control are designed so that any single failure within the system shall not prevent proper action at the system level.

Two separate and independent systems are provided for each unit. A failure of any one train does not affect the operation of the other train. Both trains are 100% capacity. Refer to the malfunction analysis Table 6-108.

7.6.2.2.5 Quality of Components and Modules

The components of the Annulus Ventilation System are of a quality consistent with 10CFR50.65, "Maintenance Rule Program".

7.6.2.2.6 Equipment Qualification

The Annulus Ventilation System Instrumentation and Controls meet the equipment requirements described in Sections 3.10 and 3.11.

7.6.2.2.7 Channel Integrity

The controls and instrumentation required for the proper operation of the Annulus Ventilation System is designed to function properly under the conditions specified in Section 3.11.

7.6.2.2.8 Channel Independence

The Annulus Ventilation System instrumentation and control channel independence is achieved through physical and electrical separation as specified by IEEE 279-1971.

7.6.2.2.9 Control and Protection System Interaction

No portion of the Annulus Ventilation System instrumentation and control is used for both control and protection functions as described in Section 2 of IEEE 279-1971.

7.6.2.2.10 Derivation of System Inputs

Annulus Ventilation System instrumentation and control inputs are derived from signals that are direct measures of the desired variables.

7.6.2.2.11 Operating Bypasses

Bypasses that are automatically removed are alarmed and indicated. The system bypass status is in compliance with NRC Regulatory Guide 1.47-1973 and IEEE 279-1971.

7.6.2.2.12 Indication of Bypasses

The system bypass for controlling the exhaust and recirculation dampers manually is indicated on the plant computer 1.47 bypass application. Indication of test or bypass conditions is given by an Operator Aid Computer (OAC) 1.47 graphic display.

7.6.3 Containment Spray System

7.6.3.1 Description

The Containment Spray System is manually actuated from the Control Room after the recirculation mode of ECCS has been initiated.

High-high pressure alarm and pressure indications are located in the Control Room.

The operating mode of the Containment Spray System is manually aligned to the Residual Heat Removal System during the containment recirculation phase of the accident. Refer to Section 7.6.9.

The Containment Pressure Control System is provided to prevent inadvertent operation of the spray. Below a +.35 psig pressure the spray pumps and discharge valves are restrained from operating. Refer to Sections 7.3 and 7.6.16.

Manual initiation of the Containment Spray System is provided in the Control Room. All safety related display instrumentation for this system and bypass indication is provided in the Control Room.

7.6.3.1.1 Design Basis Information

The control and instrumentation for the Containment Spray System is designed to provide reliable and continuous control of system equipment under LOCA conditions.

Manual controls are provided for actuation of Containment spray during ECCS recirculation phase..

Section 3 of IEEE 279-1971 addresses the monitoring and detection of plant operating conditions requiring protective action. The required monitoring and detection capability is not provided directly in the Containment Spray System instrumentation and control system. Instead, these functions are performed externally in the Containment Pressure Control System (CPCS) monitoring circuits. Containment Spray actuation is accomplished through manual actuation with permissive CPCS hardware. Refer to discussions in Section 7.6.16. Other design basis considerations are discussed in Sections 8.1.4, 8.3.1, 3.10, 3.11, and Table 3-3, Table 3-7.

7.6.3.2 Analysis

The intent of this analysis is to present the extent to which the design of system instrumentation meets the applicable portions of IEEE 279-1971 in compliance with NRC Regulatory Guide 1.70. Conformance with the applicable portions of IEEE 279-1971, Section 4, is discussed in the following sections.

7.6.3.2.1 General Functional Requirements

The instrumentation and control provided for the (CSS) Containment Spray System enables the operator to evaluate system performance and detect malfunctions. The CSS is designed to be manually actuated during ECCS recirculation mode. The CSS Instrumentation essential to the system safety function is designed for operation under the environmental conditions specified in Section 3.11.

7.6.3.2.2 Single Failure Criterion

The CSS is designed so that any single failure within the system does not prevent spray of borated water into Containment. Two separate and independent trains (A & B) are provided for each unit, as shown in Figure 6-194. The instrumentation and controls of the components of Train A are physically and electrically separate and independent of the instrumentation and controls of the components of Train B. Single failure of the control circuitry will cause, at maximum, only a failure of a component or components within one of the two independent trains.

7.6.3.2.3 Quality of Components and Modules

The components of the Containment Spray System are of a quality consistent with the requirements of 10CFR50.65, "Maintenance Rule Program".

7.6.3.2.4 Equipment Qualification

The CSS instrumentation and controls meet the requirements as described in Sections 3.10 and 3.11.

7.6.3.2.5 Channel Integrity

The instrumentation and controls associated with the CSS that are essential to each train function are designed to maintain the necessary functional capability under the conditions specified in Section 3.11.

7.6.3.2.6 Channel Independence

The CSS channel independence is achieved by physical and electrical separation as described in Section 7.6.3.2.2.

7.6.3.2.7 Control and Protection System Interaction

No portion of the CSS is used for both control and protection functions as described in Section 4 of IEEE 279-1971.

7.6.3.2.8 Derivation of System Inputs

The CSS inputs are derived from signals that are direct measures of the desired variables.

7.6.3.2.9 Capability for Sensor Checks

CSS sensors are checked by cross-checking between channels. These channels bear a known relationship to each other, and this method ensures the operability of each sensor during reactor operation.

7.6.3.2.10 Capability for Test and Calibration

Testing is described in Sections 7.3.2.2.5 and 7.2.2.2.3.

7.6.3.2.11 Indication of Bypasses

Indication of test or bypass conditions or removal of any channel from service is given by lights in the Control Room.

7.6.4 Containment Air Return & Hydrogen Skimmer System

The Containment air return fans provide rapid return of air to the lower compartment after the initial LOCA blowdown. Both fans are 100% capacity and receive emergency diesel back-up power.

The Hydrogen Skimmer System prevents hydrogen pocketing in closed Containment spaces and compartments. Two 100% capacity fans are provided. The system control logic is shown on Figure 7-19. Refer to Section 6.2.1 for additional discussion. See Figure 6-107 for a flow diagram of the Containment Air Return and Hydrogen Skimmer System.

7.6.4.1 Instrumentation Application

The following subdivision describes the instrumentation for the Containment Air Return and Hydrogen Skimmer System. This system does not operate during normal plant operation.

7.6.4.1.1 Containment Pressure

The Containment Pressure Control System is provided to prevent depressurization of Containment. The Containment Pressure Control System described in Section 7.6.16 prevents inadvertent operation of the air return fans when Containment pressure is less than .35 psig.

7.6.4.1.2 Fan Monitoring

The Containment air return fan discharge pressure and the hydrogen skimmer fan suction pressure are monitored.

7.6.4.1.3 Supporting Systems

The Containment Air Return Hydrogen Skimmer System receives electrical power from the Essential Auxiliary Power System which is described in Section 8.3.

7.6.4.1.4 Design Basis Information

7.6.4.1.4.1 Design Bases

The control and instrumentation for the Containment Air Return & Hydrogen Skimmer System is designed to provide reliable and continuous manual control of system equipment under LOCA conditions. Automatic controls are provided to realign the equipment to a safety mode of operation upon receipt of a safety actuation signal.

7.6.4.1.4.2 Conformance to IEEE 279-1971

Section 3 of IEEE 279-1971 addresses the monitoring and detection of plant operating conditions requiring protective action. The required monitoring and detection capability is not provided directly in the Containment Air Return & Hydrogen Skimmer System instrumentation and control system. Instead, these functions are performed externally in the SSPS. Safety mode actuation is accomplished through control interfaces, implemented as control outputs provided in the SSPS. A discussion of the required monitoring and detection functions therefore concerns the SSPS, and is discussed in Section 7.3. Other design basis considerations are discussed in Sections 3.10, 3.11, 9.4 & Table 3-7.

7.6.4.2 Analysis

7.6.4.2.1 NRC General Design Criteria

Implementation of the requirements of the NRC General Design Criteria is described in Section 3.1.

7.6.4.2.2 Conformance to IEEE 279-1971

IEEE 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations,” establishes minimum requirements for the reactor protective and engineered safety features instrumentation and control systems. The instrumentation and controls associated with the Containment Air Return and Hydrogen Skimmer System are not defined as a protective system in IEEE 279-1971; however, many criteria of IEEE 279-1971 have been incorporated in the design of the instrumentation and controls for this system.

7.6.4.2.3 General Functional Requirements

The instrumentation and controls associated with the Containment Air Return and Hydrogen Skimmer System is designed to enable the operator to manually control the isolation dampers and detect system malfunction with indicator lights.

The system is designed to operate automatically under the environmental conditions specified in Section 3.11.

7.6.4.2.4 Single Failure Criterion

The Containment Air Return and Hydrogen Skimmer System instrumentation and controls are designed so that any single failure within the system does not prevent proper action at the system level.

Two separate and independent systems are provided for each unit. A failure of any one train does not effect the operation of the other train. Both trains are 100% capacity.

Refer to the Air Return Fan Failure Analysis Table 6-68.

7.6.4.2.5 Quality of Components and Modules

The components of the Containment Air Return and Hydrogen Skimmer System are of a quality consistent with requirements of 10CFR50.65, "Maintenance Rule Program".

7.6.4.2.6 Equipment Qualification

The Containment Air Return and Hydrogen Skimming System instrumentation and controls meet the equipment requirements described in Sections 3.10 & 3.11.

7.6.4.2.7 Channel Integrity

The controls and instrumentation for the proper operation of the Containment Air Return and Hydrogen Skimmer System is designed to function properly under the conditions specified in Section 3.11.

7.6.4.2.8 Channel Independence

The Containment Air Return and Hydrogen Skimmer System instrumentation and control channel independence is achieved through physical and electrical separation as specified by IEEE 279-1971.

7.6.4.2.9 Control and Protection System Interaction

No portion of the Containment Air Return and Hydrogen Skimmer System instrumentation and controls are used for both control and protection functions as described in Section 2 of IEEE 279-1971.

7.6.4.2.10 Derivation of System Inputs

Containment Air Return and Hydrogen Skimmer System inputs are derived from signals that are direct measures of desired variables.

7.6.4.2.11 Operating Bypasses

Bypasses that are automatically removed are alarmed and indicated. The system bypass status is in compliance with NRC Regulatory Guide 1.47-1973 and IEEE 279-1971.

7.6.4.2.12 Indication of Bypass

The system bypass for controlling the isolation dampers manually is indicated on the bypass indication panel in the Control Room. Indication of test or bypass condition is provided in the Control Room.

7.6.5 Ice Condenser System

7.6.5.1 Description

The ice condenser's primary function is the absorption of thermal energy released abruptly in the event of a loss-of-coolant accident for the purpose of limiting the initial peak pressure in the Containment. A secondary function of the ice condenser is the further absorption of energy after the initial incident causing the Containment pressure to be reduced to and held at a lower level for a period of time. (Refer to Sections 6.1.5 and 6.2.2.

7.6.5.1.1 Ice Condenser Instrumentation

The ice condenser is a passive device requiring only the maintenance of the ice inventory in the ice bed. As such there are no actuation circuits or equipment, which are required for the ice condenser to operate in the event of a LOCA. The instrumentation provided for the ice condenser serves only to monitor the ice bed status. Therefore, the ice condenser instrumentation provides an early warning of any incipient ice condenser anomalies. In this way the operator can evaluate the anomaly and take proper remedial action. Depending upon the anomaly, the operator typically may perform a local or system defrost, switch to a back up glycol circulation pump, start a backup chiller package, provide glycol makeup, isolate a glycol leak, or perform a safe and orderly shutdown.

7.6.5.1.1.1 Lower Door Position Indication

For door monitoring purposes, the ice condenser is divided into six zones (refer to Figure 7-13). Each zone contains four inlet door assemblies, or a total of eight door panels. Each lower inlet door panel is provided with a single pole double throw limit switch for position indication and alarm.

Each zone is provided a pair of monitor lights (one for “Door Open” and one for “Door Closed” indication) on the door position display panel. A “Door Open” indication is given if any door panel within a zone is opened. (Refer to Figure 7-14.)

A Control Room alarm (“Ice Cond. Lower Inlet Doors Open”) is provided on an annunciator panel. This alarm is activated if any door panel in any zone is opened. (Refer to Figure 7-15.)

The door position display panel, located in the Incore Instrument Room, is accessible during normal plant operation in the event an ice condenser door open alarm is annunciated in the Control Room (refer to Table 12-1 for occupancy and dose rate limit for the Incore Instrument Room).

7.6.5.1.2 Equipment and Personnel Access Doors

The position of the equipment access doors and seals and the equipment access personnel doors is monitored by a green “DOORS CLOSED” and a red “DOORS OPEN” indicating light on the Door Position Display Panel. (Refer to Figure 7-16.)

The equipment access doors (EAD) and seals (EADS), the equipment access personnel doors (EAPD), and the personnel access door (PAD) are monitored in the control room for a “door open” condition. This indication is provided on a status indication display window. (Refer to Figure 7-15.)

The Equipment Access Door Seals (EADS) have been modified so that the Equipment Access Doors are permanently in the closed position with the Equipment Access Door Seals deflated. Therefore, the alarm indication has been rewired to remove the Equipment Access Door Seals (EADS) alarm portion from the rest of the circuitry.

7.6.5.1.3 Ice Bed Temperature Monitoring

Resistance temperature detectors (RTD’s) and temperature switches are located in various parts of the ice condenser. They serve to verify attainment of a uniform equilibrium temperature in the ice bed and to detect general gradual temperature rise in the cooling system if breakdown occurs.

Ice Bed RTD’s include two that are plenum mounted and forty-five that are probe assembly mounted, attaching to the lattice frame located throughout the ice bed. Floor Thaw RTD’s are mounted to the wear slab and located in bays most vulnerable to freeze-thaw cycles. These forty-eight (forty-seven with one spare) Ice Bed RTD’s and eight Floor Thaw RTD’s tie into a temperature scanner unit, located adjacent to the Incore Instrument Room area. The scanner multiplexes the ice condenser RTD's signals to a Westronics recorder in the main control room. There are also six temperature switches located at various points in the ice bed to serve as backup indication should the scanner unit or recorder fail to operate. These inputs provide an alarm on the Control Room annunciator panel should the ice bed temperature exceed present value. (Refer to Table 7-16 and Figure 7-17 for location of these detectors.) (Refer to Figure 7-18 for a monitor system block diagram.)

In addition, there are other RTD’s that terminate inside a panel adjacent the Incore Instrument Room area for manual temperature gathering. Sixteen Floor Cooling RTD’s are surface mounted to the glycol outlet pipe as it transitions from specific bays to the return header. Four Floor Cooling Glycol RTD’s are surface mounted to the glycol pipe headers near the floor cooling pumps and the defrost heaters. Eight Wall Panel RTD’s are mounted in the duct from air handling units. Six Wear Slab RTD’s are mounted to the floor. (Refer to Figure 7-17 and Figure 7-18, and Table 7-16.)

7.6.5.2 Ice Condenser Controls

Ice condenser controls are designed to sequence the operation of the system. The refrigeration subsystem and the ice condenser region must be in operation and the Containment ice bed region maintained at 15°F before any ice can be placed in the Containment area.

In order to facilitate the discussion the Ice Condenser System has been grouped into the following Subsystems.

Refrigeration Subsystem
Ice Condenser Region

7.6.5.2.1 Refrigeration Subsystem

Four 50 ton chiller packages are provided, each package consists of two separate self-contained 25 ton units, individually operable but mounted on a common base. Each unit is a closed refrigeration system provided with local control. Three of the packages are normally operating with the fourth package as a stand-by.

Six ice condenser glycol pumps are designated to supply glycol through the ice condenser refrigeration units and then to all the heat transfer areas. During normal operation four pumps are operating with two pumps on stand-by. Controls are provided on the local control panel in the Auxiliary Building (ice condenser control cabinet) with local status indication.

One ice condenser glycol mixing and storage pump is utilized for injecting freshly mixed glycol into the main glycol recirculation piping as necessary. This pump is controlled locally from the ice condenser control cabinet with local status indication.

7.6.5.2.2 Ice Condenser Region

During normal operation thirty (30) air handling units serve to cool the air and to circulate the cooled air through the ice condenser wall panels to keep the ice subcooled in the ice beds. Each air handling unit consists of two air handlers in a common housing. Each sub-unit consists of two separate coils, fans, drive motors and control circuits with defrost heaters, dampers, unit isolation valves, hoses and glycol control valve. Motor controls and status indication is provided for each unit on a local control panel (air handler control panel) located in the Auxiliary Building. Proximity switches are installed on each back draft damper of the air handler units. Whenever a particular damper is closed, a light is lit on the local back-draft damper status panel in the Incore Instrumentation Room. If this condition persists for more than two hours, an alarm annunciates on the Control Room annunciator panel.

The ice condenser glycol expansion tank is provided with annunciation and display on the Control Room annunciator panel to warn the operator of coolant level excursions in the glycol tank. Indication of Hi-Hi, Hi, Lo, and Lo-Lo liquid levels are displayed. Two normally open solenoid valves are provided to prevent excessive spillage. These valves close on a “Lo-Lo” signal from level sensor in the glycol expansion tank.

There are two 100% capacity floor cooling pumps provided to distribute the glycol coolant to the floor cooling coils. One pump is operating normally, with the other pump for stand-by. Local control and indication is provided on the ice condenser control panel.

One air operated valve 1NF233B (glycol return Containment isolation valve) is provided to isolate the glycol flow inside Containment. This valve is normally open. Upon receipt of an St signal from the SSPS, the valve is closed for Containment isolation. Control and indication of valve status is also provided in the Control Room on the main control board.

Two air-operated solenoid valves 1NF234A and 228A (glycol return Containment isolation valves) are provided to isolate the glycol flow outside Containment. Each valve is normally open. Upon receipt of a St signal from the SSPS, the valve is closed for Containment isolation. Control and indication of each valve is also provided in the Control Room on the main control board.

In the unlikely event of a loss of glycol in the floor coolant system, pressure sensors are provided to monitor the glycol flow. An alarm and indication is provided on the annunciator panel in the Control Room to make the operator aware of any loss. The glycol temperature is also alarmed on the annunciator panel if the temperature is too high or too low.

7.6.5.2.3 Design Basis Information

The control and instrumentation for the Ice Condenser System is designed to provide reliable and continuous manual control of system equipment under normal plant operating conditions. Automatic controls are provided for isolation of the Ice Condenser Systems glycol flow upon receipt of an St signal.

Conformance to Section 3 of IEEE 279-1971 is discussed in Sections 7.6.5.1 thru 7.6.5.2.2 above. The required monitoring and detection capability is provided directly in the Ice Condenser System instrumentation and control system and externally in the SSPS. Safety mode actuation is accomplished through control interfaces, implemented as control outputs provided by the SSPS. Refer to Section 7.3. Other design basis considerations are discussed in Sections 8.1.4, 8.3.1, 3.10, 3.11, and Table 3-3, and Table 3-7.

7.6.5.3 Analysis

7.6.5.3.1 Introduction

The design of the Ice Condenser System, including design bases, evaluation and test and inspection, is discussed in Sections 6.1.5 and 6.2.2. The intent of this analysis is to present the extent to which the design of systems instrumentation meets the applicable portions of IEEE 279-1971 in compliance with NRC Regulatory Guide 1.70.

7.6.5.3.2 General Functional Requirements

The instrumentation and control provided for the Ice Condenser System enables the operator to evaluate system performance and detect malfunctions. The instrumentation essential to the systems safety function is designed for operation under environmental conditions specified in Section 3.11.

7.6.5.3.3 Single Failure Criterion

The Ice Condenser System is designed so that any single failure within the systems safety related valves actuated by Train A and Train B or any portion of the system does not affect the integrity of the ice bed. The design objective is that the insulation of the cavity is adequate to prevent ice melting for at least 7 days in the unlikely event of a complete loss of refrigeration capability. Time exists for an orderly shutdown prior to ice melting.

7.6.5.3.4 Quality of Components and Modules

The components of the Ice Condenser System are of a quality consistent with requirements of 10CFR50.65, "Maintenance Rule Program".

7.6.5.3.5 Equipment Qualification

The Ice Condenser System instrumentation and controls meet the requirements as described in Sections 3.10 and 3.11.

7.6.5.3.6 Channel Integrity

The instrumentation and controls associated with the Ice Condenser System that are essential to each trains function are designed to maintain the necessary functional capability under the conditions specified in Section 3.11.

7.6.5.3.7 Channel Independence

Channel independence is achieved by physical and electrical separation of Train A and Train B components. The instrumentation and controls of the components of Train A are physically and electrically separate and independent of the instrumentation and controls of the components of Train B. Single failure of the control circuitry will cause, at maximum, only a failure of a component or components within one of the two independent trains.

7.6.5.3.8 Control and Protection System Interaction

No portion of the Ice Condenser System instrumentation and controls are used for both control and protection as described in Section 4 of the IEEE 279-1971.

7.6.5.3.9 Derivation of System Inputs

The Ice Condenser System inputs are derived from signals that are direct measures of the desired variable. Variables which are measured directly include temperature, Containment pressure, flow and level.

7.6.5.3.10 Indication of Bypasses

There are no bypasses capable of preventing the safety mode initiation signal from performing its intended function.

7.6.6 Deleted Per 2008 Update

7.6.6.1 Deleted Per 2008 Update

7.6.6.2 Deleted Per 2008 Update

7.6.6.2.1 Deleted Per 2008 Update

7.6.6.2.2 Deleted Per 2008 Update

7.6.6.2.3 Deleted Per 2008 Update

7.6.6.2.4 Deleted Per 2008 Update

7.6.6.2.5 Deleted Per 2008 Update

7.6.6.2.6 Deleted Per 2008 Update

7.6.6.2.7 Deleted Per 2008 Update

7.6.6.2.8 Deleted Per 2008 Update

7.6.6.2.9 Deleted Per 2008 Update

7.6.6.2.10 Deleted Per 2008 Update

7.6.6.3 Deleted Per 2008 Update

7.6.7 Spent Fuel Cooling System

The Spent Fuel Cooling System design is described in Section 9.1.3 and shown on Figure 9-13. The system is not needed for safety injection, but is designed to meet appropriate sections of IEEE 279-1971 to guarantee the spent fuel pool water is maintained at the design temperatures. The instrumentation and controls for this system are presented below.

7.6.7.1 Description

7.6.7.1.1 Initiation Circuits

The fuel pool cooling pumps are actuated manually from the Control Room, and, on a blackout condition, are powered from the diesel generators and can be manually restarted if needed.

7.6.7.1.2 Logic

Instrumentation is provided in the Control Room for indication of spent fuel pool temperature and level. Additional instrumentation is provided locally to indicate the discharge pressure of each fuel pool cooling pump and the effluent flow of each fuel pool cooling heat exchanger.

Alarms are provided in the Control Room for high and low fuel pool cooling heat-exchanger outlet flow, high fuel pool temperature, high and low fuel pool level, and low fuel pool cooling

demineralizer flow. A status light is provided in the Control Room to warn the operator when any administrative action is taken that defeats either of the safety trains. Alarms are actuated in sufficient time to allow the operator to take the appropriate corrective action. Additional detail is provided in Section 9.1.3.2.6.1 regarding system instrumentation.

7.6.7.1.3 Bypasses

There are no bypasses capable of preventing the loading of the fuel pool cooling pumps on the Essential Auxiliary Power System. Additional testing information is contained in Section 8.3.1.

7.6.7.1.4 Interlocks

There are no interlocks capable of preventing the operation of the fuel pool cooling pumps.

7.6.7.1.5 Sequencing

The fuel pool cooling pumps are sequentially supplied power from the Essential Auxiliary Power System following safety mode initiation. The pumps can then by manually started from the Control Room. The conditions for this are described in Section 8.3.1.1.7 and in the order shown on Figure 8-3.

7.6.7.1.6 Redundancy

The two trains of spent fuel pool cooling equipment per unit are completely redundant. The purification and skimmer loops are not redundant and are not safety related.

7.6.7.1.7 Diversity

Conditions requiring the sequencing of the fuel pool cooling pumps on the Essential Auxiliary Power System during blackout are detected by diverse means.

7.6.7.1.8 Actuated Devices

No devices in the Spent Fuel Cooling System are directly actuated by the safety mode initiation signal. However, the fuel pool cooling pumps are given a permissive start by the sequencer.

7.6.7.1.9 Supporting Systems

The Spent Fuel Pool Cooling System receives electrical power from the Essential Auxiliary Power System which is described in Section 8.3. The system also receives cooling water from the Component Cooling System which is described in Section 9.2.2.

7.6.7.1.10 Design Basis Information

The design basis of the Fuel Pool Cooling System instrumentation is to provide alarms and indication for the manual operation of the cooling and purification system. This system has no protective function as defined in Section 2 of IEEE 279-1971. However, the following discussion responds to the provisions of Section 3 of IEEE 279-1971 as applicable to this instrumentation.

1. The system instrumentation provides indication for monitoring the operation of the Spent Fuel Cooling System, and provides alarms for abnormal system conditions.

2. The variables monitored to provide the required function are fuel pool level, fuel pool temperature, fuel pool heat exchanger inlet and outlet temperature, and fuel pool pump discharge pressure.
3. One level switch is provided in the fuel pool for the high and the low level alarms.

   One temperature sensor is provided in the fuel pool for indication and for the high temperature alarm.

   One temperature test connection is provided at the inlet and outlet of each fuel pool heat exchanger for the testing indication.

   One pressure detector is provided at the discharge of each fuel pool pump for local indication.

7.6.7.2 Analysis

There are no specific NRC Regulatory Guides or General Design Criteria applicable to this instrumentation.

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard, and as such, are not directly applicable to this instrumentation. A discussion of the extent to which the design of this system's instrumentation meets the applicable portions of IEEE 279-1971 is provided below in compliance with the NRC Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants.

The following refers to the requirements set forth in Section 4 of IEEE 279-1971.

1. General Functional Requirements

   The Spent Fuel Cooling System instrumentation essential to the system's required function is designed for the normal plant operating environment and is not required to function under abnormal or accident conditions.

2. Single Failure Criterion

   No single failure to the Spent Fuel Cooling System instrumentation can affect the operation of more than one of the pool cooling loops. Each of the redundant pool cooling loops is designed to maintain the pool temperature within the required limits.

3. Quality of Components and Modules

   Components of the Spent Fuel Cooling System instrumentation are of a quality consistent with 10CFR50.65 "Maintenance Rule Program".

4. Channel Integrity

   The instrumentation associated with the Spent Fuel Cooling System which is essential to the system's required function is designed to maintain the necessary functional capability under normal plant environmental conditions.

5. Channel Independence

   Instrumentation associated with one of the safety related pool cooling loops is physically and electrically isolated from that of the redundant pool cooling loop.

6. Control and Protection System Interaction

   No protective function, as defined in Section 2 of IEEE 279-1971, is required of this instrumentation.

7. Derivation of System Inputs

   System inputs are derived from direct measurement of the desire variable.

8. Operating Bypasses

   There are no bypasses of protective functions, as defined in Section 4-12 of IEEE 279-1971, associated with this instrumentation.

7.6.8 Fuel Handling System

The Fuel Handling System design is described in Section 9.1.4 The refueling interlocks are the only part of the Fuel Handling System required for safety and thus covered under Section 7.6.8.

7.6.8.1 Description

7.6.8.1.1 Initiating Circuits

The manipulator cranes travel under local manual, semi-automatic or automatic control with direct operator supervision. All hoist operations are under direct manual control. Interlocks are completely automatic and prevent any actions by the operator that could be detrimental to the system.

7.6.8.1.2 Logic

Refer to Section 9.1.4.3.1 for a description of the refueling interlock logic.

7.6.8.1.3 Bypasses

7.6.8.1.3.1 Fuel Transfer System

There are three interlock bypasses in the Fuel Transfer System.

1. Upender/Manipulator Crane Interlock Bypass - A bypass switch located on the Fuel Transfer System refueling canal control console allows for operation of the refueling canal upender even though the reactor manipulator crane gripper is not in the up position (gripper in the mast when a fuel assembly is not engaged; gripper full up when a fuel assembly engaged) or the reactor manipulator crane is not located over the core. A similar bypass switch on the Fuel Transfer System spent fuel pool control console allows for operation of the fuel pool upender even though the fuel pool manipulator crane gripper is not in the up position or the spent fuel manipulator crane is not located outside of the basket area.
2. Transfer Car/Upender Position Interlock Bypass - A bypass switch located on the Fuel Transfer System spent fuel pool control console allows for operation of the transfer car even though one or both upenders are not in the down position.
3. Upender/Transfer Car Position Interlock Bypass - Bypass switches on each Fuel Transfer System control console allows for operation of the upenders even though the transfer car is not located at either end of its travel.

7.6.8.1.3.2 Reactor and Fuel Pool Manipulator Cranes

Deleted Per 2012 Update.

There are three interlock bypasses on the reactor manipulator crane and four on the fuel pool manipulator crane. The control switches/buttons for these bypasses are located on the crane control consoles.

1. Travel Override Switch - This switch bypasses all travel interlocks and essentially allows the crane to bridge and trolly unrestricted anywhere that is physically possible regardless of the proximity of the mast to interferences (e.g. walls, pipes, etc.). The switch allows operators access to areas that are outside of the normal secure zone but at reduced speeds to perform miscellaneous activities (e.g. access spent fuel pool perimeter cell locations).
2. Interlock Override Switch - This key switch essentially bypasses all PLC interlocks and is typically only used for equipment testing or to recover from equipment failure.
3. Hoist Load Bypass Button - This button temporarily adjusts the load protection setpoints while raising and lowering fuel assemblies to eliminate nuisance load trips. When the button is pressed and held, the maximum allowable fuel assembly drag force is increased by a preset value until the button is released. The load bypass preset value is based on the fuel manufacturers' guidelines.
4. Monorail Up Bypass Switch (fuel pool manipulator crane only) - This switch allows the manipulator crane hoist, bridge, and trolley to operate without the north monorail hoist in the full up position.

7.6.8.1.4 Interlocks, Redundancy

Deleted Per 2012 Update.

In the analysis below, the refueling interlocks have only been analyzed for failure in the permissive mode. The consequences of interlock failure in the interlocked mode are the same for all; the failed interlock would prevent normal operation of the equipment until repaired. There is no case where failure in the interlocked mode can result in a hazardous situation. The manipulator crane interlocks are as listed in Section 9.1.4.3.

1. Bridge, Trolley, and Hoist Drive Mutual Interlocks

   Because the drives are mutually interlocked, at least two component failures would be required to defeat the interlock. Therefore the single failure criterion is satisfied.

2. Bridge and Trolley Drive/Gripper Interlock

   This interlock is based on inputs from the hoist encoders, load cell, and gripper engaged position switch. Because the hoist encoders are redundant and the loaded/unloaded conditions are based on combined inputs from the load cell transducer and the gripper engaged position switch, more than one component failure would be required to defeat this interlock. Therefore the single failure criterion is satisfied.

3. Gripper/Load Cell Interlock

   Because the mechanical weight actuated lock in the gripper provides backup protection to the PLC interlock based on the load cell input, more than one component failure would be required to defeat the interlock. Therefore the single failure criterion is satisfied.

4. Hoist Overload/Underload Interlocks

   Normal hoist overload/underload protection relies on a single load input from the load cell transducer and therefore could be defeated by a single component failure. This could result in drag forces imposed on fuel assemblies in excess of fuel manufacturers' recommendations, but would not cause a breach of the fuel cladding because an external

mechanical overload switch would limit the maximum load when raising a fuel assembly to approximately 3200 lbs. When lowering a fuel assembly the maximum load would be naturally limited to the combined weight of the fuel assembly, insert, and the inner mast/gripper weight (less than 2500 lbs).

5. Hoist/Gripper Position Interlock

   Gripper position consists of two PLC inputs from separate switches for the engaged and disengaged gripper positions. The permissive to allow hoist motion is active when only one of the switches is closed, so both switches would have to fail to defeat the interlock. Therefore the single failure criterion is satisfied.

6. Bridge and Trolley Travel Interlocks

   Because bridge and trolley travel within the secured zone is based on redundant encoder inputs to the PLC, more than one component failure would be required to allow a collision. Therefore the single failure criterion is satisfied within the secured zone. Travel outside the secured zone is available by defeating the interlock using a bypass switch, but travel speed would be limited to reduced speeds and in the event of a collision the fuel assembly would be protected from damage by the outer mast. The mast is a 16 inch diameter, 3/4 inch wall pipe that completely encloses the fuel. Within the mast, the fuel is restrained by guide bars at all four corners that limit the lateral movement of the fuel to 1/4 inch maximum.

7. "Slow Zone" Interlocks

   The hoist "Slow Zones" are defined by inputs from the redundant hoist encoders (vertical position), redundant bridge and trolley encoders (horizontal position), and combined inputs from the load cell transducer and the gripper engaged position switch. Multiple component failures would be required to permit a fuel assembly to transit a "Slow Zone" at a higher speed. Therefore the single failure criterion is satisfied.

8. Manipulator Crane/Upender Full Up Interlock

   This interlock is based on a single input from the upender controls and therefore could be defeated by a single component failure. Failure of this interlock in the permissive mode would allow a fuel assembly to be raised out of or lowered into the upender when the upender is not in the full up position. However damage to the fuel would be prevented by the hoist load interlock that would stop the hoist if loads in excess of the normal overload and underload setpoints were imposed on the fuel assembly. Since more the one component failure would be required to cause fuel assembly damage, the single failure criterion is satisfied.

9. Fuel Pool Manipulator Crane/New Fuel Elevator Interlocks

   These interlocks are based on single inputs from the fuel pool manipulator crane and the new fuel elevator and therefore they can be defeated by a single component failure. Failure of these interlocks in the permissive mode could result in physical contact between the crane mast and the elevator basket either by moving the mast into a raised elevator or by raising the elevator into the mast. In either case the fuel assembly would be protected from damage by the outer mast.

10. Monorail Hoist Up Interlock

    This interlock is based on a single input from the north monorail hoist and therefore can be defeated by a single component failure. Failure of this interlock could result in moving the crane with a fuel assembly partially inserted in a storage location (e.g. fuel storage rack, new fuel elevator, etc.). Prevention of this scenario relies on the crane operator adhering to

procedure requirements to not bridge or trolley the manipulator crane unless the north monorail hoist is in the full up position.

The fuel transfer system interlocks are as listed in Section 9.1.4.3.

1. Transfer Car/Upender Position Interlock

   This interlock does not satisfy the single failure criterion. The interlock is primarily designed to protect the equipment from overload and possible damage.

   Assuming the interlock fails in the permissive mode, there are two accidents to be considered. First, the upender basket in the fuel transfer canal is up or partially up and the car is driven towards the fuel pool home position. In this case, the bottom end of the upender basket is pivoted down so the car and fuel container cannot pass under it. The car would hit the end of the upender basket and stall the drive. No fuel damage is possible since the container structure protects it from contacting the lifting frame.

   The second case occurs when the upender basket has engaged the fuel container and lifted it to a vertical position. If the interlock has failed and an attempt is made to move the car, the result would be that the car tries to move out from under the fuel container which is held fast in the upender basket. The car drive is not powerful enough to pull the fuel container out of the lifting frame and the system would stall.

2. Transfer Car Permissive Switch Interlock

   This interlock is a backup for the Transfer Car/Upender Position Interlock. Even if the interlock between the permissive switches fails in the permissive position, the transfer car cannot be moved unless the upender position interlock is satisfied. The interlock, therefore, satisfies the single failure criterion.

3. Upender/Transfer Car Position Interlock

   This interlock is redundant and satisfies the single failure criterion.

4. Transfer Car/Transfer Tube Valve Position Interlock

   This interlock does not satisfy the single failure criteria. If the interlock fails in the permissive mode, the car can be started with the valve not fully open. The transfer car would contact the valve gate and stall the motor drive with no damage to the fuel.

5. Upender/Manipulator Crane Interlock

   This interlock does not satisfy the single failure criteria. If the interlock fails in the permissive mode, the upender could be started down from the vertical position while the manipulator is lowering a fuel assembly into the fuel container. The fuel container would move downward until the top contacts the fuel. Since the fuel container is not driven down, the force it could exert on the fuel assembly is limited to the overturning moment built into the equipment to make it lower by gravity.

7.6.8.1.5 Actuated Devices

The only device actuated on an interlock failure is the gripper interlock failure audible alarm located on each of the crane control consoles. This alarm occurs when the gripper engaged and gripper disengaged limit switches are both closed or both open.

7.6.8.1.6 Supporting Systems

The Fuel Handling System receives electrical power from the Normal Auxiliary Power System which is described in Section 8.3.

7.6.8.1.7 Design Bases Information

7.6.8.1.7.1 Design Bases

The design bases for the safety related portions of the Fuel Handling System is to provide the necessary interlocks, controls, and alarms to prevent fuel assembly damage during refueling operations. Refer to Section 9.1.4.3.1 for a description of the provisions made to ensure safe handling of the fuel assemblies.

7.6.8.1.7.2 Conform to IEEE 279-1971

Sections 3 (1) through 3 (6) of IEEE 279-1971 address the monitoring and detection of plant operating conditions requiring protective action. The Fuel Handling System is not operational during normal plant operation; and, therefore, the above sections are not applicable.

Information required by Section 3 (7) of IEEE 279-1971 concerning the energy supply is discussed in Sections 8.1.4 and 8.3.1 Environmental considerations are discussed in Section 9.1.4.

Equipment malfunction information is covered in Section 7.6.8.1.4. Accidents and unusual events are covered in Section 9.1.

7.6.8.1.8 Final System Drawings

Functional block diagrams, electrical elementaries and other drawings required to assure electrical separation and perform a safety review are provided in the McGuire Electrical Schematics.

7.6.8.2 Analysis

7.6.8.2.1 NRC General Design Criteria

Implementation of the requirements of NRC General Design Criteria is described in Section 3.1.

7.6.8.2.2 Single Failure Criterion

See Section 7.6.8.1.4.

7.6.9 Refueling Water System

The Refueling Water System design is described in Section 9.2.5 and shown on Figure 9-65. The instrumentation and controls for this system are presented below.

7.6.9.1 Description

7.6.9.1.1 Initiating Circuits

The system normally operates under manual control by the plant operator. Safety mode operation is initiated by actuation of the unit Solid State Protection System. The realignment

process is fully automatic, with the initiation signal overriding the normal control system. The SSPS actuation initiates realignment of all isolation valves required for safety mode operation of the Refueling Water System of the affected unit.

7.6.9.1.2 Logic

In normal operation the Refueling Water System is manually controlled by the plant operator as described in Section 9.2.5.2. On receipt of a safety actuation signal, the system is realigned to isolate the Refueling Water Storage Tank (RWST) and assure that the water is available for the Emergency Core Cooling System (ECCS).

7.6.9.1.2.1 RWST Temperature

Instrumentation is provided in the Control Room to allow the operator accurate indication of the RWST water temperature. Adequate alarms are also provided in the Control Room to warn the operator of decreasing RWST water temperature. There are three 40 KW heater clusters available to heat this water. The first heater cluster starts automatically while the second and third heater clusters are manually actuated.

7.6.9.1.2.2 RWST Level

Instrumentation is provided in the Control Room in triplicate to allow the operator accurate indication of the RWST level. Adequate alarms are also provided in the Control Room to warn the operator of decreasing RWST level. On receipt of a safety actuation signal, the system is aligned and water is supplied to the ECCS. Upon completion of the injection mode, the valve in the RWST line to the safety injection pump line is closed by the operator as discussed in Section 6.3.2.2.2 and delineated in Table 6-125 through Table 6-129.

7.6.9.1.3 Bypasses

There are no bypasses capable of preventing the SSPS signal from performing its intended functions. Additional bypass discussion is contained in Section 7.8.2.

7.6.9.1.4 Interlocks

There are no interlocks capable of blocking the SSPS signal from performing its intended functions. There are no interlocks capable of preventing the operation of the valve in the discharge line of the RWST.

7.6.9.1.5 Sequencing

The Refueling Water System safety equipment is sequentially loaded on the Essential Auxiliary Power System following safety mode initiation under the conditions described in Section 8.3.1.1.7.

7.6.9.1.6 Redundancy

The two trains of RWST isolation valves are completely redundant.

7.6.9.1.7 Diversity

Operating conditions requiring isolation of the RWST on SSPS are detected by diverse means.

7.6.9.1.8 Actuated Devices

Devices in the Refueling Water System actuated by the safety mode initiation signal are shown on Figure 9-65 and include the RWST isolation valves.

7.6.9.1.9 Supporting Systems

The Refueling Water System receives electrical power from the Essential Auxiliary Power System which is described in Section 8.3.

7.6.9.1.10 Design Basis Information

7.6.9.1.10.1 Design Bases

The controls and instrumentation for the Refueling Water System are designed to provide reliable and continuous manual control of system equipment under normal plant operating conditions. Overriding automatic controls are provided to realign the equipment to a safety mode of operation upon receipt of a safety actuation signal.

7.6.9.1.10.2 Conformance to IEEE 279-1971

Section 3 of the IEEE 279-1971 addresses the monitoring and detection of plant operating conditions requiring protective action. The required monitoring and detection capability is not provided directly in the Refueling Water System instrumentation and control system. Instead, these functions are performed externally in the SSPS and power monitoring circuits and safety mode actuation is accomplished through control interfaces, implemented as control outputs provided in the SSPS and power monitor hardware, and hard wired into Refueling Water System control circuits. A discussion of the required monitoring and detection functions therefore concerns the SSPS and power monitors rather than Refueling Water System. The SSPS is discussed in Section 7.3. The Essential Auxiliary Power System is discussed in Section 8.1.4 and Section 8.3.

7.6.9.2 Analysis

7.6.9.2.1 NRC General Design Criteria

Implementation of the requirements of the NRC General Design Criteria is described in Section 3.1.

7.6.9.2.2 Conformance to IEEE 279-1971

IEEE 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations,” establishes minimum requirements for the reactor protective and engineered safety features instrumentation and control systems. The instrumentation and controls associated with the Refueling Water System are not defined as a protective system in IEEE 279-1971; however, many criteria of IEEE 279-1971 have been incorporated in the design of the instrumentation and controls for this system.

The Refueling Water System controls are designed such that no single failure can prevent a safe shutdown.

Single failures considered include electrical faults (e.g., open, shorted or grounded circuits) and physical events (e.g., fires, missiles) resulting in mechanical damage. Compliance with single

failure criterion is accomplished by separating the redundant elements electrically and physically to achieve the required independence.

7.6.10 Control, Equipment and Cable Rooms Heating, Ventilation and Air Conditioning

The Control, Equipment, and Cable Rooms Heating, Ventilation and Air Conditioning (CRA HVAC) system design is described in Section 6.4 and shown on Figure 6-191. The instrumentation and controls are presented below.

7.6.10.1 Description

7.6.10.1.1 Initiating Circuits

Safety mode operation is initiated by a unit Engineered Safety Features Actuation System (ESFAS) signal or LOOP condition. The safety mode realignment process is fully automatic.

The ESFAS or blackout actuation initiates realignment of all equipment required for safety mode operation.

7.6.10.1.2 Logic

The HVAC System can be aligned to one of several modes of operation from the Control Room. System alignment in these various operator selected modes is automatic from the point of operator selection of chilled water pump and chiller compressors. Upon receipt of an ESFAS or LOOP signal, an automatic system realignment is initiated which effects complete isolation of the two redundant trains through repositioning of crossover isolation valves. The chilled water pump, chiller, CRA-AHU, SWGR AHUs & battery room fans associated with the selected train are automatically sequenced to the Essential Auxiliary Power System at this time. In addition, both OAPFTs & C/R AHUs start, regardless of the selected train. The other train remains in a standby condition as a backup to the preferred train, but is not required to provide cooling capacity. The backup train can be placed in service at any time by operator action from the Control Room. Either train alone is capable of providing the required cooling capacity for maintaining the habitability of the Control Room environment under design basis conditions.

Isolation of the outside air intakes is initiated manually following either high radiation or high chlorine concentration alarms. High radiation is sensed by a radiation monitor located at each location. High chlorine concentration is sensed by a chlorine monitor located at each intake. In the event one of these conditions is sensed at both outside air intake locations, the least contaminated intake is selected.

High smoke level in the discharge duct of the Control Room AHU or the Control Room Area AHU stops the AHU with the high smoke level. Smoke detector instrumentation is provided in the discharge air ducts of the above AHU's by the Fire Protection System. A smoke purge fan with manual controls is provided to clear the Control Room of smoke.

7.6.10.1.3 Bypasses

Selector switches are provided to select the HVAC train that will operate during a LOOP or a LOCA. The remaining train of HVAC is available as a backup. When swapping trains, the inactive train is selected while allowing the operating train to run. An annunciator will alarm any time both trains are selected to remind the operator to trip one train. When both trains are selected, the banana-type dampers will allow flow from both control room area air handling

units, so no damage should occur to these fans. It is not recommended that both trains be run simultaneously for an extended period of time.

Both trains of chilled water valves, control room air handling units and control room area outside pressure filters are automatically activated by a LOOP or a LOCA and are not affected by the train selector switches.

7.6.10.1.4 Interlocks

Other than normal operating interlocks, there are no interlocks capable of blocking the safety alignment initiation signals. Normal operating interlocks include instrumentation which shuts down the Control Room and Control Room Area AHU's on discharge smoke detection, or shuts down a chiller compressor upon:

a. Indication of unexpected refrigerant temperatures and pressures.

b. Indications of abnormal oil lubricant conditions.

7.6.10.1.5 Sequencing

CRA HVAC equipment is sequentially loaded on the Essential Auxiliary Power System under conditions described in Section 8.3.1.1.7 and in the order shown in Table 8-1.

7.6.10.1.6 Redundancy

Most components of the two trains of the CRA HVAC System are 100% electrically redundant. Exceptions include dampers CRA-OAD-3, CRA-OAD-4, SP-D-1, SP-D-2.

7.6.10.1.7 Diversity

Operating conditions requiring actuation of the CRA HVAC on ESFAS are detected by diverse means.

7.6.10.1.8 Actuated Devices

Devices actuated on ESFAS and LOOP are shown in Table 7-17.

7.6.10.1.9 Supporting Systems

The CRA HVAC System receives electrical power from the Essential Auxiliary Power System which is described in Section 8.3.

Cooling water is supplied to the chiller compressor condensers from the Nuclear Service Water System (RN) which is described in Section 7.4.1.2. Makeup water for the Chilled Water System is provided by the Makeup Demineralizer System (YM).

The Radiation Monitoring System and the Fire Protection System provide instrumentation for radiation and smoke detection, respectively.

7.6.10.1.10 Design Basis Information

7.6.10.1.10.1 Design Bases

The control and instrumentation for the CRA HVAC System is designed to provide reliable and continuous control of CRA HVAC equipment under all plant operating conditions. The controls provide for manual operation under normal conditions with automatic safety realignment

following the onset of abnormal plant conditions. Control and instrumentation is designed to maintain the separation and redundancy provided by the mechanical design of the CRA HVAC system.

7.6.10.1.10.2 Conformance to IEEE 279-1971

Section 3 of IEEE 279-1971 addresses the monitoring and detection of plant operating conditions requiring protective action. The required monitoring and detection capability is not provided directly in the CRA HVAC instrumentation and control system. Instead, these functions are performed externally in the ESFAS and power monitoring circuits. Safety mode actuation is accomplished through control interfaces, implemented as control outputs provided in the ESFAS and power monitor hardware and hard wired into CRA HVAC control circuits.

The ESFAS is in the vendor scope of supply and is discussed in Section 7.3. The Essential Auxiliary Power System is discussed in Sections 8.1.4 and 8.3.

7.6.10.1.11 Summary Flow Diagrams

See Figure 6-191.

7.6.10.1.12 Location Layout Drawings

See Figure 1-6.

7.6.10.1.13 Conformance to NRC General Design Criteria 19

See Section 6.4 and 3.1 - Criterion 19.

7.6.10.2 Analysis

7.6.10.2.1 NRC General Design Criteria

Implementation of the requirements of NRC General Design Criteria is described in Section 3.1.

7.6.10.2.2 IEEE 279-1971

IEEE 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations,” establishes minimum requirements for the reactor protective and engineered safety features instrumentation and controls systems. The instrumentation and controls associated with the CRA HVAC system are not a protective system as defined in IEEE 279; however, many criteria of IEEE have been incorporated in the design of the instrumentation and controls for this system. These criteria are addressed in the following sections.

7.6.10.2.2.1 Single Failure Criteria

The CRA HVAC system instrumentation and controls are designed and located such that no single failure can prevent the system from performing its design function. Single failures considered include electrical faults (e.g., open, shorted, or grounded circuits) and physical events (e.g., fires, missiles) resulting in mechanical damage. Compliance with single failure criterion is accomplished by providing redundancy of power supplies, actuation capability and by separating the redundant elements electrically and physically to achieve the required independence.

7.6.10.2.2.2 Quality of Components and Modules

The Quality Assurance Program is described in Chapter 17. This program has established requirements for design review procurement, inspection, and testing to ensure that system components are of a quality consistent with 10CFR50.65, "Maintenance Rule Program".

7.6.10.2.2.3 Equipment Qualifications

System instrumentation and controls meet the equipment requirements as described in Sections 3.10 and 3.11.

7.6.10.2.2.4 Channel Integrity

The CRA HVAC system will maintain its functional integrity within the environmental boundaries established in Section 3.11.4 and Section 6.4.

7.6.10.2.2.5 Channel Independence

Channel independence is achieved by physical and electrical separation as described in Section 7.6.10.2.2.1.

7.6.10.2.2.6 Control and Protection System Interaction

Isolation relays are provided for separation between the ESFAS and control system where ESFAS signals are used as part of the control system. These isolation devices meet all requirements previously stated Section 7.6.10.2.2.

7.6.10.2.2.7 Derivation of System Inputs

System inputs are derived from signals that are direct measures of the desired variables.

7.6.10.2.2.8 Operating Bypasses

Refer to Section 7.6.10.1.3 for a description of bypasses.

7.6.10.2.3 Other Appropriate Standards and Criteria

The identification and extent of applicability of other appropriate standards and criteria is presented in Section 7.1.2.

7.6.10.2.4 Failure Mode and Effects Analysis

See Table 6-138.

7.6.11 Groundwater Drainage System

The Groundwater Drainage System is described in Section 2.4.13.5 and Section 9.5.8. Physical layout and instrumentation are shown in Figure 2-62, Figure 2-63 and Figure 9-146 respectively. The instrumentation and controls associated with the system include redundant sump level measurements and fully automatic controls for the redundant Safety Class 3 pumps.

7.6.11.1 Description

7.6.11.1.1 Initiating Circuits

Pump operation and remote high level alarms are initiated by the redundant level instrumentation provided in the sump.

7.6.11.1.2 Logic

For each of the three sumps, a lead-lag pump control system is used which provides automatic response to sump level signals. In sumps A, B and C, the lead pump is started at the normal high level and the backup pump is started at the normal high-high level. Operating pumps are stopped at the normal low level.

The following alarms are provided in the Control Room:

1. Failure of either pump to start at the proper level in sumps A, B, or C.
2. High water level and high-high water level in sumps A, B, and C.
3. Pump motor overloads.

7.6.11.1.3 Bypasses

Each sump pump is controlled by an auto-manual-off switch. When a switch is in the off position, the condition is indicated on the plant computer 1.47 bypass application.

7.6.11.1.4 Interlocks

There are no permissive interlocks capable of blocking actuation of either the pumps or of the remote level alarms.

7.6.11.1.5 Redundancy

The sump pumps provided for the system are Safety Class 3 and, along with their respective level instrumentation and controls, are fully redundant. Components and equipment associated with one safety class train are physically and electrically separated from and independent of the redundant train in all respects.

7.6.11.1.6 Diversity

As noted in Section 7.6.11.2.2, this system has no protection functions. The instrumentation provided, while redundant is not diverse.

7.6.11.1.7 Actuated Devices

The level instrumentation actuates the sump pumps and remote high water level alarms.

7.6.11.1.8 Supporting Systems

The system receives electrical power from the Essential Auxiliary Power System which is described in Section 8.3.

7.6.11.1.9 Design Basis Information

7.6.11.1.9.1 Design Basis

The instrumentation and controls provided are designed to provide reliable indication of sump level and continuous automatic control of pump operation to maintain water levels within the design limits.

7.6.11.1.9.2 Conformance with IEEE 279-1971 (By Section 3 Item Number)

1. The generating station conditions requiring action by this system are sump water levels in excess of the design levels. For sumps A, B, and C, levels in excess of high level require the lead pump to run and remote alarm indication of high water levels. Levels in excess of high-high level require the backup pump to run and remote alarm indication of high-high water levels.
2. The monitored generating station variable is sump water level.
3. Two independent channels of level instrumentation are provided. The instrumentation and associated alarm and control channels are physically separated and fully redundant.
4. Alarm is activated on high-high level.
5. In Conformance.
6. Levels requiring action are given in (1) above.
7. Information concerning the energy supply is presented in Section 8.1.4 and 8.3.1. Environmental considerations are described in Table 3-7.
8. Structures and equipment associated with this system are seismic Category 1 and as such are designed to withstand events and environmental conditions are described in Chapter 3.
9. Minimum system performance requirements are discussed in Section 2.4.13.5. System instrumentation accuracies of ± 0.25 feet are satisfactory for alarm and control purposes.

7.6.11.2 Analysis

7.6.11.2.1 Conformance With NRC General Design Criteria

There are no specific General Design Criteria applicable to this system.

7.6.11.2.2 Conformance With IEEE 279-1971, Section 4 (By Item Number)

This system has no protective functions as defined in IEEE 279-1971. The extent to which the design of this system satisfies the requirements of this Standard is described below.

4.1 The instrumentation and controls associated with this system are designed to initiate the appropriate action automatically and reliably at the design levels.

4.2 The instrumentation and controls associated with this system meet the Single Failure Criterion. The two trains of equipment provided are fully redundant and are electrically independent of each other.

4.3 Instrumentation and control components used with the system are of established quality.

4.5 Instrumentation and controls associated with the system are designed to maintain channel integrity under design basis conditions.

4.6 The redundant instrumentation and control channels are completely independent of and are physically separated from each other.

4.10 Capability for testing and calibrating instrumentation channels is provided.

7.6.12 Diesel Generator Fuel Oil System

7.6.12.1 System Description

The Diesel Generator Fuel Oil System is discussed in Section 9.5.4.2.

Alarms are provided locally for a low level condition in the diesel fuel oil storage tank and for high and low level in the fuel oil day tank. A local and Operator Aid Computer (OAC) alarm is provided for low fuel oil pressure to the engine. The operator is alerted to these conditions by a common alarm in the Control Room in sufficient time to take the appropriate corrective action.

The fuel oil transfer pump is automatically actuated by a low level in the diesel fuel oil day tank.

The fuel oil booster pump is automatically started with the diesel engine by the diesel start circuit. The pump runs until adequate fuel oil pressure is provided by the engine driven fuel oil pump at which time the booster pump is deenergized by a pressure switch sensing the fuel oil supply pressure.

7.6.12.1.1 Design Basis Information

The design basis for the fuel oil system instrumentation is to control and monitor the operation of the fuel oil system so that the diesel generator can function properly under accident conditions and during testing. This system has no protective function as defined in Section 2 of IEEE 279-1971. However, the following discussion responds to the provisions of Section 3 of the standard as applicable to this instrumentation.

1. The system instrumentation provides control of the fuel oil system to assure the supply of fuel oil to the diesel engine.
2. The variables monitored to provide the required function are diesel fuel oil storage tank level, fuel oil day tank level, and fuel oil supply pressure.
3. Indicating one level transmitter is provided for the fuel oil storage tank to actuate a low level alarm.

   One pressure transmitter and two current modules are provided for the fuel oil day tank. One current module provides the high and low level alarms, and the other controls fuel oil transfer pump starting and stopping on low and high levels. Local level indication is also provided.

   Two pressure switches are provided on the diesel engine fuel oil influent line. One switch provides the low pressure alarm, the other controls the operation of the booster pump.
4. No protective function as defined in Section 2 of IEEE 279-1971 is required of this instrumentation.

7.6.12.2 Analysis

There are no specific NRC Regulatory Guides or General Design Criteria applicable to this instrumentation.

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard, and as such, are not directly applicable to this instrumentation. A discussion of the extent to which the design of this system's instrumentation meets the applicable portions of IEEE 279-1971 is provided below in compliance with the NRC Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants.

The following refers to the requirements set forth in Section 4 of IEEE 279-1971:

1. General Functional Requirements

   The Diesel Generator Fuel Oil System instrumentation essential to the system safety function is designed for operation under the environmental conditions specified in Section 3.8.4.

2. Single Failure Criterion

   Any failure of the Diesel Generator Fuel Oil System instrumentation affects only the fuel oil system to which it is associated, and will in no way affect the operation of the redundant diesel generator.

3. Quality of Components and Modules

   Components of the Diesel Generator Fuel Oil System instrumentation are of a quality consistent with 10CFR50.65, "Maintenance Rule Program".

4. Channel Integrity

   The instrumentation associated with the Diesel Generator Fuel Oil System which is essential to the system's required function is designed to maintain the necessary functional capability under the environmental conditions specified in Section 3.8.4.

5. Channel Independence

   The Diesel Generator Fuel Oil System instrumentation associated with one diesel generator is physically and electrically isolated from that of the redundant diesel generator.

6. Control and Protection System Interaction

   No protective function, as defined in Section 2 of IEEE 279-1971, is required of this instrumentation.

7. System inputs are derived from direct measurement of the desired variable.

8. Operating Bypasses

   There are no bypasses of protective functions, as defined in Section 4-12 of IEEE 279-1971 associated with this instrumentation.

7.6.13 Diesel Generator Cooling Water System

7.6.13.1 System Description

The Diesel Generator Cooling Water System design is discussed in Section 9.5.5.2.

The Diesel Generator Cooling Water System instrumentation controls and monitors the system operation to maintain diesel engine temperature within its operating range. During standby

operation the jacket water heater pump circulates cooling water through the thermostatically controlled jacket water heater. The diesel starting circuit automatically deenergizes the jacket water heater and its circulating pump, and starts the jacket water pump/intercooler pump motor. Cooling water temperature during engine operation is determined by a temperature controlled valve that regulates the amount of water circulated through the systems heat exchanger.

The diesel is interlocked to automatically shutdown if the cooling water temperature, pressure or surge tank level exceeds the predetermined value. However, these interlocks are automatically bypassed for emergency operation.

Cooling water high temperature, low pressure, and low surge tank level are alarmed locally, on the OAC, and at a common alarm point in the Control Room. Setpoints are arranged to provide the alarm before the shutdown setpoint is reached. An alarm is provided locally and at the common alarm point in the Control Room when cooling water temperature falls below the level required to keep the engine ready for an emergency start.

7.6.13.1.1 Design Basis Information

The design basis for the Diesel Generator Cooling Water System instrumentation is to control the operation of the system to provide sufficient cooling water to operate the diesel at its rated output. This instrumentation has no protective function as defined in Section 2 of IEEE 279-1971. However, the following discussion responds to the provisions of Section 3 of IEEE 279-1971 as applicable to this instrumentation.

1. The system instrumentation provides control of the cooling water temperature, and provides alarms to indicate abnormal conditions of cooling water temperature, pressure, and surge tank level.
2. Diesel cooling water temperature, pressure, and surge tank level are monitored to provide the required function.
3. Two high and one low temperature switches are provided in the engine cooling water effluent line to provide the temperature alarms and the high water temperature shutdown interlock.

   One temperature sensor is provided in the jacket water heater circulating pump discharge line for control of the jacket water heater.

   Two pressure switches are provided in the engine cooling water influent line, one for the low cooling water pressure alarm and one for the shutdown interlock.

   Two level transmitters, one current module and one pressure switch are provided on the diesel generator cooling water surge tank. These provide surge tank low level alarm and engine shutdown interlock.
4. No protective function as defined in Section 2 of IEEE 279-1971 is required of this instrumentation.

7.6.13.2 Analysis

There are no specific NRC Regulatory Guides or General Design Criteria applicable to this instrumentation.

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard, and as such, are not directly applicable to this instrumentation. A discussion of the extent to which the design of this system's instrumentation meets the applicable portions of

IEEE 279-1971 is provided below in compliance with the NRC Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants.

The following refers to the requirements set forth in Section 4 of IEEE 279-1971:

1. General Functional Requirements

   The Diesel Generator Cooling Water System instrumentation essential to the system safety function is designed for operation under the environmental conditions specified in Section 3.8.4.

2. Single Failure Criterion

   Any failure of the Diesel Generator Cooling Water System instrumentation affects only the cooling water system to which it is associated, and will in no way affect the operation of the redundant diesel generator.

3. Quality of Components and Modules

   Components of the Diesel Generator Cooling Water System instrumentation are of a quality consistent with 10CFR50.65, "Maintenance Rule Program".

4. Channel Integrity

   The instrumentation associated with the Diesel Generator Cooling Water System which is essential to the system's function is designed to maintain the necessary functional capability under the environmental conditions specified in Section 3.8.4.

5. Channel Independence

   The Diesel Generator Cooling Water System instrumentation associated with one diesel generator is physically and electrically isolated from that of the redundant diesel generator.

6. Control and Protection System Interaction

   No protective function, as defined in Section 2 of IEEE 279-1971, is required of this instrumentation.

7. Derivation of System Inputs

   System inputs are derived from direct measurement of the desired variable.

8. Operating Bypasses

   There are no bypasses of protective functions, as defined in Section 4-12 of IEEE 279-1971, associated with this instrumentation.

7.6.14 Diesel Generator Starting Air System

7.6.14.1 System Description

The Diesel Generator Starting Air System design is discussed in Section 9.5.6.2. A pressure transmitter and associated current alarm module on each of the two starting air tanks for each diesel starting air system controls the operation of the air compressor associated with that air tank.

Alarms are provided locally and on the OAC for low air pressure in either of the two air tanks, for low air pressure at the engine, and low control air pressure. The operator is alerted to these conditions by a common alarm in the Control Room in sufficient time to take the appropriate corrective action.

7.6.14.1.1 Design Basis Information

The design basis for the Diesel Generator Starting Air System instrumentation is to assure that adequate air pressure is maintained in the air starting system to allow one fast start and five total starts of the associated diesel engine. Analysis based on results obtained during testing finds the McGuire diesels are capable of starting 5 times consecutively from the initial conditions of one of the two starting air receivers isolated, the other receiver at the lowest pressure allowed by Technical Specifications and diesel room temperature at the highest allowed by Selected License Commitments. At least the first of these 5 consecutive starts will be a fast start. This instrumentation has no protective function as defined in Section 2 of IEEE 279-1971 as applicable to this instrumentation:

1. The Diesel Generator Starting Air System instrumentation controls the operation of the system air compressors to maintain adequate air pressure to allow one fast start and five total starts of the diesel engine.
2. The variables monitored to provide the required function are air tank pressure and engine air pressure.
3. One pressure transmitter is provided on each of the two starting air tanks.

   One pressure switch is provided on each of the two starting air lines at the diesel engine.

   One pressure switch is provided on the control air header.
4. No protective function as defined in Section 2 of IEEE 279-1971 is required of this instrumentation.

7.6.14.2 Analysis

There are no specific NRC Regulatory Guides or General Design Criteria applicable to this instrumentation.

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard, and as such, are not directly applicable to this instrumentation. A discussion of the extent to which the design of this system's instrumentation meets the applicable portions of IEEE 279-1971 is provided below in compliance with the NRC Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants.

The following refers to the requirements set forth in Section 4 of IEEE 279-1971:

1. General Functional Requirements

   The Diesel Generator Starting Air System instrumentation essential to the system's required function is designed for operation under the environmental conditions specified in Section 3.8.4.
2. Single Failure Criterion

   Any failure of the Diesel Generator Starting Air System instrumentation affects only the air starting system to which it is associated, and will in no way affect the operation of the redundant diesel generator.
3. Quality of Components and Modules

   Components of the Diesel Generator Starting Air System instrumentation are of a quality consistent with 10CFR50.65, "Maintenance Rule Program".
4. Channel Integrity

The Diesel Generator Starting Air System instrumentation essential to the system safety function is designed to maintain the necessary functional capability under the environmental conditions specified in Section 3.8.4.

5. Channel Independence

   The instrumentation associated with the air starting system of one diesel generator is physically and electrically isolated from that of the redundant diesel generator.

6. Control and Protection System Interactions

   No protective function, as defined in Section 2 of IEEE 279-1971, is required of this instrumentation.

7. Derivation of System Inputs

   System inputs are derived from direct measurement of the desired variable.

8. Operating Bypasses

   There are no bypasses associated with this instrumentation.

7.6.15 Diesel Generator Lubricating Oil System

7.6.15.1 System Description

The Diesel Generator Lubricating Oil System design is discussed in Section 9.5.7.2.

Diesel engine lubricating oil temperature and pressure are monitored to provide interlock functions in the start circuit. Low-lube oil pressure will shutdown the engine in any mode of operation, while the high temperature interlock is automatically bypassed for emergency operation. (See Section 8.3). This trip requires a manual reset.

The design of the low lube oil pressure trip includes pressure switches whose contacts are arranged in the start circuit such that both devices must indicate low pressure for a trip of the diesel generator to occur. This permissive is bypassed for a sufficient time after the engine reaches full speed to allow the engine driven pump to charge the lube oil system. If, at the end of this period lube oil pressure has not reached the desired minimum value, then the diesel generator is shutdown. (See Section 8.3). This trip requires a manual reset.

Low lubricating oil pressure automatically energizes the before and after lube oil pump.

Local and OAC alarms are provided for high and low lube oil temperature and low lube oil pressure. A common alarm in the Control Room alerts the operator to these conditions in sufficient time to allow corrective action to be taken.

7.6.15.1.1 Design Basis Information

The design basis for the Diesel Generating Lubricating Oil System instrumentation is to provide control and alarms for the lubricating system to assure lubrication of the diesel engine, and to interlock the engine to prevent its operation without adequate oil pressure. This instrumentation has no protective function as defined in Section 2 of IEEE 279-1971. However, the following discussion responds to the provisions of Section 3 of IEEE 279-1971 as applicable to this instrumentation.

1. The system instrumentation provides control and alarms for the Diesel Generating Lubricating Oil System, and protection of the engine against operation without the minimum required oil pressure.

2. Lubricating oil temperature and pressure are monitored to provide the required function.
3. Three temperature switches are provided in the lube oil pump discharge header. One switch each is provided for the high and low alarm, the third provides the high temperature interlock.

   Two pressure switches, a pressure transmitter, a current alarm and a receiver gauge are provided to monitor the engine lube oil pressure. The pressure switches trip the engine on low lube oil pressure. The transmitter sends a signal to the current alarm and receiver gauge. The current alarm starts the before and after lube oil pump on low pressure. The receiver gauge provides outputs for alarms on low pressure.
4. No protective function as defined in Section 2 of IEEE 279-1971 is required of this instrumentation.

7.6.15.2 Analysis

There are no specific NRC Regulatory Guides or General Design Criteria applicable to this instrumentation.

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of that standard, and as such, are not directly applicable to this instrumentation. A discussion of the extent to which the design of this system's instrumentation meets the applicable portions of IEEE 279-1971 is provided below in compliance with the NRC Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. The following refers to the requirements set forth in Section 4 of IEEE 279-1971.

1. General Functional Requirements

   The Diesel Generator Lubricating Oil System instrumentation essential to the system's required function is designed for operation under the environmental conditions specified in Section 3.8.4.
2. Single Failure Criterion

   Any failure of the Diesel Generator Lubricating Oil System instrumentation affects only the lubricating system to which it is associated, and in no way affects the operation of the redundant diesel generator.
3. Quality of Components and Modules

   Components of the Diesel Generator Lubricating Oil System instrumentation are of a quality consistent with 10CFR50.65, "Maintenace Rule Program".
4. Channel Integrity

   The instrumentation essential to the system's required function which is associated with the Diesel Generator Lubricating Oil System is designed to maintain the necessary functional capability under the environmental conditions specified in Section 3.8.4.
5. Channel Independence

   The Diesel Generator Lubricating Oil System instrumentation associated with one diesel generator is physically and electrically isolated from that of the redundant diesel generator.
6. Control and Protection System Interaction

   No protective function, as defined in Section 2 of IEEE 279-1971, is required of this instrumentation.

7. Derivation of System Inputs

   System inputs are derived from direct measurement of the desired variable. For the low lube oil pressure trip redundant sensing devices are provided to prevent a false shutdown of the diesel generator.

8. Operating Bypasses

   There are no bypasses of protective functions, as defined in Section 4-12 of IEEE 279-1971 associated with this instrumentation.

7.6.16 Containment Pressure Control System

As described in Sections 7.3 and 7.6 the Containment Pressure Control System is provided to preclude depressurization.

The basic design criteria for these systems is that they are only initiated when required and that they be terminated when no longer required. The initiation of the safety features systems is described in Sections 7.3 and 7.6.

The permissive and termination features of the redundant Containment Pressure Control System are accomplished by eight independent pressure sensors (transmitters) (i.e., four on each train) which provide interlocks to prohibit initiation of Containment spray and automatic initiation of Containment air return fans, and terminate their operation, when Containment pressure is below approximately .35 psig. If pressure increases above 0.8 psig and the Sp signal is still present, the Containment air return fans will automatically restart. The CPCS permits Containment spray to be manually restarted, and isolation valves manually opened, once pressure increases above 0.35 psig.

This system is designed such that no single failure can prevent manual Containment spray or automatic Containment air return fan initiation nor can it allow Containment spray or Containment air return fan operation when not required.

This control system is designed in accordance with IEEE 279-1971, with one minor modification. This difference is that the .35 psig permissive termination feature is automatically reset such that under accident conditions spray, and air return fan operation is automatically terminated upon pressure decay to .35 psig, thereby, controlling Containment pressure. See Table 7-15 for single failure analysis and Figure 7-19 for control logic of the system.

7.6.17 Reactor Coolant System Overpressure Protection System for Low Pressure/Temperature, Water Solid Conditions

7.6.17.1 Description

The Reactor Coolant System Overpressure Protection System prevents the Reactor Coolant System from exceeding the pressure/temperature limits of 10CFR 50, Appendix G, for periods of water solid operation during startup and shutdown. The maximum RCS pressure is limited by providing a low pressure setpoint interlocked with reactor coolant temperature to actuate the pressurizer power operated relief valves (PORV). Refer to Section 5.2.2.3 for a description of the PORVs.

The protection provided by this system is required for periods of water solid operation during startup and shutdown. Therefore, the PORV low pressure setpoint is enabled by the operator as plant conditions dictate. A key-lock switch, located on the main control board, is provided for each train of PORVs to enable the low pressure setpoint.

A logic diagram for the Reactor Coolant System Overpressure Protection System is provided in Figure 7-20.

As RCS temperature approaches the temperature setpoint during plant cooldown but before collapse of the pressurizer steam bubble, an annunciator alerts the operator that plant conditions require low temperature overpressure protection. The operator places each key-lock switch to the LOW PRESSURE position to enable the PORV low pressure setpoint.

Should a pressure excursion occur while in the low pressure mode with plant temperature below the temperature setpoint, system pressure in excess of the PORV low pressure setpoint would be relieved to the pressurizer relief tank (refer to Section 5.2.2.1). An annunciator in the Control Room would alert the operator to system overpressure in this condition.

When system temperature rises above the temperature setpoint during plant heatup, the RCS Overpressure Protection System is automatically disarmed, and an annunciator alerts the operator that low temperature overpressure protection is no longer required. The operator then returns each key-lock switch to the NORMAL position.

The permissive signal which allows the operator to enable the PORV to respond to the low pressure setpoint and the annunciator which alerts the operator that the low pressure mode is required are derived from the RCS wide range temperature instrument. Additionally, the temperature permissive signal functions as an interlock to prevent inadvertent actuation of the PORVs during normal operation and, also, to automatically remove the low pressure setpoint when system temperature is above the low temperature setpoint.

7.6.17.1.1 Design Basis Information

The following addresses the design bases for the RCS Overpressure Protection System:

1. This system protects the Reactor Coolant System from exceeding the pressure/temperature limits of 10CFR 50, Appendix G, as defined by the Technical Specifications.
2. The variables monitored to provide protection are RCS temperature (wide range) and RCS loop pressure (narrow range).
3. The pressurizer power operated relief valves are opened on the low pressure setpoint at a pressure below the Appendix G requirements. The low pressure setpoint is functional only when plant temperature is below the low temperature setpoint.

7.6.17.2 Analysis

1. General Functional Requirements

   The overpressure protection system is enabled manually by the operator upon receipt of an alarm which indicates the approach of a condition requiring low pressure protection. Once enabled, the system operates automatically on an over pressure condition to relieve excessive pressure through the PORVs.

2. Single Failure Criterion

   No single component failure in the instrumentation for the overpressure protection system can prevent the operation of at least one train of PORVs to relieve excess pressure.

3. Quality of Components and Modules

   Components of the overpressure protection system are of a quality consistent with requirements of 10CFR50.65, "Maintenance Rule Program".

4. Channel Integrity

   The instrumentation associated with this system is designed to maintain its function integrity under the extremes of environmental conditions expected at its location in the plant.

5. Channel Independence

   Instrumentation associated with one channel of the overpressure protection system is physically and electrically separated form that of the redundant channel.

6. Control and Protection System Interaction

   No control functions are provided by this system.

7. Derivation of System Inputs

   The system inputs are derived from signals which are direct measures of the desired variables.

8. Capability for Sensor Checks

   The sensors for this system are the RCS loop pressure sensors (narrow range) and the RCS temperature sensors (wide range). Train A protection employs RCS Loop D sensors and Train B uses the Loop C sensors. The availability of a given sensor can be verified by cross-checking the sensor with the remaining narrow/wide range sensors (choose appropriate sensor) monitoring the same variable in other reactor coolant loops.

9. Capability for Test and Calibration

   For each train of the Reactor Coolant System Overpressure Protection System, the capability for testing and calibration is provided.

7.6.18 Hydrogen Mitigation System

The Hydrogen Mitigation System (Reference 4, Section 7.6.20) is designed to protect the containment structure from sudden overpressure resulting from an uncontrolled burn of the hydrogen released during a beyond design-basis degraded core accident. Under these conditions, the system would ignite and burn off low concentrations of hydrogen gas. The Hydrogen Mitigation System is non safety-related because the requirements of 10 CFR 50.44 to mitigate hydrogen generated as a result of a 75% metal-water reaction address beyond design-basis combustible gas control.

7.6.18.1 Description

7.6.18.1.1 Initiating Circuits

The Hydrogen Mitigation System is actuated manually from the main control room and receives power from motor control centers in the 600VAC essential auxiliary power system which can be aligned to the emergency diesel generators. In addition, Train A igniters receive power from a motor control center in the 600VAC essential auxiliary power system that can be aligned to the Standby Shutdown Facility (SSF) diesel generator as well as the emergency diesel generators. Train A igniters can also be actuated manually from controls remote from the main control room.

7.6.18.1.2 Logic

There is no other control logic associated with this system.

7.6.18.1.3 Bypasses

There are no bypasses associated with this system.

7.6.18.1.4 Interlocks

The Hydrogen Mitigation System is interlocked with the diesel generator load sequencer to assure that the system must be placed into service as an operator action.

7.6.18.1.5 Sequencing

Power to Hydrogen Mitigation System panelboard HMPPA is controlled using contactors in 600VAC essential motor control center EMXA-4. Power to Hydrogen Mitigation System panelboard HMPPB is controlled using contactors in 600VAC essential motor control center EMXB. Power will therefore be available to power panelboards HMPPA and HMPPB during loss of off-site power (LOOP) conditions. In the event of a safety injection (S_s) signal generated by the SSPS power panelboards HMPPA and HMPPB are load shed from the diesel backed power supply. The Hydrogen Mitigation System can be manually reloaded onto the diesel generators using control room controls. HMPPA can be manually reloaded onto the diesel generators using either control room controls or controls remote from the main control room. During station blackout (SBO) conditions, HMPPA can be manually aligned to the Standby Shutdown Facility (SSF) diesel generator via EMXA-4, and manually actuated from controls remote from the main control room.

7.6.18.1.6 Actuated Devices

All devices in the Hydrogen Mitigation System are actuated manually.

7.6.18.1.7 Supporting Systems

Hydrogen Mitigation System power panelboards HMPPA and HMPPB receive electrical power from the 600VAC Essential Auxiliary Power System which is described in 8.3.1.1.6.

7.6.18.1.8 System Design

Each igniter assembly contains a glow coil type igniter and an enclosure. There are seventy (70) igniter assemblies, which are segregated into 35 per train. Power is distributed to the group A igniters from power panelboard HMPPA and to group B from power panelboard HMPPB. The igniter assemblies, respective cabling, and power supplies are fully redundant.

Two status lights, one for each igniter group, and computer points, one for each circuit within each group, are provided in the main control room to indicate when power is being supplied to the igniter system.

7.6.18.2 Analysis

Although IEEE 279-1971 is not directly applicable to the non-class IE Hydrogen Mitigation System, the system does not meet the single failure, manual initiation and testability criteria of IEEE 279-1971. The igniter assemblies and their respective power cabling are physically and electrically separated and the igniter assemblies are seismically mounted.

7.6.19 Main Feedwater Flow Isolation on High Doghouse Water Level Instrumentation

7.6.19.1 Description

The doghouse water level instrumentation provides for the termination of forward feedwater flow in the event of a postulated pipe break in the main feedwater piping in the doghouses to prevent flooding safety-related equipment essential to the safe shutdown of the plant.

The level instrumentation consists of two independent and redundant trains of level switches which monitor level in each of the doghouses. These switches are powered from the vital instrumentation and control power system as described in Section 8.3.2.

Each doghouse contains six level switches. Three switches are assigned to each redundant train of instrumentation. One of these switches is assigned to an alarm function and also is part of the two-out-of-three trip logic. Whenever two of the three level switches sense a flooding condition, they will initiate the isolation logic described below.

The level switches provide input to the control room alarms through appropriate isolation. Control room annunciator alarms for each doghouse are activated at a 6” water level to alert the operator to a potential flooding condition. Additional confirmation of the annunciator alarms is provided by individual lights on the status light panel that display hi-level warnings for each train of level instrumentation in each doghouse.

At a 12 inch set point the following occurs:

1. Trip Main Feedwater Pump Turbines (MFWPT)
2. Close Main Feedwater Pump Discharge Valve for each Pump
3. Close the S/G Tempering Header Isolation Valve

The following devices will close to isolate feedwater flow to the affected doghouse.

1. S/G Feedwater Flow Control Valves
2. S/G Feedwater Flow Control Bypass Valves
3. S/G Main Feedwater Containment Isolation Valves
4. S/G Main Feedwater Containment Isolation Valves Bypass Valves
5. S/G Main Feedwater to Auxiliary Feedwater Nozzle Isolation Valves
6. S/G Tempering Flow to Auxiliary Feedwater Nozzle Valves

7.6.19.2 Design Bases

The doghouse water level switches and controls are designed to ensure proper response to a postulated pipe break in a doghouse and availability of safety related equipment located in these areas.

7.6.19.3 Analysis

The requirements of IEEE 279-1971 are written for protection systems as defined in Section 1 of the standard; therefore, these requirements are not directly applicable to these controls. However, a discussion of the extent to which the design of this system meets the appropriate portions of IEEE 279, Section 4, is provided below:

7.6.19.3.1 General Function Requirements

The instrumentation and controls associated with doghouse water level are designed with reliability and redundancy to automatically initiate their safety function.

7.6.19.3.2 Single Failure Criterion

The doghouse water level instrumentation and controls are designed such that no single failure can prevent the safety function from being performed.

7.6.19.3.3 Quality of Components and Modules

The quality assurance program under which the components of this system are qualified is described in Chapter 17. This program includes appropriate requirements for design review, procurement, inspection, and testing to ensure that system components are of a quality consistent with minimum maintenance requirements and low failure rates.

7.6.19.3.4 Equipment Qualification

Qualification of electrical equipment is discussed in Sections 3.10 and 3.11.

7.6.19.3.5 Channel Integrity

The redundant trains of the safety related instrumentation and controls associated with doghouse water level monitoring are designed to maintain their functional capability.

7.6.19.3.6 Channel Independence

The safety-related instrumentation and controls associated with doghouse water level monitoring are physically separated and electrically isolated as discussed in Section 8.3.1.2.

7.6.19.3.7 Control and Protection System Interaction

The safety-related instrumentation and controls for doghouse water level monitoring are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.19.3.8 Derivation of System Inputs

System inputs are derived from direct measurement of the defined variables.

7.6.19.3.9 Capability for Test, Calibration, and Sensor Checks

The safety-related instrumentation and controls are designed to facilitate testing and calibration as required by the Technical Specifications.

7.6.19.3.10 Channel Bypass or Removal From Operation

The safety-related instrumentation and controls associated with doghouse water level are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.19.3.11 Operating Bypasses

The doghouse water level instrumentation and controls do not employ operating bypasses in their initiating logic.

7.6.19.3.12 Indication of Bypass

The doghouse water level instrumentation has no designed bypass capability and therefore no indication of a bypass is provided.

7.6.19.3.13 Access to Means for Bypassing

Access to the controls and equipment that could be manipulated to make the doghouse water level instrumentation inoperable is controlled by administrative and security measures.

7.6.19.3.14 Multiple Setpoints

Annunciator alarms are initiated at the 6 inch water level in the doghouse while trip outputs are initiated by the 12 inch setpoint.

7.6.19.3.15 Completion of Protective Action Once it is Initiated

Once initiated the doghouse water level instrumentation and controls continue to perform their safety function until the condition requiring its operation has been eliminated.

7.6.19.3.16 Manual Initiation

There is no system level manual initiation associated with doghouse water level monitoring.

7.6.19.3.17 Access to Setpoint Adjustments, Calibration, and Test Points

Access to setpoint adjustments, calibration, and test points for the safety-related instrumentation and controls associated with doghouse level monitoring are controlled by administrative and security measures.

7.6.19.3.18 Identification of Protective Action

The safety-related instrumentation and controls associated with doghouse level monitoring are train related and do not include protection channels as defined in IEEE 279-1971.

7.6.19.3.19 Information Read-Out

Information read-outs are provided in the control room to allow confirmation of system safety functions.

7.6.19.3.20 System Repair

The doghouse water level instrumentation and controls are designed to facilitate the replacement, repair, or adjustment of malfunctioning instruments and controls.

7.6.19.3.21 Identification

The safety-related instrumentation and control equipment associated with doghouse level monitoring is physically identified as described in Section 7.1.2 for non-rack mounted equipment.

7.6.20 References

1. The Institute of Electrical and Electronic Engineers, Inc., IEEE Standard: “IEEE Standard Criteria for Class 1E Power Systems for Nuclear Generating Stations,” IEEE-STD 308-1971.
2. The Institute of Electrical and Electronic Engineers, Inc., IEEE Standard: “Criteria for Protection Systems for Nuclear Power Generating Stations,” IEEE Standard 279-1971.

3. The Institute of Electrical and Electronic Engineers, Inc., IEEE “Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems,” IEEE Standard 338-1971.
4. An Analysis of Hydrogen Control Measures at McGuire Nuclear Station - Duke Power Company, October, 1981.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.6.

7.7 Control Systems Not Required for Safety

The general design objectives of the unit control systems are:

1. To establish and maintain power equilibrium between primary and secondary system during steady state unit operation;
2. To constrain operational transients so as to preclude unit trip and re-establish steady state unit operation;
3. To provide the reactor operator with monitoring instrumentation that indicates all required input and output control parameters of the systems and provides the operator the capability of assuming manual control of the system.

7.7.1 Description

The unit control systems described in this section perform the following functions:

1. Reactor Control System
   a. Enables the nuclear unit to accept a step load increase or decrease of 10 percent and a ramp increase or decrease of 5 percent per minute within the load range of 15 percent to 100 percent without reactor trip, steam dump, or pressurizer relief actuation, subject to possible xenon limitations.
   b. Maintains reactor coolant average temperature T_{avg} within prescribed limits by creating the bank demand signals for moving groups of full length rod cluster control assemblies during normal operation and operational transients. The T_{avg} control also supplies a signal to pressurizer water level control, and steam dump control.
2. Rod Control System
   a. Provides for reactor power modulation by manual or automatic control of full length control rod banks in a preselected sequence and for manual operation of individual banks.
   b. Systems for Monitoring and Indicating

      Provide alarms to alert the operator if the required core reactivity shutdown margin is not available due to excessive control rod insertion.

      Display control rod position.

      Provide alarms to alert the operator in the event of control rod deviation exceeding a preset limit.
3. Unit Control System Interlocks
   a. Prevent further withdrawal of the control banks when signal limits are approached that predict the approach of a DNBR limit or kw/ft limit.
   b. Inhibit automatic turbine load change as required by the Nuclear Steam Supply System.
4. Pressurizer Pressure Control
   a. Maintains or restores the pressurizer pressure to the design pressure ±35 psi (which is well within reactor trip and relief and safety valve actuation setpoint limits) following normal operational transients that induce pressure changes by control (manual or

automatic) of heaters and spray in the pressurizer. Provides steam relief by controlling the power relief valves.

5. Pressurizer Water Level Control

   a. Establishes, maintains, and restores pressurizer water level within specified limits as a function of the average coolant temperature. Changes in level are caused by coolant density changed induced by loading, operational, and unloading transients. Level changes are produced by means of charging flow control (manual or automatic) as well as by manual selection of letdown orifices. Maintaining coolant level in the pressurizer within prescribed limits by actuating the charging and letdown system thus provides control of the reactor coolant water inventory.

6. Steam Generator Water Level Control

   a. Establishes and maintains the steam generator water level to within predetermined limits during normal operating transients.

   b. The Steam Generator Water Level Control System also restores the steam generator water level to within predetermined limits at unit trip conditions. It regulates the feedwater flow rate such that under operational transients the heat sink for the Reactor Coolant System does not decrease below a minimum. Steam generator water inventory control is manual or automatic through the use of feedwater control valves.

7. Steam Dump Control

   a. Permits the nuclear unit to accept a sudden loss of load less than 50% without incurring reactor trip. Steam is dumped to the condenser as necessary to accommodate excess power generation in the reactor during turbine load reduction transients.

   b. Insures that stored energy and residual heat are removed following a reactor trip to bring the unit to equilibrium no load conditions without actuation of the steam generator safety valves.

   c. Maintains the unit at no load conditions and permits a manually controlled cooldown of the unit.

8. In-Core Instrumentation

   Provides information on the neutron flux distribution and on the core outlet temperatures at selected core locations.

7.7.1.1 Reactor Control System

The Reactor Control System enables the nuclear unit to follow load changes automatically. The system is designed to accept step load changes of 10 percent and ramp changes of 5 percent per minute within the load range of 15 percent to 100 percent without a reactor trip, steam dump, or pressure relief. Depending on core life and power level, controllability may be subject to xenon limitations. The system is also capable of restoring reactor coolant average temperature to within the programmed temperature control deadband following a change in reactor load. Manual control rod operation may be performed at any time.

The primary inputs used for the reactor control system are derived as follows:

- **Reactor Power** - Validated input (typically second highest) from four nuclear instrumentation power range channels.

- **Reactor Coolant Average Temperature (Tavg)** - Validated input (typically second highest) from four inputs (one per reactor coolant loop) received from the W7300 protection cabinets.
- **Turbine Inlet Pressure** - Two input channels, one received from W7300 protection cabinets and one received directly from a pressure transmitter, are averaged to produce **turbine power** and reference average reactor coolant temperature **(Tref)**.

Turbine inlet pressure increases linearly as turbine power increases from 0 to 100% and it can be scaled and compared directly with reactor power. Similarly, Tavg also increases linearly as reactor power increases from 0 to 100%. The reactor control system compares Reactor power, Tavg, and scaled turbine inlet pressure and their differences are used to produce a control signal to reposition control rods and restore primary and secondary power equilibrium. The power mismatch signal is obtained by comparing reactor power and turbine power and applying a derivative function to the difference for anticipatory transient response. A variable gain that increases system response at lower power levels is also applied. A lead-lag function is applied to Tavg and it is compared to Tref to obtain the temperature mismatch signal. The power mismatch and temperature mismatch signals are summed and used to drive rod speed demand, and insertion and withdrawal commands to the rod control system.

The core axial power distribution is controled during load following maneuvers by manually changing the boron concentration in the reactor coolant system. The control board $\Delta\varphi$ displays (Section 7.7.1.3.1) indicate the need for an adjustment in the axial power distribution. Adding boron to the reactor coolant will reduce Tavg and cause the rods to be withdrawn. This action will reduce power peaks in the bottom of the core. Likewise, removing boron from the reactor coolant will increase Tavg and cause the rods to be inserted into the core to control power peaks in the top of the core.

7.7.1.2 Rod Control System

7.7.1.2.1 Full Length Rod Control System

The full length Rod Control System receives rod speed and direction signals from the T_{avg} control system. The rod speed demand signal varies over the corresponding range of 3.75 to 45 inches per minute (6 to 72 steps/minute) depending on the magnitude of the input signal. The rod direction demand signal is determined by the positive or negative value of the input signal. Manual control is provided to move a control bank in or out at a prescribed fixed speed.

When the turbine load reaches approximately 15 percent of rated load, the operator may select the AUTOMATIC mode, and rod motion is then controlled by the Reactor Control System. A permissive interlock C-5 (See Table 7-18) derived from measurements of turbine inlet pressure prevents automatic control when the turbine load is below 15 percent. In the AUTOMATIC mode, the rods are again withdrawn (or inserted) in a predetermined programmed sequence by the automatic programming equipment. The manual and automatic controls are further interlocked with the control interlocks (See Table 7-18).

The shutdown banks are moved to the fully withdrawn position at a constant speed by manual control prior to criticality. During normal operations the shutdown banks are kept in the fully withdrawn position, except during the rod movement surveillance required by Technical Specifications. A reactor trip signal causes them to fall by gravity into the core. There are five shutdown banks.

The control banks are the only rods that can be manipulated under automatic control. Each control bank is divided into two groups to obtain smaller incremental reactivity changes per step.

All rod cluster control assemblies in a group are electrically paralleled to move simultaneously. There is individual position indication for each rod cluster control assembly.

Power to rod drive mechanisms is supplied by two motor generator sets operating from two separate 575 volt, three-phase buses. Each generator is the synchronous type and is driven by a 150 hp induction motor. The AC power is distributed to the rod control power cabinets through the two series connected reactor trip breakers.

The variable speed rod drive programmer affords the ability to insert small amounts of reactivity at low speed to accomplish fine control of reactor coolant average temperature about a small temperature deadband, as well as furnishing control at high speed. A summary of the rod cluster control assembly sequencing characteristics is given below.

1. Two groups within the same bank are stepped such that the relative position of the groups does not differ by more than one step.
2. The control banks are programmed such that withdrawal of the banks is sequenced in the following order: control bank A, control bank B, control bank C, and control bank D. The programmed insertion sequence is the opposite of the withdrawal sequence, i.e., the last control bank withdrawn (bank D) is the first control bank inserted.
3. The control bank withdrawals are programmed such that when the first bank reaches a preset position, the second bank begins to move out simultaneously with the first bank. When the first bank reaches its full out position, it stops, while the second bank continues to move toward its fully withdrawn position. When the second bank reaches a preset position, the third bank begins to move out, and so on. This withdrawal sequence continues until the unit reaches the desired power level. The control bank insertion sequence is the opposite.
4. Overlap between successive control banks is adjustable between 0 to 150 steps, with an accuracy of ±1 step.
5. Rod speeds for either shutdown banks or control banks are capable of being controlled between a minimum of 6 steps per minute and a maximum of 72 steps per minute.

7.7.1.3 Unit Control Signals for Monitoring and Indicating

7.7.1.3.1 Monitoring Functions Provided by the Nuclear Instrumentation System

A comprehensive discussion of the Nuclear Instrumentation System power ranges is described in Reference 1. The Neutron Flux Monitoring System (NFMS) is described in Reference 5. The Wide Range Neutron Flux monitoring system and shutdown monitor is described in Reference 9.

The power range channels are important because of their use in monitoring power distribution in the core within specified safe limits. They are used to measure power level, axial power imbalance, and radial power imbalance. These channels are capable of recording overpower excursions up to 200 percent of full power. Suitable alarms are derived from these signals as described below.

Basic power range signals are:

1. Total current from a power range detector (four such signals from separate detectors); these detectors are vertical and have an active length of 10 feet.
2. Current from the upper half of each power range detector (four such signals).
3. Current from the lower half of each power range detector (four such signals).

Derived from these basic signals are the following (including standard signal processing for calibration):

1. Indicated neutron flux (four such).
2. Indicated axial flux imbalance, derived from upper half flux minus lower half flux (four such).

Alarm functions derived are as follows:

1. Deviation (maximum minus minimum of four) in indicated nuclear power.
2. Upper radial tilt (maximum to average of four) on upper-half currents.
3. Lower radial tilt (maximum to average of four) on lower-half currents.

Provision is made to continuously record, on strip charts on the control board, the 8 ion chamber signals, i.e., upper and lower currents for each detector. Indicators are provided on the control board for nuclear power and for axial power imbalance.

The source range channels are used to monitor core neutron levels and provide indication of reactivity changes that may occur as a result of events such as boron dilution. Nuclear SR/IR Neutron Flux Monitoring System (NFMS) channels (N31/N35 and N32/N36) provide a high flux at shutdown alarm that actuates containment evacuation alarm, and an audible counting indication in the control room and upper containment.

The wide range neutron flux monitoring channels (Gamma-metrics N51/N52) supplement the NFMS function, and perform the post-accident neutron flux monitoring function described in Chapter 1. There are two trains of wide range neutron flux monitoring channels each with a shutdown monitor installed on the main control board. One train is also displayed on the Auxiliary Shutdown Panel and in the Standby Shutdown Facility. The wide range neutron flux monitoring system's shutdown monitor provides an indication of neutron count rate and a high flux at shutdown alarm in the control room. The wide range neutron flux monitoring system's shutdown monitor provides a visual alarm indication and an audible alarm via the plant annunciator system that is routed through an adjacent alarm bypass switch. The wide range neutron flux monitoring system's shutdown monitor high flux at shutdown alarm does not actuate an automatic containment evacuation alarm or provide audible counting indication.

Deleted per 2015 update

7.7.1.3.2 Control Rod Drive Position Indication System

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

1. Digital Rod Position Indication System

   The digital rod position indication system is described in Reference 4. It measures the actual position of each full length rod using a detector which consists of 42 discrete coils mounted concentric with the rod drive pressure housing. The coils are located axially along the pressure housing on 3.75 inch spacing. They magnetically sense the entry and presence of the rod drive shaft through its center line. The coils are interlaced into two data channels, and are connected to the Containment electronics (Data A and B) by separate multi-conductor cables. Multiplexing is used to transmit the digital position signals from the Containment electronics to the digital rod position indication cabinet. The digital position signal is displayed on the main control board for each full length control rod. By employing two separate channels of information, the digital rod position indication system can continue to function (at reduced accuracy) when one channel fails.

Included in the system is a rod at bottom signal that operates a local alarm and a Control Room annunciator.

2. Demand Position Indication System

   The demand position indication system counts pulses generated in the Rod Control System to provide a digital readout of the demanded bank position.

The demand position and digital rod position indication systems are separate systems; each serves as backup for the other. Operating procedures require the reactor operator to compare the demand and actual reading from the rod position indicating system so as to verify proper operation of the rod control system.

7.7.1.3.3 Control Bank Rod Insertion Monitoring

When the reactor is critical, the normal indication of reactivity status in the core is the position of the control bank in relation to reactor power (as indicated by the Reactor Coolant System loop ΔT and coolant average temperature. These parameters are used to calculate insertion limits for the control banks. Two alarms are provided for each control bank.

1. The “low” alarm alerts the operator of an approach to the rod insertion limits requiring boron addition by following normal procedures with the Chemical and Volume Control System.
2. The “low-low” alarm alerts the operator to verify shutdown margin and to take action to return control rods above the insertion limits such as adding boron to the Ractor Coolant System by any one of several alternate methods.

The purpose of the control bank rod insertion monitor is to give warning to the operator of excessive rod insertion. The insertion limit maintains sufficient core reactivity shutdown margin following reactor trip and provides a limit on the maximum inserted rod worth in the unlikely event of a hypothetical rod ejection, and limits rod insertion such that acceptable nuclear peaking factors are maintained. Since the amount of shutdown reactivity required for the design shutdown margin following a reactor trip increases with increasing power, the allowable rod insertion limits must be decreased (the rods must be withdrawn further) with increasing power. Two parameters which are proportional to power are used as inputs to the insertion monitor. These are the ΔT between the hot leg and the cold leg, which is a direct function of reactor power, and T_{avg}, which is programmed as a function of power. The rod insertion monitor uses these parameters for each control rod bank as follows:

$$Z_{LL} = K_1(\Delta T)_{auct} + K_2(T_{avg})_{auct} + K_3$$

Note: The above equation was revised in OCT 1999 update.

where

Z_{LL} = Maximum permissible insertion limit for affected control bank

$(\Delta T)_{auct}$ = Highest ΔT of all loops

$(T_{avg})_{auct}$ = Highest T_{avg} of all loops (not used since $K_2 = 0$ at McGuire)

K_1, K_2, K_3 = Constants chosen to maintain $Z_{LL} \geq$ actual limit based on physics calculations

The control rod bank demand position (Z) is compared to Z_{LL} as follows:

If $Z - Z_{LL} \leq K_4$ a low alarm is actuated.

If $Z - Z_{LL} \leq K_5$ a low-low alarm is actuated.

Since the highest values of T_{avg} and ΔT are chosen by auctioneering, a conservatively high representation of power is used in the insertion limit calculation.

Actuation of the low alarm alerts the operator of an approach to a reduced shutdown reactivity situation. Administrative procedures require the operator to add boron through the Chemical and Volume Control System unless the condition is due to a Unit runback. Actuation of the low-low alarm requires the operator to initiate emergency boration procedures unless the condition is due to a Unit runback. For a Unit runback, shutdown margin is calculated and the control rods are returned above the insertion limits. The value of K_5 is chosen such that the low-low alarm is normally actuated before the insertion limit is reached. The value of the K_4 is chosen to allow the operator to follow normal boration procedures. Figure 7-32 shows a block diagram representation of the control rod bank insertion monitor. In addition to the rod insertion monitor for the control banks, the unit computer, which monitors individual rod positions, provides an alarm system that is associated with the rod deviation alarm discussed below (Section 7.7.1.3.4) to warn the operator if any shutdown rod cluster control assembly leaves the fully withdrawn position.

Rod insertion limits are established by:

1. Establishing the allowed rod reactivity insertion at full power consistent with the purposes given above.
2. Establishing the differential reactivity worth of the control rods when moved in normal sequence.
3. Established the change in reactivity with power level by relating power level to rod position.
4. Linearizing the resultant limit curve. All key nuclear parameters in this procedure are measured as part of the initial and periodic physics testing program.

Any unexpected change in the position of the control bank under automatic control, or a change in coolant temperature under manual control, provides a direct and immediate indication of a change in the reactivity status of the reactor. In addition, samples are taken periodically of coolant boron concentration. Variations in concentration during core life provide an additional check on the reactivity status of the reactor, including core depletion.

7.7.1.3.4 Rod Deviation Alarm

The demanded and measured rod position signals are displayed on the control board. They are also monitored by the unit computer which provides a visual printout and an audible alarm whenever an individual rod position signal deviates from the other rods in the bank by a preset limit. The alarm can be set with appropriate allowance for instrument error and within sufficiently narrow limits to preclude exceeding core design hot channel factors.

Figure 7-30 is a block diagram of the rod deviation comparator and Alarm System.

7.7.1.3.5 Rod Bottom Alarm

A rod bottom signal for the full length rods bistable in the Digital Rod Position System as described in Reference 6, is used to operate a control relay, which generates the ROD BOTTOM ROD DROP alarm.

7.7.1.4 Unit Control System Interlocks

The listing of the unit control system interlocks, along with the description of their derivations and functions, is presented in Table 7-18. It is noted that the designation numbers for these interlocks are preceded by "C.". The development of these logic functions is shown in the functional diagrams (Figure 7-1, Sheets 11 to 16, Figure 7-32 and Figure 7-33).

7.7.1.4.1 Rod Stops

Rod stops are provided to prevent abnormal power conditions which could result from excessive control rod withdrawal initiated by either a control system malfunction or operator violation of administrative procedures.

The C1, C2, C3, C4, and C5 control interlocks identified in Table 7-18 are rod stops. The C3 rod stop derived from overtemperature ΔT and the C4 rod stop, derived from overpower ΔT are also used for turbine runback, which is discussed below:

7.7.1.4.2 Automatic Turbine Load Runback

Automatic turbine load runback is initiated by an approach to an overpower or overtemperature condition. This prevents high power operation that might lead to an undesirable condition, which, if reached, is protected by reactor trip.

Turbine load reference reduction is initiated by either an overtemperature or overpower ΔT signal. Two-out-of-four coincidence logic is used.

A rod stop and turbine runback are initiated when

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

for both the overtemperature and the overpower condition.

For either condition in general

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

where

B_p = a setpoint bias

where ΔT setpoint refers to the overtemperature ΔT reactor trip value and the overpower ΔT reactor trip value for the two conditions.

The turbine runback is continued until ΔT is equal to or less than $\Delta T_{rod\ stop}$. This function serves to maintain an essentially constant margin to trip.

7.7.1.5 Pressurizer Pressure Control

The Reactor Coolant System pressure is controlled by using either the heaters (in the water region) or the spray (in the steam region) of the pressurizer plus steam relief for large transients. The electrical immersion heaters are located near the bottom of the pressurizer. A portion of the heater group is proportionally controlled to correct for small pressure variations. These variations are due to heat losses, including heat losses due to a small continuous spray. The remaining (backup) heaters are turned on when the pressurizer pressure controlled signal demands approximately 100 percent proportional heater power.

The spray nozzles are located on the top of the pressurizer. Spray is initiated when the pressure controller spray demand signal is above a given setpoint. The spray rate increases proportionally with increasing spray demand signal until it reaches a maximum value.

Steam condensed by the spray reduces the pressurizer pressure. A small continuous spray is normally maintained to reduce thermal stresses and thermal shock and to help maintain uniform water chemistry and temperature in the pressurizer.

Power relief valves limit system pressure for large positive pressure transients. In the event of a large load reduction, not exceeding the design unit load rejection capability, the pressurizer power operated relief valves might be actuated for the most adverse conditions, e.g., the most negative Doppler coefficient, and the minimum incremental rod worth. The relief capacity of the power operated relief valves is sized large enough to limit the system pressure to prevent actuation of high pressure reactor trip for the above condition provided the rod controls are set for automatic operation and the steam dump system operates properly. The power relief valves also limit system pressure during cold start-up to avoid exceeding reactor vessel stress limits, by opening the valves when the reactor coolant system pressure exceeds setpoint limit and the system temperature setpoint is below the vessel nilductility temperature limit.

A diagram of the pressurizer pressure control system is shown on Figure 7-34.

7.7.1.6 Pressurizer Water Level Control

The pressurizer operates by maintaining a steam cushion over the reactor coolant. As the density of the reactor coolant adjusts to the various temperatures, the steam water interface moves to absorb the variations with relatively small pressure disturbances.

The water inventory in the Reactor Coolant System is maintained by the Chemical and Volume Control System. During normal plant operation, the charging flow varies to produce the flow demanded by the pressurizer water level controller. The pressurizer water level is programmed as a function of coolant average temperature, with the highest average temperature (auctioneered) being used. The pressurizer water level decreases as the load is reduced from full load. This is a result of coolant contraction following programmed coolant temperature reduction from full power to low power. The programmed level is designed to match as nearly as possible the level changes resulting from the coolant temperature changes.

To control pressurizer water level during startup and shutdown operations, the charging flow is manually regulated from the main Control Room.

A diagram of the pressurizer water level control system is shown on Figure 7-34.

7.7.1.7 Steam Generator Water Level Control

For each steam generator, narrow range level is maintained at programmed level by regulating feedwater control valve position and main feedwater pump speed. There is one main feedwater control valve and one bypass feedwater control valve arranged in a parallel configuration for each steam generator loop. The bypass feedwater control valves are used during lower power operations with the larger main feedwater control valves closed for finer control at lower flow conditions. As feedwater flow increases and steam flow increases above approximately 30%, control is switched to the main feedwater control valves. The feedwater flow demand values calculated for each steam generator loop are used to drive feedwater control valve postion demands. Speed demand to the two main feedwater pumps is determined by the highest steam generator loop feedwater flow demand. The primary inputs used for steam generator level control are derived as follows.

- Programmed reference level - Calculated based on the validated input (typically second highest) from four nuclear instrumentation power range channels.
- Narrow range steam generator level - Validated input (typically second highest) from four channels for each steam generator received from the W7300 protection cabinets.
- Wide range steam generator level - One channel per steam generator received from the W7300 protection cabinets.
- Feedwater flow - Median value of three channels for each steam generator.
- Steam flow - Arbritrated value from two channels for each steam generator. Under normal conditions, the arbitrated value is the average of the two channels. If the deviation between the two channels exceeds a pre-set value, an arbitrator (calculated from second highest of four reactor coolant loop normalized delta-T) is used to determine the appropriate channel.
- Reactor coolant loop normalized delta-T - Validated input (typically second highest) from four inputs (one per reactor coolant loop) received from the W7300 protection cabinets. Used an arbitrator for steam flow.
- Steam geneator pressure - Median value of three channels for each steam generator received from the W7300 protection cabinets. Used for steam flow compensation.
- Feedwater tempeature - Validated input (typically second highest) from four inputs (one per steam generator loop).

Two steam generator level control algorithms are used - one for lower power operation (less than approximately 15% power, based on feedwater flow) and one for high power operation (greater than approximately 15% power). For the low power control mode, narrow range steam generator level is compared with the programmed reference level to provide an input to a proportional plus integral controller. The deviation of wide range steam generator level from its normal operating value is used as an anticipatory feed-forward signal that is added to the output of the low power controller to produce a feedwater flow demand for each steam generator loop. Controller gain and reset time constant values are adjusted based on feedwater temperature to accommodate changes in steam generator shrink and swell characteristics during low power operation. During high power mode control, again, narrow range steam generator level is compared with the programmed reference level to produce a level mismatch signal that serves as the primary input to a proportional plus integral controller. Feedwater temperature isused to scale the level mismatch signal. Feedwater flow is subtracted from steam flow to produce a steam flow feedwater flow mismatch signal. After applying a rate-lag function to the steam flow feedwater flow mismatch signal, it is added to the level mismatch value and applied to the high power controller input to enhance anticipatory response. The high power controller output provides a feedwater flow demand for each steam generator loop.

The highest loop feedwater flow demand value, during both low and high power control modes, is used to develop the speed demands for two turbine-driven main feedwater pumps. These speed demand values are characterized to provide optimum feedwater control valve positions at all power levels. The two main feedeater pump control loops have five speed probe inputs which are used to determine actual feedwater pump speed. Actual feedwater pump speed is compared to speed demand to determine feedwater pump turbine governor valve demands. Each feedwater pump turbine has a high pressure governor valve and a low pressure governor valve both of which are positioned using motor-driven actuators. Hydraulically controlled stop valves are used to cut off governor valve steam supplies to provide over-speed and other feedwater pump trip functions. When a feedwater pump trip condition occurs, the control system will automatically close the governor valves. An interlock is provided to prevent theses

stop valves from being opened unless both governor valves are closed. Upon a reactor trip, the feedwater pump speed demand is automatically rolled back to a low set point to prevent excessive feedwater conditions.

A diagram of the steam generator water level control system is shown in Figure 7-35. A diagram of main feedwater pump speed control system is shown in Figure 7-35.

7.7.1.8 Steam Dump Control

The steam dump system is designed to accept a 50 percent loss of net load without tripping the reactor provided the rod controls are set for automatic operation.

The automatic steam dump system is able to accommodate this abnormal load rejection and to reduce the effects of the transient imposed upon the Reactor Coolant System. By bypassing main steam directly to the condenser, an artificial load is thereby maintained on the primary system. The Rod Control System can then reduce the reactor temperature to a new equilibrium value without causing overtemperature and/or overpressure conditions.

The four isolated (one per loop) Tavg input signals from protection are the same as that used in the Reactor Coolant System.

If the difference between the reference T_{avg} (T_{ref}) based on turbine inlet pressure and the lead/lag compensated 2nd highest T_{avg} exceeds a predetermined amount, and the interlock mentioned below is satisfied, a demand signal actuates the steam dump to maintain the Reactor Coolant System temperature within control range until a new equilibrium condition is reached.

To prevent actuation of steam dump on small load perturbations, an independent load rejection sensing circuit is provided. This circuit senses the rate of decrease in the turbine load as detected by the turbine inlet pressure. It is provided to unblock the dump valves when the rate of load rejection exceeds a preset value corresponding to a 10 percent step load decrease or a sustained ramp load decrease of 5 percent/minute.

A diagram of the steam dump control system is shown on Figure 7-33.

7.7.1.8.1 Load Rejection Steam Dump Controller

This circuit prevents large increases in reactor coolant temperature following a large, sudden load decrease or a turbine trip without a reactor trip. The error signal is a difference between the lead/lag compensated 2nd highest T_{avg} and the reference T_{avg} is based on turbine inlet pressure.

The lead/lag compensation for the 2nd highest T_{avg} signal is to compensate for lags in the plant thermal response and in valve positioning. Following a sudden load decrease, T_{ref} is immediately decreased and T_{avg} tends to increase, thus generating an immediate demand signal for steam dump. Since control rods are available, in this situation steam dump terminates as the error comes within the maneuvering capability of the control rods.

7.7.1.8.2 Plant Trip Steam Dump Controller

Following a reactor trip, the load rejection steam dump controller is defeated and the plant trip steam dump controller becomes active. Since control rods are not available in this situation, the demand signal is the error signal between the lead/lag compensated 2nd highest T_{avg} and the no load reference T_{avg}. When the error signal exceeds a predetermined setpoint, the dump valves are tripped open in a prescribed sequence. As the error signal reduces in magnitude indicating that the Reactor Coolant System T_{avg} is being reduced toward the reference no-load value, the

dump valves are modulated by the plant trip controller to regulate the rate of removal decay heat and thus gradually establish the equilibrium hot shutdown condition.

Following a reactor trip, the steam dump capacity requirement is only that necessary to maintain steam pressure below the steam generator relief valve setpoint (≅40 percent capacity to the condenser); therefore, only the first two groups of valves are opened. The error signal determines whether a group is to be tripped open or modulated open. In either case, they are modulated when the error is below the trip-open setpoints.

7.7.1.8.3 Steam Pressure Controller

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

The steam pressure controller utilizes the selected steam pressure signal. The selected steam pressure signal is the 2nd highest of the loop steam pressures or in the case of multiple input signal failures, steam header pressure.

7.7.1.9 In-Core Instrumentation

The In-Core Instrumentation System consists of Chromel-Alumel thermocouples at fixed core outlet positions, movable miniature neutron detectors used by the flux mapping system which can be positioned at the center of selected fuel assemblies, anywhere along the length of the fuel assembly vertical axis. The basic system for insertion of these detectors is shown in Figure 7-27. Sections 1 and 2 of Reference 3 outline the In-Core Instrumentation System in more detail.

7.7.1.9.1 Thermocouples

Chromel-Alumel thermocouples are inserted into guide tubes that penetrate the reactor vessel head through seal assemblies, and terminate at the exit flow end of the fuel assemblies. The thermocouples are provided with two primary seals, a conoseal and swage type seal from conduit to head. The thermocouples are supported in guide tubes in the upper core support assembly. Thermocouple readings are monitored by the computer with backup readout provided by a precision indicator with manual point selection located in the Control Room. Information from the in-core instrumentation is available even if the computer is not in service.

7.7.1.9.2 Movable Neutron Flux Detector Drive System

Miniature fission chamber detectors can be remotely positioned in retractable guide thimbles to provide flux mapping of the core. See Reference 3 for neutron flux detector parameters. The stainless steel detector shell is welded to the leading end of helical wrap drive cable and to stainless steel sheathed coaxial cable. The retractable thimbles, into which the miniature detectors are driven, are pushed into the reactor core through conduits which extend from the bottom of the reactor vessel down through the concrete shield area and then up to a thimble seal table.

The thimbles are closed at the leading ends, are dry inside, and serve as the pressure barrier between the reactor water pressure and the atmosphere. Mechanical seals between the retractable thimbles and the conduits are provided at the seal table. During reactor operation, the retractable thimbles are stationary. They are extracted downward from the core during

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

The drive system for the insertion of the miniature detectors consists basically of drive assemblies, five path rotary transfer assemblies, and ten path rotary transfer assemblies, as shown in Figure 7-27. These assemblies are described in Reference 3. The Drive System pushes hollow helical wrap drive cables into the core with the miniature detectors attached to the leading ends of the cables and small diameter sheathed coaxial cables threaded through the hollow centers back to the ends of the drive cables. Each drive assembly consists of a gear motor which pushes a helical wrap drive cable and a detector through a selective thimble path by means of a special drive box and includes a storage device that accommodates the total drive cable length.

The leakage detection and gas purge provisions are discussed in Reference 3.

Manual isolation valves (one for each thimble) are provided for closing the thimbles. When closed, the valve forms a 2500 psig barrier. The manual isolation valves are not designed to isolate a thimble while a detector/drive cable is inserted into the thimble. The detector/drive cable must be retracted to a position above the isolation valve prior to closing the valve.

A small leak would probably not prevent access to the isolation valves and thus a leaking thimble could be isolated during a hot shutdown.

A large leak might require cold shutdown for access to the isolation valve.

7.7.1.9.3 Control and Readout Description

The control and readout system provides means for inserting the miniature neutron detectors into the reactor core and withdrawing the detectors while plotting neutron flux versus detector position. The control system consists of two sections, one physically mounted with the drive units, and the other contained in the Control Room. Limit switches in each transfer device provide feedback of path selection operation. Each gear box drives an encoder for position feedback. One five path operation selector is provided for each drive unit to insert the detector in one of five functional modes of operation. A ten path rotary transfer assembly is a transfer device that is used to route a detector into any one of up to ten selectable paths. A common path is provided to permit cross calibration of the detectors.

The Control Room contains the necessary equipment for control, position indication, and flux recording for each detector. Additional panels are provided for such features as drive motor controls, core path selector switches, plotting and gain controls.

Flux mapping is accomplished by selecting (by panel switches) flux thimbles in given fuel assemblies at various core quadrant locations. The detectors are driven to the top of the core and stopped automatically. An X-Y plot (position versus flux level) is initiated with the slow withdrawal of the detectors through the core from the top to a point below the bottom of the core. In a similar manner other core locations are selected and plotted. Each detector provides axial flux distribution data along the center of the selected fuel assembly.

Various radial positions of the detectors are then compared to obtain a flux map for a region of the core.

The thimbles are distributed nearly uniformly over the core with approximately the same number of thimbles in each quadrant. The number and location of these thimbles have been chosen to permit measurement of local to average peaking factors to an accuracy of ±5 percent (95 percent confidence). Measured nuclear peaking factors are increased by 5 percent to allow for

this accuracy. If the measured power peaking is larger than acceptable, reduced power capability is indicated.

Operating experience has demonstrated the adequacy of the in-core instrumentation in meeting the design bases stated.

7.7.1.10 Gross Failed Fuel Detection

Gross fuel cladding failures are detected by a sodium iodide scintillation detector continuously monitoring gross gamma activity in the Reactor Coolant System. The design of this monitor is evaluated for satisfactory ability to detect fission products from ruptured fuel cladding in the presence of the design maximum primary coolant activity.

7.7.1.11 NSS Design Differences

See Section 7.1.1.1.

7.7.1.12 Loose Parts Monitoring Systems

A loose Parts Monitoring System is installed on each of the McGuire Units.

The following design considerations form each basis for the Loose Parts Monitoring Systems (LPMS) installed at McGuire.

1. The Loose Parts Monitoring System (LPMS) is designed to detect and capture metal-to-metal impacts occurring within the Reactor Coolant System. The occurence of false alarms is minimized.
2. Regulatory Guideline 1.133 sets forth a method acceptable to the Nuclear Regulatory Commission(NRC) staff for implementing a loose part detection program that meets "instrumentation channels (e.g. cabling, amplifiers) associated with the two sensors recommended at each natural collection region should be physically separated from each other starting at the sensor locations to a point in the plant that is always accessible for maintenance during full-power operation." It can be shown that the LPMS design does not introduce any significant safety concerns, and no new failure modes are introduced. Each individual channel consists of a sensor, dedicated hardline and softline cables, and a preamplifier. Cabling from multiple sensors will be installed in common conduit as required to facilitate installation and preamplifiers for multiple channels will be located within the same electrical boxes. The preamplifiers are located in containment at locations normally accessible during full power operations. The only external events for which failure modes could be introduced would be the result for which a unit shutdown and subsequent equipment damage inspection would be required (such as fire or high energy line break). Since the LPMS is not required for safe shutdown of a unit, the criteria concerning safe shutdown do not apply to the LPMS. The LPMS is not needed during the shutdown since it is only required during power operations, so safe shutdown compliance is not degraded.
3. The LPMS cabinet is seismically mounted and contains all electronics for capture and data analysis. The in-containment portion of the LPMS consists of accelerometers, preamplifiers and interconnection cables.
4. The LPMS provides analysis capability to determine damage potential of a detected loose part.

Accelerometers (transducers) are located the areas where loose parts are most likely to become entrapped. These are:

1. Three on the lower Reactor Vessel, mounted on incore guide tubes.
2. Three on the Upper Reactor Vessel, mounted on the lifting lugs.
3. Three on the steam generators. One mounted at the base between the primary nozzle and manway, one at the tubesheet elevation and one at the primary deck level.

In addition, one sensor is mounted on each reactor coolant pump support leg.

Experience has shown that the exact location of these transducers within each collection area is not critical. The acoustic wave that results from an impact propagates throughout the collection area.

The transducers are piezoelectric accelerometers.

The accelerometers on the lower reactor vessel are positioned on the incore instrument guide tubes as close to the reactor vessel as practical for inspection and maintenance. Mounting blocks are provided to physically clamp the accelerometer and associated junction box to the guide tube.

The accelerometers on the upper reactor vessel are stud mounted directly to the reactor head lifting lugs. The associated junction boxes are also mounted to the lugs. The steam generator accelerometers are stud mounted directly to each steam generator shell. The associated junction boxes are also mounted to each steam generator shell.

High temperature, high radiation, low noise hardline cable connects the sensor to a splice box where it is coupled to a high temperature, high radiation, low noise, softline cable. The softline cable connects to a pre-amplifier that is housed in a wall mounted enclosure. Twisted shielded pair cable is used to carry the signal out of containment to the LPMS cabinet.

The LPMS is a digitally based system. The analog field signals are converted to a digital signal for processing by the system. Alarm discrimination is a feature of this system. Extraneous alarms can be discriminated out by comparing the short term RMS average of the background signal to the long term RMS average. This method prevents alarms caused by electrical interferences and by small increases in the background level not indicative of a metal-to-metal impact.

The alarm detection sensitivity of the system is enhanced by filtering the background noise to remove noise outside of the frequency range of loose parts. The filters on the LPMS are hardware adjustable and are initially set to band-pass filter the signal between 1 and 15 KHZ. This allows the system to detect loose parts on the order of 4 ounces up to 30 lbs. in mass.

Metal-to-metal impacts detected by the system are captured digitally and recorded on tape. All channels are simultaneously captured for analysis. Software resides on the system to provide immediate analysis capability. Also, an audio monitor is available to allow the operator to listen to previously recorded or live signals.

Once a captured impact signal is verified to be a valid loose part, the mass and location of the part is evaluated. From this information, damage estimates can be evaluated.

The operator interface with the main computer in the control room provides both visual and audible indications to the control operator. This main computer also contains the interface to analysis software for determining the damage potential of a loose part. In addition, there is a tape recorder used to listen or analyze previously recorded loose parts indications and an audio monitor unit that allows the user to listen to live or previously recorded signals. The audio monitor includes special filters to enhance sound quality.

Lights on the front panel provide an indication of when a channel exceeds its setpoint or there is a system failure. Upon incidence of any of these alarms, a control board indication is also activated along with its associated audible alarm. Both indications are latched in the alarm state and require an operator response to reset.

The LPMS monitors its various components to verify correct operation. The system has sensor health monitoring features that verify that the in-containment portion of the system is functioning correctly. Also, the alarm setpoints and sensitivity are constantly adjusted by the system to maintain a specified value above background. System failure alarms are sounded if critical LPMS control room equipment fails and warnings are presented for other component failures.

7.7.1.13 Deleted Per 2005 Update

7.7.1.14 Fuel Handling Ventilation Exhaust System Instrumentation and Control

The electrical portion of the fuel handling ventilation exhaust subsystem is designed to provide exhaust fan run status, open-close status of check dampers, supply air flow monitoring, and to detect malfunctions in the filter units.

A description of the mechanical portion of the system is found in Section 9.4.2.2.

7.7.1.14.1 Controls

An on/off switch for fan control is provided on the HVAC Panel in the Control Room. The on/off switch will either energize or deenergize both 50% capacity fuel handling exhaust fans.

7.7.1.14.2 Indication

Indicator lights on the HVAC Panel in the Control Room are used to monitor exhaust fan run status, check damper open-close status, supply fan normal run status, and filter bypass status.

7.7.1.14.3 Alarms

Annunciator alarms for filter malfunction, high temperature and fire alarm are provided.

Alarm bells are provided at each end of the fuel pool to indicate loss of exhaust fan operation.

7.7.1.14.4 Bypass

A dampered bypass is provided around the fuel pool exhaust filter train for use during normal operation. Bypass position status is indicated on the HVAC Panel in the Control Room.

Refer to Table 9-37, page 4, “Exceptions and Comments,” C-2-i, for a complete description of the filter bypass.

7.7.1.15 RCS Leak Detection System

Exceptions taken from certain regulatory criteria for the performance of pipe break analysis in certain piping systems resulted in a commitment to monitor eight postulated break locations in the CLA injection piping. This commitment is documented in NUREG-0422, Supplement 4 (NRC SER related to the operation of MNS). The Acoustic Leak Detection System (ALDS), in conjunction with an augmented inservice inspection program and analyses performed, provided adequate protection from the postulated breaks within the CLA injection piping. The ALDS was designed to provide leak detection capability at the eight locations. This system monitored the cold leg accumulator injection lines at the first elbow off reactor coolant system loops A, B, C,

and D. This provided an early warning of possible degradation of the pressure boundary at the postulated break locations so that appropriate action (unit shutdown) could be taken prior to castastrophic failure of the 10 inch CLA injection line.

This regulatory commitment was revised to allow the RCS leakage detection system to perform the monitoring function. Although the RCS leakage detection system is less sensitive than the ALDS, the RCS leakage detection system will still be able to provide early warning of leakage from the postulated break locations. The indication of leakage from the postulated break locations by the RCS leakage detection system will still be well in advance of the piping failing catastrophically (rupture). Analysis has been performed to show that even with a leak rate of approximately 20 gpm, rupture of the CLA injection piping will not occur. A leak rate of 20 gpm is well within the capabilities of the RCS leakage detection system. As such, the RCS leakage detection system will provide early warning of possible degradation of the pressure boundary so that unit shutdown prior to catastrophic failure of the piping would still be accomplished. Additional discussions regarding the RCS leakage detection system is provided in Section 5.2.7 of the FSAR.

7.7.1.16 ATWS Mitigation Actuation Circuitry

An ATWS is an anticipated operational occurrence (such as loss of feedwater, condenser vacuum, or offsite power) which is accompanied by a failure of the Reactor Trip System (RTS) to shut down the reactor.

The ATWS Mitigation System and Actuation Circuitry (AMSAC) at McGuire Nuclear Station is based on the Westinghouse Owners Group WCAP-10858-P-A, Rev. 1, generic design 3. The AMSAC design for McGuire is based on conditions that indicate a loss of main feedwater event, which if accompanied by a failure of the RTS to scram leads to overpressurization of the Reactor Coolant System (RCS). The system monitors the position of all main feedwater control and isolation valves and the operating status of both main feedwater pumps.

Description

AMSAC actuation will occur when either both main feedwater pumps trip or when main feedwater flow to the steam generators is blocked due to valves closing in the line. When an actuation occurs the AMSAC circuitry will perform the following:

1. Trip the main turbine
2. Start both motor driven auxiliary feedwater pumps
3. Close the steam generator blowdown and sampling valves

Annunciators, a status indicator and computer alarms in the control room are also available.

To monitor the operating status of the main feedwater pumps, pressure switches are used that monitor the hydraulic control oil pressure to the stop valves. Each of the feedwater pump turbine stop valves will close when the pump turbine trips. The pressure switches monitor the hydraulic oil pressure holding the stop valves open. When a loss of pressure is indicated by 2 of the 3 pressure switches on a pump, the logic circuit will enable the AMSAC circuitry for the tripped pump. If both pump logic circuits are enabled, the AMSAC circuitry will actuate and perform as outlined earlier.

Position of the main feedwater control valves, feedwater control valve bypass valves and main feedwater isolation valves is monitored by limit switches on the valves. These switches are set to enable the AMSAC circuitry when a control valve in a main feedwater flow path is less than 25% open, with the associated control valve bypass valve less than 100% open or when a containment isolation valve is closed. Minimum AMSAC flow requirements can be maintained

with the control valve closed and the control valve bypass valve fully open. Therefore, the control valve indication is interlocked with the bypass valve indication such that both the control valve and the bypass valve must be closed to the stated setpoints to indicate a blocked flow path. If 3 out of 4 flow paths are blocked, the AMSAC circuitry will actuate and perform as outlined earlier. A bypass switch with a bypass indication light is installed on a control room control board. This bypass allows the operators to manually disable the control and isolation valve portion of the AMSAC circuitry when the unit is below 40% unit load during which time the feedwater control valves are cycling in the lower part of the stroke range. This bypass is initiated automatically when unit load is below 40% and after a 120 second time delay. This bypass resets automatically when the unit load reaches 40%. A 30 second delay is also installed for the control valve portion of the AMSAC circuitry. This delay will prevent normal valve movements from causing spurious AMSAC actuations at all power levels.

The AMSAC circuitry responds to an ATWS event through new inputs to existing control circuitry. The turbine trip is initiated by an input to the Turbine Control Supervisory Instrumentation System. Starting the motor driven auxiliary feedwater pumps and closing the blowdown and sampling valves is initiated by an input on the non-safety side of an existing isolation device in the auxiliary feedwater controls. The isolation device separates the non-safety signals from the safety related controls system.

The AMSAC design complies with all sections of the Safety Evaluation Report issued by the NRC (references 10, 11 12).

Seismic reviews have been completed for mounting the bypass switch on the control board and for mounting the limit switches onto the control and isolation valves. A 10 CFR 50.48 review has also been performed.

A principal criteria applied to AMSAC is that the AMSAC functions be accomplished without relying on the existing reactor shut down system. Separate equipment is used for AMSAC and for the Reactor Protection System (RPS). The pressure switches which will monitor the main feedwater pumps will have no RPS interface. The limit switches which will monitor the main feedwater control and isolation valves for AMSAC provide no signals to the RPS. The AMSAC logic circuitry has a non-interruptible non-safety 125 V dc power source. The Auxiliary Feedwater, Steam Generator Blowdown and Steam Generator Sampling are systems which are safety related or have safety related components and will receive an AMSAC input. The interface with these systems is through an existing non-safety/safety isolation device and is designed so that the safety related system will perform as designed coincident with a postulated failure of the non-safety AMSAC input.

Non-safety related equipment in the AMSAC circuitry is subject to specific quality assurance guidance identified in NRC Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment that is Not Safety-Related," (Reference 13).

7.7.2 Analysis

The Unit Control Systems are designed to assure high reliability in any anticipated operational occurrences. Equipment used in these systems is designed and constructed with a high level of reliability.

Proper positioning of the control rods is monitored in the Control Room by bank arrangements of the individual position columns for each rod cluster control assembly. A rod deviation alarm alerts the operator of a deviation of one rod cluster control assembly from the other rack in that bank position. There are also insertion limit monitors with visual and audible annunciation. A rod bottom alarm signal is provided to the Control Room for each full length rod cluster control

assembly. Four excore long ion chambers also detect asymmetrical flux distribution indicative of rod misalignment.

Overall reactivity control is achieved by the combination of soluble boron and rod cluster control assemblies. Long term regulation of core reactivity is accomplished by adjusting the concentration of boric acid in the reactor coolant. Short term reactivity control for power changes is accomplished by the unit control systems which automatically move rod cluster control assemblies. The input signals to the unit control systems include neutron flux, coolant temperature, and turbine load.

The axial core power distribution is controlled by moving the control rods through changes in reactor coolant system boron concentration. Adding boron causes the rods to move out thereby reducing the amount of power in the bottom of the core, this allows power to redistribute toward the top of the core. Reducing the boron concentration causes the rods to move into the core thereby reducing the power in the top of the core, the result redistributes power towards the bottom of the core.

The Unit Control Systems prevent an undesirable operating condition to be reached. If this condition is reached, the plant is protected by reactor trip. The description and analysis of this protection is covered in Section 7.2. Worst case failure modes of the unit control systems are postulated in the analysis of off-design operational transients and accidents covered in Chapter 15, such as, the following:

1. Uncontrolled rod cluster control assembly withdrawal from a subcritical condition.
2. Uncontrolled rod cluster control assembly withdrawal at power.
3. Rod cluster control assembly misalignment.
4. Loss of external electrical load and/or turbine trip.
5. Loss of all ac power to the station auxiliaries (Station Blackout).
6. Excessive heat removal due to Feedwater System malfunctions.
7. Excessive load increase.
8. Accidental depressurization of the Reactor Coolant System.

These analyses show that a reactor trip setpoint is reached in time to protect the health and safety of the public under these postulated incidents and that the resulting coolant temperatures produce a DNBR well above the limiting value (see Section 4.4.1.1). Thus, there is no cladding damage and no release of fission products to the Reactor Coolant System under the assumption of these postulated worst case failure modes of the plant control systems.

7.7.2.1 Separation of Protection and Control Systems

In some cases, it is advantageous to employ control signals derived from individual protection channels through isolation amplifiers contained in the protection channel. As such, a failure in the control circuitry does not adversely affect the protection channel. Test results have shown that a short circuit or the application of 120 vac or 150 vdc on the isolated output portion of the circuit (nonprotection side of the circuit) does not affect the input (protection) side of the circuit.

Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper aciton of a protection system channel designed to protect against the condition, the remaining redundant protection channels are capable of providing the protective action even when degraded by a second random failure. This meets the applicable requirements of Section 4.7 of IEEE 279-1971.

The pressurizer pressure channels needed to derive the control signals are physically isolated from the pressure channels used to derive protection signals.

7.7.2.2 Response Considerations of Reactivity

Reactor shutdown with control rods is completely independent of the control functions since the trip breakers interrupt power to the full length rod drive mechanisms regardless of existing control signals. The design is such that the system can withstand accidental withdrawal of control groups or unplanned dilution of soluble boron without exceeding acceptable fuel design limits. The design meets the requirements of Criteria 25 of the 1971 GDC.

No single electrical or mechanical failure in the Rod Control System can cause the accidental withdrawal of a single rod cluster control assembly from the partially inserted bank at full power operation. An enhancement of the licensing basis for system response to a single failure in the Rod Control System was implemented by a new rod drive mechanism current order timing specified in Reference 8, and a new current order surveillance test. The operator can deliberately withdraw a single rod cluster control assembly in the control bank; this feature is necessary in order to retrieve a rod, should one be accidentally dropped. In the extremely unlikely event of simultaneous electrical failures which could result in single RCCA withdrawal, rod deviation is displayed on the unit annunciator, and the individual rod position readouts indicate the relative positions of the rods in the bank. Withdrawal of a single rod cluster control assembly by operator action, whether deliberate or by a combination of errors, results in activation of the same alarm and the same visual indications.

The Chemical Volume Control System (CVCS) provides for boron concentration control to maintain the reactor in the cold shutdown state irrespective of the disposition of the control rods.

The NRC issued Generic Letter 93-04, “Control Rod System Failure and Withdrawal of Rod Control Cluster Assemblies, 10 CFR 50.54(f),” on June 21, 1993. This generic letter notified licensees of the occurrence at the Salem Nuclear Generating Station, Unit 2, of a control rod position indicator malfunction during reactor startup which had the possibility of placing that unit outside its fuel design bases (rod withdrawal actual exceeding indicated). Accordingly, the NRC requested review of the similar McGuire Nuclear Station systems supplied by Westinghouse. As stated in the initial responses to Generic Letter 93-04 (letter from M.S. Tuckman to the NRC, dated August 5, 1993; and letter from M.S. Tuckman to the NRC, dated September 20, 1993), the evaluations presented for similar control rod equipment failures concluded that Departure from Nucleate Boiling (DNB) would not occur for the worstcase asymmetric rod withdrawal. Short-term compensatory measures were identified which were implemented by MNS to preclude an event similar to that described in the generic letter. Further long-term actions committed to were to implement the Westinghouse Owner’s Group (WOG) recommended current order timing modification and the new current order surveillance test.

Each bank of control and shutdown rods in the system is divided into two groups of up to 4 or 5 mechanisms each. The rods comprising a group operate in parallel through multiplexing thyristors. The two groups in a bank move sequentially such that the first group is always within one step of the second group in the bank. A definite schedule of actuation and deactuation of the stationary gripper, moveable gripper, and lift coils of a mechanism is required to withdraw the rod cluster control assembly attached to the mechanism. Since the four stationary grippers, moveable gripper, and lift coils associated with the rod cluster control assemblies of a rod group are driven in parallel, any single failure which could cause rod withdrawal would affect a minimum of one group of rod cluster control assemblies. Mechanical failures are in the direction of insertion, or immobility.

The identified multiple failure involving the least number of components consists of open circuit failure of the proper two-out-of-sixteen wires connected to the gate of the lift coil thyristors. The probability of open wire (or terminal) failure is 0.016×10^{-6} per hour by MIL-HDB217A. These wire failures would have to be accompanied by failure, or disregard, of the indications mentioned above. The probability of this occurrence is therefore too low to be significant.

Concerning the human element, to erroneously withdraw a single rod cluster control assembly, the operator has to improperly set the BANK SELECTOR switch, the LIFT COIL DISCONNECT switches, and the IN-OUT-HOLD switch. In addition, the three indications have to be disregarded or ineffective. Such series of errors requires a complete lack of understanding and administrative control. A probability number cannot be assigned to a series of errors such as these.

The Rod Position Indication System provides direct visual displays of each control rod assembly position. The unit computer alarm is actuated for deviation of rods from their banks. In addition, a rod insertion limit monitor provides an audible and visual alarm to warn the operator that an abnormal condition is approaching due to dilution. The low-low insertion limit alarm alerts the operator to follow emergency boration procedures. The facility reactivity control systems are such that acceptable fuel damage limits are not exceeded even in the event of a single malfunction of either system.

An important feature of the Rod Control System is that insertion is provided by gravity fall of the rods.

In all analyses involving reactor trip, the single, highest worth rod cluster control assembly is postulated to remain untripped in its full out position.

One way of detecting a stuck control rod assembly is available from the actual rod position information displayed on the control board. The control board position readouts, one for each full length rod, give the operator the actual position of the rod in steps. The indications are grouped by banks (e.g., CONTROL BANK A, CONTROL BANK B, etc.) to indicate to the operator the deviation of one rod with respect to other rods in a bank. This serves as a means to identify rod deviation.

The computer monitors the actual position of all rods. Should a rod be misaligned from the other rods in that bank by greater than $\pm$7.5 inches, the rod deviation alarm is actuated.

Misaligned rod cluster control assemblies are also detected and alarmed in the Control Room via the flux tilt monitoring portion of the Nuclear Instrumentation System which is independent of the unit computer.

Isolated signals derived from the Nuclear Instrumentation System are compared with one another to determine if a preset amount of deviation of average power level has occurred. Should such a deviation occur, the comparator output operates a bistable unit to actuate a control board annunciator. This alarm alerts the operator to a power imbalance caused by a misaligned rod. By use of individual rod position readouts, the operator can determine the deviating control rod and take corrective action. The design of the plant control systems meets the requirements of Criteria 23 of 10CFR 50 Appendix A.

The CVCS boron control can compensate for all xenon burnout reactivity transients without exception.

The Rod Control System can compensate for xenon burnout reactivity transients over the allowed range of rod travel. Xenon burnout transients of larger magnitude must be accompanied by boration or by reactor trip (which eliminates the burnout).

The CVCS boron control is not used to compensate for the reactivity effects of fuel/water temperature changes accompanying power level changes.

The Rod Control System can compensate for the reactivity effect of fuel/water temperature changes accompanying power level changes over the full range from full load to no load at the design maximum load uprate.

Automatic control of the rods is limited to the range of approximately 15 percent to 100 percent of rating.

The CVCS boron concentration control maintains the reactor in the cold shutdown state irrespective of the disposition of the control rods.

7.7.2.3 Step Load Changes Without Steam Dump

The Reactor Control System restores equilibrium conditions, without a trip, following a plus or minus 10 percent step change in load demand, over the 15 to 100 percent power range for automatic control. Steam dump is blocked for load decrease less than or equal to 10 percent. A load demand greater than full power is prohibited by the administrative control limits used when the turbine is operated under load control.

The Reactor Control System minimizes the reactor coolant average temperature deviation during the transient within a given value and restores average temperature to the programmed setpoint. Excessive pressurizer pressure variations are prevented by using spray and heaters and power relief valves in the pressurizer.

The control system must limit nuclear power overshoot to acceptable values following a 10 percent increase in load to 100 percent.

7.7.2.4 Loading and Unloading

Ramp loading and unloading of 5 percent per minute can be accepted over the 15 to 100 percent power range under automatic control without tripping the unit. The function of the control system is to maintain the coolant average temperature as a function of turbine-generator load.

The coolant average temperature increases during loading and causes a continuous insurge to the pressurizer as a result of coolant expansion. The sprays limit the resulting pressure increase. Conversely, as the coolant average temperature is decreasing during unloading, there is a continuous outsurge from the pressurizer resulting from coolant contraction. The pressurizer water level is programmed such that the water level is above the setpoint for heater cutout during the loading and unloading transients. The primary concern during loading is to limit the overshoot in nuclear power and to provide sufficient margin in the overtemperature ΔT setpoint.

The automatic load controls are designed to adjust the unit generation to match load requirements within the limits of the unit capability and licensed rating.

7.7.2.5 Load Rejection Furnished By Steam Dump System

When a load rejection occurs and the difference between the required temperature setpoint of the Reactor Coolant System and the actual average temperature exceeds a predetermined amount, a signal actuates the steam dump to maintain the Reactor Coolant System temperature within control range until a new equilibrium condition is reached.

The reactor power is reduced at a rate consistent with the capability of the Rod Control System. Reduction of the reactor power is automatic. The steam dump flow reduction is as fast as rod cluster control assemblies are capable of inserting negative reactivity.

The Rod Control System can then reduce the reactor temperature to a new equilibrium value without causing overtemperature and/or overpressure conditions. The steam dump steam flow capacity is 40 percent of full load steam flow at full load steam pressure.

The steam dump flow reduces proportionally as the control rods act to reduce the average coolant temperature. The artificial load is therefore removed as the coolant average temperature is restored to its programmed equilibrium value.

The dump valves are modulated by the reactor coolant average temperature signal. The required number of steam dump valves can be tripped quickly to stroke full open or modulate, depending upon the magnitude of the temperature error signal resulting from loss of load.

7.7.2.6 Reactor Trip

The unit is operated with a programmed average temperature as a function of load, with the full load average temperature significantly greater than the equivalent saturation pressure of the safety valve setpoint. The thermal capacity of the Reactor Coolant System is greater than that of the secondary system, and because the full load average temperature is greater than the no load temperature, a heat sink is required to remove heat stored in the reactor coolant to prevent actuation of steam generator safety valves for a trip from full power. This heat sink is provided by the combination of controlled release of steam to the condenser and by makeup of cold feedwater to the steam generators.

The Steam Dump System is controlled by the reactor coolant average temperature signal whose setpoint values are programmed as a function of turbine load. Actuation of the steam dump is rapid to prevent actuation of the steam generator safety valves. With the dump valves open, the average coolant temperature starts to reduce quickly to the no load setpoint. A direct feedback of temperature acts to proportionally close the valves to minimize the total amount of steam which is bypassed.

Following a reactor trip, the feedwater flow is cut off when the average coolant temperature decreases below a given temperature or when the steam generator water level reaches a given high level.

Additional feedwater makeup is then controlled manually to restore and maintain steam generator water level while assuring that the reactor coolant temperature is at the desired value. Residual heat removal is maintained by the steam header pressure controller (manually selected) which controls the amount of steam flow to the condensers. This controller operates a portion of the same steam dump valves to the condensers which are used during the initial transient following a 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 provides full charging flow to restore water level in the pressurizer. Heaters are then turned on to restore pressurizer pressure to normal.

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

7.7.3 References

1. Lipchak, J. B., Nuclear Instrumentation System, Westinghouse Electric Corporation, *WCAP-8255*, January, 1974.
2. Blanchard, A. E. and Katz, D. N., Solid State Rod Control System, Full Length, Westinghouse Electric Corporation, *WCAP-7778*, December, 1971.
3. Loving, J. J., In-Core Instrumentation (Flux-Mapping System and Thermocouples), Westinghouse Electric Corporation, *WCAP-7607*, July, 1971.
4. Blanchard, A. E. and Calpin, J. E., Digital Rod Position Indication, Westinghouse Electric Corporation, *WCAP-8014*, December, 1972.
5. IM827, Rev. 1; Thermo-Scientific Instruction Manual for *Excore Neutron Flux Monitoring System*; MCM-1399.04-0123, Rev. 2.
6. Safety Evaluation Report Regarding Compliance with ATWS Rule (10CFR 50.62).
7. MCC-1503-13-00-0543, Rev 0, USQ Evaluation for a Revision to an NRC commitment regarding the monitoring of 8 Postulated Break Locations in the CLA Injection Piping.
8. NSD-TB-94-05-R0, Rod Control - CRDM Timing Change, May 6, 1994 and NSD-TB-94-05-ADA-R0, October 20, 1994.
9. Neutron Flux Monitor for Duke Power Company McGuire Nuclear Plant, Copyright 1995 by Gamma-metrics.
10. D. Hood (NRC) letter to H.B. Tucker (Duke) dated September 22, 1986, “Anticipated Transients Without Scram, McGuire Nuclear Plant”.
11. D.S. Hood (NRC) letter to H.B. Tucker (Duke) dated November 6, 1987, “ATWS Rule (10 CFR 50.62) for McGuire and Catawba Nuclear Stations”.
12. D.S. Hood (NRC) letter to H.B. Tucker (Duke) dated August 3,1989, “Approval of Changes in ATWS / AMSAC Design, McGuire and Catawba Nuclear Stations”.
13. NRC Generic Letter 85-06, “Quality Assurance Guidance for ATWS Equipment that is Not Safety-Related, ” April 16, 1985.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.7.

7.8 Operating Control Stations

Consistent with proven power station design philosophy, all controls, instrumentation displays and alarms required for startup, operation and shutdown of Units 1 and 2 are located in one centralized Control Room and are readily available to the operator. Remote control stations are provided for certain auxiliary systems which do not involve unit control or emergency functions.

7.8.1 General Layout

The Control Room design is such that one man can supervise operation of both units during normal steady state conditions; however, other qualified operators are always available to assist during normal and abnormal operating conditions. Figure 7-29 shows the control board arrangement for both units.

7.8.2 Information Display and Control Functions

An integral part of the main control board design philosophy is to provide the operator with the required information and controls to enable him to evaluate system status and performance and to control the unit in a minimum of time under all conditions. Therefore, consideration is given in main control board layout to the fact that certain systems normally require more attention from the operator. Controls are generally arranged by system in well defined groups with special emphasis being given to the reactor and to other systems requiring frequent or continuous operator attention.

The Ovation PCS provides advanced display and control functions, such as graphical displays, trending, logging, and soft controls. The Human Machine Interface (HMI) includes Operator and Engineering Workstations. In certain cases, Ovation M/A stations are provided, capable of performing loop control functions should the soft controls on the DCS become inoperable.

System level bypass indication is automatically provided to the operator by the plant computer 1.47 bypass application. Each bypass or deliberately induced inoperability which

1. affects an automatic function important to public safety, and
2. can be reasonably expected to occur more frequently than once per year (during times when the affected system is required to be operable),

shall be automatically indicated in the control room.

The Bypass Indication System is designed and installed such that a failure of the System will not have adverse effects on the monitored systems or the failure of one train of the System will not have adverse effects on the other train of the System.

The Bypass Indication System obtains its input from such devices as valve position limit switches, circuit breaker auxiliary contacts, mode switch contacts, loss of voltage relays, etc. A means of manual actuation for each indication exists in the Control Room. Individual indicators provided for each unit even though the system may be shared between units. Indicator window legend terminology will be explicit as to the safety system affected. The operator cannot disable any bypass indications at any time.

It is our intention to fully comply with the intent of the requirements stated in Paragraph 4.13 of IEEE 279-1971 and the position explained in NRC Regulatory Guide 1.47.

In general, if any analog channel in the ESF Actuation and Reactor Protection Systems is taken out of service for any reason, the channel is placed in the tripped mode, and a channel trip

status light is lit on the control board. In addition, an alarm will sound and an associated alarm or panel light will be lit. Due to the severity of the consequences, the channel bistable output relays associated with the Phase B Containment Isolation function are not tripped, to reduce the possibility of an inadvertent actuation. In general, analog channels in the ESF Actuation and Reactor Protection System may be placed in the bypassed condition for test and maintenance purposes. However, the Technical Specifications dictate which channels may be placed in the bypassed condition. A status light indicating a bypassed condition is provided for each protection channel.

When testing or maintenance is performed on the solid state logic protection racks, or on the associated safeguards test cabinets, an alarm is energized (one per rack or cabinet per train).

A process computer is used on each unit to provide fuel management measurements and calculations for both units. A process computer for each unit is also provided for sequence monitoring, alarm monitoring, performance monitoring, and data logging of the startup and shutdown of the turbine-generator. Monitoring and display functions of the computer which audit Nuclear Steam Supply System parameters of major interest are duplicated elsewhere in the Control Room. This type of computer application has been successfully applied to units presently in operation on the Duke system.

7.8.3 Summary of Alarms

Visible and audible alarm units are incorporated into the control boards to warn the operator if limiting conditions are approached by any system. Audible Containment evacuation alarms are initiated from the Radiation Monitoring System and from the source range nuclear instrumentation. Audible alarms are sounded in appropriate areas throughout the station if high radiation conditions are present in that area. Alarms for the nuclear systems are indicated in process diagrams in Chapter 6, Chapter 7 and Chapter 9.

7.8.4 Communication

Station Telephone and Paging Systems are provided with redundant power supplies to provide the Control Room operator with constant communication with all areas of the station. Communication outside the station is through the Bell South System and the Duke private Telephone and Microwave System. Refer to Section 9.5.2 for detailed information.

7.8.5 Occupancy

Safe occupancy of the Control Room during abnormal conditions is provided for in the design of the Auxiliary Building. Adequate shielding is used to maintain tolerable radiation levels in the Control Room for maximum hypothetical accident conditions. The Control Area Ventilation System is provided with radiation detectors and appropriate alarms. Provisions are made for the control room air to be recirculated through absolute and charcoal filters. Emergency lighting is provided.

The potential magnitude of a fire in the Control Room is limited by the following factors:

1. The Control Room construction and furnishings are of noncombustible materials.
2. Control cables and switchboard wiring meet the flame test as described in the Insulated Power Cable Engineers Association Publication S-61-402 and National Electrical Manufacturers Association Publication WC 5-1961.
3. Qualified trained personnel, adequate extinguishers and accessibility to all Control Room areas are provided.

A fire, if started, would be of such a small magnitude that it could be extinguished by the operator using a hand fire extinguisher. The resulting smoke and vapors would be removed by the Control Area Ventilation System.

Essential auxiliary equipment is controlled by either stored energy air circuit breakers or AC motor starters. Air circuit breakers, which are accessible, can be manually closed in the event dc control power is lost. The essential power supplied to essential ac motors also supplies control power for their motor starters.

In the unlikely event that temporary abandonment of the Control Room becomes necessary, the operator immediately takes the necessary actions to shut the reactor down. Sufficient instrumentation and controls are provided external to the Control Room to maintain the reactor in a safe shutdown condition (see Section 7.4).

7.8.6 Auxiliary Control Stations

Auxiliary control stations are provided where their use simplifies control of auxiliary systems equipment such as waste evaporator, sample valve selectors, chemical addition, etc. Sufficient indicators and alarms are provided so that the Control Room operator is made aware of abnormal conditions involving remote control stations.

7.8.7 Safety Features

Control Room layouts provide the necessary controls to start, operate and shut down the units with sufficient information display and alarm monitoring to assure safe and reliable operation under normal and accident conditions. Special emphasis is given to maintaining control during accident conditions. The layout of the Engineered Safety Feature devices of the control board is designed to minimize the time required for the operator to evaluate the system performance under accident conditions.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.8.

THIS PAGE LEFT BLANK INTENTIONALLY.