Table of Contents

List of Tables

List of Figures

7.0 Instrumentation and Control

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.0.

THIS PAGE LEFT BLANK INTENTIONALLY.

7.1 Introduction

Instrumentation and control systems include the Reactor Protective System, the Engineered Safeguards Protective Systems, the Rod Drive Control System, the Integrated Control System, the Nuclear Instrumentation System, the Non-Nuclear Instrumentation System, the Incore Monitoring System and the Automatic Feedwater Isolation System.

7.1.1 Identification of Safety-Related Systems

The protective systems, which consist of the Reactor Protective Systems, the Engineered Safeguards System and the Automatic Feedwater Isolation System perform important control and safety functions. The protective systems extend from the sensing instruments to the final actuating devices, such as circuit breakers and pump or valve motor contactors.

7.1.2 Identification of Safety Criteria

7.1.2.1 Design Bases

The protective systems are designed to sense plant parameters and actuate emergency actions in the event of abnormal plant parameter values. They meet the intent of the Proposed IEEE "Criteria for Nuclear Power Plant Protection Systems" dated August, 1968. (IEEE No. 279). The TXS RPS/ESPS also meets the intent of IEEE Std 603-1998. Protective system equipment located in the Control Room, Cable Room, and Aux Building is designed for a mild environment, not LOCA conditions (i.e. 59 psig, 273°F).

7.1.2.2 Single Failure

The protective options meet the single failure criterion of IEEE No. 279 and for TXS RPS/ESPS IEEE Std 603-1998 to the extent that:

1. No single component failure will prevent a protective system from fulfilling its protective functions when action is required.
2. No single component failure will initiate unnecessary protective system action where implementation does not conflict with the criterion above.

7.1.2.3 Redundancy

All protective system functions are implemented by redundant sensors, measuring channels, logic, and actuation devices. These elements combine to form the protective channels.

7.1.2.4 Independence

Redundant protective channels are electrically independent and are packaged to provide physical separation.

7.1.2.5 Separation

Protective channels are physically separate and are electrically isolated from regulating instrumentation. Only one string of instrumentation may be selected at a given time for use in a system control function, and electrical isolation is assured through the use of appropriate isolation devices. A fifth channel of regulating instrumentation not associated with protection is employed for additional control purposes.

For Units with the digital ESPS/RPS installed, protective channels of the RPS and ESPS are interconnected with fiber optic cabling for inter-channel communication. These cables are used for

diagnostic data that is shared between protective channels over fiber optic communications links, do not serve a mutually redundant safety related function, and are not required for the RPS and ESPS to perform their safety related functions. Therefore, these fiber optic cables do not require physical separation. The fiber optic cables that run between safety-related cabinets or enclosures are colored red. Fiber optic media without metallic shields or armor inherently provides sufficient Class 1E electrical isolation for data exchange pathways between devices. Fiber optic cable that is used for mutually redundant safety related functions are required to be physically separated.

7.1.2.6 Manual Trip

Manual trip switches, independent of the automatic trip instrumentation, are provided.

7.1.2.7 Testing

Manual testing facilities are built into the protective systems to provide for:

1. Preoperational testing to give assurance that a protective system can fulfill its required protective functions.
2. On-line testing to prove operability and to demonstrate reliability.
3. For Units with the digital Reactor Protective System (RPS) and Engineered Safeguards Protective System (ESPS) not installed, BWNT STAR module provides both manual and automated test capability, and self diagnostic tests performed during start-up and operation. The front panel of the STAR module has LED indicators which indicate module status.
4. For Units with the digital Reactor Protective System (RPS) and Engineered Safeguards Protective System (ESPS) installed, a test mode and a manual bypass are provided. The system provides the capability to perform start-up and operational testing through the Graphical Service Monitor when the test mode is enabled. The system performs continuous testing through self checking routines.

7.1.3 Identification of Protective Equipment

All safety related sensors, transmitters, transducers, cabinets, etc. located outside the control room are physically identified by placement of a permanent, conspicuous tag on or adjacent to the device. A typical tag bears the wording "Safety Related." The following are examples of equipment that should be tagged:

Swgr 1TC

LD Ctr lX8

MCC lXSl

ESG channel 1, 3, 5, & 7

DC Pnlbd 1DIA

Vital Pwr Pnlbd 1KVIA

RPS Ch A

AFIS Analog Channel 1

Swgr 1TD

LD Ctr 1X9

MCC 1XS2

ESG channel 2, 4, 6, & 8

DC Pnlbd 1DIB

Vital Pwr Pnlbd 1KVIB

RPS Ch B

AFIS Analog Channel 2

Swgr 1TE

MCC lXS3

DC Pnlbd 1DIC

Vital Pwr Pnlbd 1KVIC

RPS Ch C

AFIS Analog Channel 3

AFIS Digital Channel 1

ESG Channel Even-Odd

DC Pnlbd 1DID

Vital Pwr Pnlbd 1KVID

RPS Ch D

AFIS Analog Channel 4

AFIS Digital Channel 2

7.1.4 NRC IE BULLETIN 90-1 AND SUPPLEMENT 1

The NRC issued IE Bulletin 90-1, "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 Power Company's Bulletin response actions included identification of transmitters from the suspect lots for Oconee 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 form 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 Oconee Nuclear Station.

The NRC issued Supplement 1 to IE Bulletin 90-01, "Loss of Fill-Oil in Transmitters Manufacturecd by Rosemount," on December 22, 1992, providing further details on monitoring programs for the transmitters described in the original bulletin. Duke Power Company responded on May 24, 1993 by the letter from H. B. Tucker to the NRC. Subsequently, the NRC issued its Safety Evaluation Report (SER) on May 19, 1995 which provided approval and closeout of IE Bulletin 90-01 and Supplemental 1 for the Oconee Nuclear Station.

7.1.5 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 Bulleting No. 90-01, Supplement 1, "Loss of Fill Oil in Transmitters Manufactured by Rosemount."
4. Nuclear Regulatory Commission, Letter from L. A. Wiens to J. W. Hampton (DPC), May 19, 1995, "NRC Bulletin 90-01 Supplement 1, Loss of Fill Oil in Transmitters Manufactured by Rosemount."

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.1.

7.2 Reactor Protective System

Deleted Paragraph (s) per 2009 Update

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

7.2.1 Design Bases

The RPS includes all design basis features of Section 7.1.2 with the following additions:

7.2.1.1 Loss of Power

A loss of power to a reactor protective channel will cause that protective channel to trip.

7.2.1.2 Equipment Removal

For Units with the digital RPS not installed, the RPS initiates a protective channel trip whenever a module or subassembly is removed from the equipment cabinet. Removing a reactor trip module causes the associated control rod drive breaker to trip.

For Units with the digital RPS installed, removal of a computer card from the RPS will initiate a protective channel trip. Removal of an input card will fault the input signals on that card and alarm, but will not initiate a protective channel trip. Removal of an output card will generate a channel trouble alarm and will initiate a half-channel trip (both of the outputs from the affected card assume a tripped state which creates a half-channel trip).

7.2.1.3 Diverse Means of Reactor Trip

In the unlikely event of a systematic or complete failure of the Reactor Coolant System low pressure signals to trip the reactor following the initiation of emergency core cooling, there is a separate, diverse means of assuring reactor trip. A high pressure in the Reactor Building is independently sensed by four sensors, and independent signals are fed from these sensors to the four Reactor Protective System channels to provide the desired diverse reactor trip signal.

7.2.2 System Design

7.2.2.1 System Logic

For Units with the digital RPS not installed, the system as shown in Figure 7-1 consists of four identical protective channels, each terminating in a trip relay within a reactor trip (RT) Module. In the normal untripped state, each protective channel functions as an AND gate, passing current to the terminating relay and holding it energized as long as all inputs are in the normal energized (untripped) state. Should any one or more inputs become de-energized (tripped), the terminating relay in that protective channel becomes an OR gate.

Each of the four protective channels terminates in a channel trip relay within a reactor trip module. There are four such modules. Each protective channel trip relay has four contacts, each controlling a logic relay in one reactor trip module. Therefore, each reactor trip module has four logic relays controlled by the four protective channels. The four logic relays combine to form a 2-out-of-4 coincidence network in each

reactor trip module. The coincidence logics in all reactor trip modules trip whenever any two of the four protective channels trip.

The reactor trip modules are given the same designation as the protective channel whose trip relay they contain and in whose cabinet they are physically located. Thus, the protective channel A reactor trip module is located in protective channel A cabinet, etc. (Figure 7-1). The coincidence logic in each of the four reactor trip modules controls the corresponding trip breaker in each incoming redundant path powering the control rod drives.

Deleted Paragraph(s) per 2009 Update.

The coincidence logic contained in the Reactor Protective System (RPS) channel A Reactor Trip Module (RTM) controls trip breaker A in the Control Rod Drive System as shown in Figure 7-1, channel B RTM controls breaker B, channel C RTM controls breaker C, and channel D RTM controls breaker D. Breakers A and C are placed in series in one parallel path, and breakers B and D are in series in the other parallel path. All 600 VAC 3-phase power to the rod drives is via these parallel paths. Combinations that could initiate a trip, in Boolean logic terms, are AB + AD + BC + CD (+ meaning logic "or"). This is 1-out-of-2 logic taken twice and is referred to as (1-out-of 2) x 2 logic. It should be noted that when any two out of four RPS channels trip, all reactor trip modules trip, commanding all CRD trip breakers to open.

For Units with the digital RPS installed the RPS consists of four independent protective channels, as shown in Figure 7-1. Each RPS protective channel contains the sensor input modules, output modules, a channel computer, four hardwired reactor trip relays (RTRs) and associated contacts. When the protective channel inputs are in the normal, or untripped, state the RTR is energized and no trip signal is sent to the CRD trip devices. Channel A provides input signals to its associated Channel A RTR within its cabinet and also sends this signal to each of its remaining Channel RTRs in the Channel B, C, and D cabinets. Each channel cabinet has the four RTR contact sets configured to provide 2-out-of-4 coincidence trip logic. When a protective channel trips, it sends the protective channel trip signal to its corresponding relays in each protective channel. When any two RPS protective channels receive channel trip signals, the RTR logic in each protective channel actuates to remove power from its associated CRD trip device. All RTRs trip whenever any two of the four protective channels trip.

The coincidence logic contained in the RPS protective channel A RTR controls breaker A in the Control Rod Drive (CRD) System as shown in Figure 7-1. Protective Channels B, C, and D will control breakers B, C, and D respectively in the Control Rod Drive System. Breakers A and C are placed in series in one parallel path and breakers B and D are in series in the other parallel path. All 600VAC 3-phase power to the rod drives is via these parallel paths. Combinations that could initiate a trip, in Boolean logic terms, are AB + AD + BC + CD (+ meaning logic "or"). This is 1-out-of-2 logic taken twice and is referred to as (1-out-of-2) x 2 logic. It should be noted that when any two out of four RPS protective channels trip, all RTRs trip, commanding all CRD trip breakers to open.

Independence is maintained in the four protective channels which are interconnected via fiber-optic data links. These links provide the means to exchange data, which is used for signal validation, fault and deviation detection, and trip actuation. This provides additional fault detection. If interchannel communications are lost, the associated signals are faulted as well. Faulted signals are eliminated from use in the signal selection logic. With only the hardwired signal as valid, the signal is passed directly to the subsequent logic, thus ensuring protective channel independence. The second maximum (2.MAX) and second minimum (2.MIN) signal selection functions are used for analog inputs, and 2-out-of-4 selection logic is used for contact inputs. The 2.MAX and 2.MIN functions remain until less than two valid signals are present. The 2-out-of-4 logic function reduces to a 2-out-of-3 logic for any condition that causes an input signal fault, including loss of power.

For Units with the digital RPS installed, three of the four RPS channel computers (A, B, and C) also perform a redundant ESPS logic function (Section 7.3.2). Therefore, three of the four RPS protective channel computers calculate both RPS and ESPS functions. RPS protective channel D calculates only RPS functions.

For Units with the digital RPS installed or not installed, the undervoltage coils of the control rod drive breakers receive their power from the protective channel associated with each breaker. The manual reactor trip switch is interposed in series between each RTM or RTR logic and the assigned breakers undervoltage coil.

In response to NRC Generic Letter 83-28 automatic actuation of the AC breaker shunt trip attachments for the Reactor Trip System and Manual Trip Actuation have been installed. This upgrade improves the reactor trip breaker reliability.

For the reactor trip breakers in each channel a relay is installed with its operating coil in parallel with the existing undervoltage device. The output contacts of these relays controls the power to the shunt trip devices. Thus, when power is removed from the breaker undervoltage trip attachment on either a manual or automatic trip signal, the shunt trip attachment is energized to provide an additional means to trip the breaker. Test switches are installed to permit independent testing of the shunt and undervoltage trip devices. Loss of shunt trip control power is annunciated in the control room indicating that the shunt trip device is not operable.

7.2.2.2 Summary of Protective Functions

The four Reactor Protective System protective channels are identical in their functions, which combine in the system logic to trip the reactor automatically and protect the reactor core for the following conditions:

1. When the reactor power, as measured by neutron flux, exceeds a fixed maximum limit.
2. When the reactor power, as measured by neutron flux, exceeds the limit set by the reactor coolant flow and power imbalance.
3. When the reactor power exceeds the limit set by the number and combination of reactor coolant pumps in operation.
4. When the reactor outlet temperature exceeds a fixed maximum limit.
5. When a specified reactor pressure-outlet temperature relationship is exceeded.
6. When the reactor pressure falls below a fixed minimum limit.
7. When Reactor Building pressure exceeds a fixed maximum limit.
8. The RPS automatically trips the reactor to protect the Reactor Coolant System whenever the reactor pressure exceeds a fixed maximum limit.
9. The RPS automatically trips the reactor upon main turbine trip or trip of both main feedwater pumps.

The abnormal conditions that initiate a reactor trip are keyed to the above listing and tabulated in Table 7-1.

7.2.2.3 Description of Protective Channel Functions

The functions of the RPS described below apply to each protective channel. Reference Figure 7-1 for Control Logic.

7.2.2.3.1 Over Power Trip

For Units with the digital RPS not installed, the nuclear instrumentation provides a linear neutron flux signal in the power range as an indication of reactor power to a protective system bistable trip module.

When the neutron flux signal exceeds the trip point of the bistable, the bistable trips, de-energizing the associated protective channel trip relay.

For Units with the digital RPS installed, the nuclear instrumentation provides a linear neutron flux signal in the power range to the four protective channels. The protective channel signals are then compared and when the 2.MAX neutron flux signal exceeds the trip setpoint in two or more protective channels, a reactor trip is generated. Reference Trip #1 of Figure 7-1 for control logic.

7.2.2.3.2 Nuclear Over Power Trip Based on Flow and Imbalance

For Units with the digital RPS not installed, the Neutron flux and the reactor coolant flow are continuously monitored. A linear neutron flux signal is received from the nuclear instrumentation and a total reactor coolant flow signal is received from the flow tubes. A power level trip setpoint is established for a STAR module as the percentage reactor coolant flow rate multiplied by the flux to flow ratio limited to a user definable value of Pmax. The reactor power imbalance (power in the top half of the core minus the power in the bottom half of the core) reduces the power level trip setpoint such that the four pump power-imbalance boundaries illustrated in Figure 7-2 are not exceeded. Less than four pump power-imbalance protection is provided by the power level trip setpoint decrease due to flow decrease. When the neutron flux signal exceeds the power level trip setpoint established by the total reactor coolant flow and the reactor power imbalance the STAR module trips, de-energizing the associated protective channel trip relay. The upper limit of this variable trip can be adjusted as necessary to prevent exceeding the limits established by the COLR in the event that indicated flow increases due to instrument failure.

For Units with the digital RPS installed, neutron flux and the reactor coolant flow are continuously monitored. Upper and Lower flux signals are received from the nuclear instrumentation and a total flux and a delta flux reading is calculated by each RPS protective channel. Total reactor coolant flow is calculated by each RPS protective channel from the differential pressure reading for each loop. A power level trip setpoint is established for each RPS protective channel based on the percentage reactor coolant flow rate multiplied by the flux to flow ratio and limited by the maximum allowed thermal power (Pmax). The value of Pmax is established to prevent exceeding the limits established by the COLR in the event that indicated reactor coolant flow increases due to instrument failure. The delta flux or imbalance (power in the top half of the core minus the power in the bottom half of the core) reduces the power level trip setpoint such that the four pump power-imbalance boundaries illustrated in Figure 7-3 are not exceeded. Less than four pump power-imbalance protection is provided by the power level trip setpoint decrease due to flow decrease. When the 2.MAX neutron flux signal exceeds the power level trip setpoints established by the total reactor coolant flow and the reactor power imbalance in two or more protective channels, a reactor trip is generated. Reference Trip #3 of Figure 7-1 for control logic.

For Units with the digital RPS installed or not installed, all flow ΔP cells for a single loop are connected to common 1-inch "low" and "high" lines from the flow tube in that loop. Severance of the "low" line will result in maximum indicated flow for the loop in all four protective channels. All console indicators for the loop will go to 110 percent full flow. Severance of the "high" line will result in zero indicated flow for the loop and possibly a power/flow reactor trip. See Section 7.4.2.3.1 for more details.

7.2.2.3.3 Power/Reactor Coolant Pumps Trip

The reactor coolant (RC) pumps are monitored to determine that they are running. Loss of a single pump initiates four independent signals, one to each protective channel. This information is received by a pump monitor logic which counts the number of RC pumps in operation and identifies the coolant loop in which

the pumps are operating. For Units with the digital RPS not installed, the pump monitor logic output controls the trip point of a power/pump comparator, and initiates a protective channel trip for the conditions in Table 7-1. Normally, the trip point corresponding to only two pumps in operation is set at approximately 2 percent full power. If two pumps are lost, a reactor trip will be initiated. For Units with the digital RPS installed, the inputs from the RC Pump monitors are processed by each RPS protective channel and a trip is generated for the conditions in Table 7-1. Reference Trip #11 of Figure 7-1 for control logic.

7.2.2.3.4 Reactor Outlet Temperature Trip

The reactor outlet temperature is measured by resistance elements.

For Units with the digital RPS installed, one of the four reactor outlet temperatures is designated for each protective channel. When the 2.MAX RTD input exceeds the predetermined setpoint, the associated protective function is automatically placed in its tripped state. When the 2.MAX reactor outlet temperature exceeds the trip setpoint in two or more protective channels, a reactor trip is generated. Reference Trip #7 of Figure 7-1 for control logic

For Units with the digital RPS not installed, the bridge for each resistance element is considered a part of, and is located within, its associated protective system channel cabinet.

The reactor outlet temperature signal from the temperature bridge passes through a signal converter and then is applied to a bistable trip module. When the temperature exceeds the trip point of the bistable, the bistable trips, de-energizing the protective channel trip relay.

7.2.2.3.5 Pressure-Temperature Trip

Figure 7-2 shows typical operating reactor coolant pressure-temperature boundaries formed by the combined reactor high temperature, high pressure, low pressure, and the pressure-temperature comparator trip settings. For Units with the digital RPS not installed, the pressure-temperature comparator trips whenever the specified reactor pressure-outlet temperature relationship is exceeded. The comparator forms the boundary line A-B in Figure 7-2.

For Units with the digital RPS installed, when reactor coolant 2.MAX or 2.MIN pressure or temperature exceeds these boundaries, a trip signal is generated within the protective channel. If two or more protective channels reach the trip condition, a reactor trip signal is generated. Reference Trip #6 of Figure 7-1 for control logic.

7.2.2.3.6 Reactor Coolant Pressure Trip

For Units with the digital RPS installed, the reactor coolant system pressure is measured by four independent pressure transmitters, one pressure input to each RPS protective channel. When the 2.MAX or 2.MIN pressure input exceeds its setpoint (high or low), the associated protective function is automatically placed in its tripped state. When the 2.MAX or 2.MIN reactor coolant pressure exceeds the trip setpoints in two or more protective channels, a reactor trip is generated. Reference Trips #4 and #5 of Figure 7-1 for control logic.

For Units with the digital RPS not installed, the reactor coolant pressure signal from the pressure transmitter is received by an isolation module in the associated protective channel cabinet. This module acts as a signal conditioner and isolation unit.

Pressure signals go to a high pressure bistable trip module and a low pressure trip module. When the pressure exceeds the trip point of the high pressure bistable, the bistable trips de-energizing the protective channel trip relay.

The low pressure bistable trips when the pressure falls below the trip point, tripping the protective channel trip relay.

7.2.2.3.7 Main Turbine Trip

Pressure switches monitoring the hydraulic fluid pressure in the Turbine Emergency Trip System header will input an open indication to the RPS on turbine trip. For Units with the digital RPS not installed, contact buffers located in each RPS channel provide isolation for the RPS System from the field contacts. Upon sensing field contact change state, the contact buffer will initiate an RPS trip when a turbine trip is indicated. This trip is bypassed below a predetermined flux level for unit startup.

For Units with the digital RPS system installed, each RPS protective channel A, B, C & D monitors one of four hydraulic fluid pressure switch contact inputs. The status of these four contact inputs is shared between protective channels over fiber optic communications links. If the reactor trip function is enabled and 2-out-of-4 Main Turbine hydraulic fluid pressure switch contacts are open, then that RPS protective channel produces a trip signal. If two or more RPS protective channels are in the tripped state, a reactor trip is generated via the 2-out-of-4 reactor trip relay logic. Reference Trip #10 of Figure 7-1 for control logic. This trip is bypassed below a predetermined flux level for unit startup.

7.2.2.3.8 Loss of Main Feedwater Trip

Hydraulic oil pressure switches for each feedwater pump turbine will input an open indication to the RPS on feedwater pump turbine trip. For Units with the digital RPS not installed, isolation contact buffers in the RPS sense the field contact inputs and initiate an RPS trip when both pumps have tripped. This trip is bypassed below a predetermined flux level for unit startup.

For Units with the digital RPS installed, each RPS protective channel A, B, C & D monitors both feedwater pump turbines hydraulic oil pressure switch contact inputs. The status of these eight contact inputs is shared between protective channels over fiber optic communication links. If the reactor trip function is enabled and both feedwater pump turbines are tripped, then that RPS protective channel produces a trip signal. If two or more RPS protective channels are in the tripped state, a reactor trip is generated via the 2-out-of-4 reactor trip relay logic. Reference Trip #9 of Figure 7-1 for control logic. This trip is bypassed below a predetermined flux level for unit startup

7.2.2.3.9 Reactor Building Pressure Trip

Each of the four protective channels receives Reactor Building pressure information from an independent pressure switch. For Units with the digital RPS not installed, a contact buffer in each protective channel continuously monitors the state of the associated pressure switch. When the state of the pressure switch changes to that corresponding to a Reactor Building pressure exceeding the trip point specified in Table 7-1, the contact buffer de-energizes the protective channel's trip relay.

For Units with the digital RPS installed, a 2-out-of-4 logic scheme is used within each RPS Protective Channel. The 2-out-of-4 logic within each RPS protective channel looks for a second open contact from the pressure switches to initiate a protective channel trip. This logic eliminates a single failure from tripping an RPS protective channel and will only provide a reactor trip when there is valid Reactor Building High Pressure (2-out-of-4). A single open contact will be annunciated via the respective protective channel's Trouble Statalarm and via the OAC computer. Reference Trip #8 of Figure 7-1 for control logic

7.2.2.4 Setpoint Adjustments for Single Loop Operation

Following amendments 165/165/162 to the facility operating license, single loop power operation is prohibited.

7.2.2.5 Availability of Information

The reactor trip components associated with a single protective channel are wholly contained within two RPS cabinets.

For units with the digital RPS installed:

All system analog and digital input signals are monitored by the plant computer. Separate from the computer, equipment failures and trip actions are sequence-annunciated in the plant status annunciator. Such sequencing permits the operator to readily identify the protective channel trip actions. Process information including power, imbalance, flow, temperature, and pressure is also available on the main control console.

Plant annunciator windows provide the operator with immediate indications of changes in the status of the RPS. The following conditions are annunciated for each RPS protective channel:

1. channel trip
2. channel trouble
3. channel on test
4. NI power supply failure
5. shutdown bypass initiated
6. manual bypass initiated

Any time a test switch is in other than the operate position, a test annunciator will be lit and the associated protective channel must be administratively declared out of service.

The digital RPS system communicates with the plant OAC and annunciators through the Monitoring and Service Interface (MSI). The MSI has three communication functions which are to: provide unidirectional data to the OAC, provide bidirectional data to the Service Unit, and provide isolated communication between the safety related digital RPS and the non-safety plant systems such as annunciators and the ICS. The Graphical Service Monitor (GSM) resides on the Service Unit and provides an interface into the digital RPS for testing and maintenance. The OAC is sent unidirectional data through a gateway which provides real time information to the OAC. Reference Figure 7-1, pg 16 for a diagram of the MSI interface.

For units with the digital RPS not installed, within the cabinets, there is a meter for most of the analog signals employed by the protective channel, and a visual indication of the state of every logic element. The exceptions to having local meters for indication of the analog signals are the RC flow and flux imbalance signals. This information may be obtained by connecting the calibration test computer to the cabinet hardware. At the top of one cabinet, and easily visible at all times, is a protective channel status panel. Lamps on this panel give a quick visual indication of the trip status of the particular protective channel and of the RT module associated with it. Additional lamps on the panel give visual indication of a channel bypass or a fan failure.

In addition to the visual indications and readouts within the protective channel cabinets, each trip function, power supply, and analog signal is monitored by the plant computer. Separate from the computer, trip actions are sequence-annunciated in the plant status annunciator. Such sequencing permits the operator to identify readily the protective channel trip actions. Process instrumentation including power, imbalance, flow, temperature, and pressure is indicated on the main control console.

Plant annunciator windows provide the operator with immediate indications of changes in the status of the Reactor Protective System. The following conditions are annunciated for each Reactor Protective System channel:

1. channel trip
2. fan failure in channel
3. channel on test
4. shutdown bypass initiated
5. manual bypass initiated
6. dummy bistable installed

Any time a test switch is in other than the operate position, annunciator (3) will be lit and the associated protective channel will be tripped. Under this condition, annunciator (1) will be lit unless annunciator (5) is lit (i.e., the channel is bypassed).

7.2.3 System Evaluation

7.2.3.1 System Logic

The RPS is a four-channel, redundant system in which the four protective channels are brought together in four identical 2-out-of-4 logic networks of the reactor trip components. Reactor trip components are Reactor Trip Modules (RTM) for Units with the digital RPS not installed. For Units with the digital RPS installed, the Reactor Trip Component is made up of two digital output modules and four Reactor Trip Relays (RTR) all contained within the respective RPS channel's cabinet. The RTC receives a channel trip signal in its own channel and channel trip signals from the digital output modules in the other three RPS channels. A trip in any 2 of the 4 protective channels initiates a trip of all four logic networks. The system to this point has the reliability and advantages of a pure 2-out-of-4 system.

Each of the reactor trip components (2-out-of-4 logic networks) controls a control rod drive breaker. A trip in any 2 of the 4 protective channels initiates a trip of all the breakers. The breakers are arranged in what is effectively a 1-out-of-2 logic taken twice (Figure 7-4). This system combines the advantages of the 2-out-of-4 and the 1-out-of-2 x 2 systems. The combination results in a system that is considered superior to either of the basic systems alone.

In evaluating system performance, it is arbitrarily assumed that "failure" can either prevent a trip from occurring or can initiate trip action.

The redundant Reactor Protective System inputs operate in a true 2-out-of-4 logic mode so that the failure of an input leaves the system in either a 2-out-of-3 or a 1-out-of-3 logic mode, with either state providing sufficient redundancy for reliable performance.

The system can tolerate several input function failures without a reduction in performance capability provided the failures occur in unlike variables in different protective channels, or are of a different mode in different protective channels, or all occur within one protective channel. When a single protective channel fails, the system is left in either a 2-out-of-3 or 1-out-of-3 logic mode as explained below.

The protective channel trip relay of each channel is located in the reactor trip component associated with the channel. Within each reactor trip component, there is a logic relay for each protective channel. These combine in each reactor trip component to form the 2-out-of-4 logic. A Failure Mode and Effects analysis of the reactor trip component has demonstrated that single failures within the reactor trip component or interconnections can produce only the following effects:

1. Trip the breaker associated with the reactor trip component.

2. Place the system in a 2-out-of-3 mode, as if the associated protective channel had a "cannot" trip failure.
3. Place the system in a 1-out-of-3 mode, as if the associated protective channel had tripped.

The combination of reactor trip components and control rod drive breakers form a 1-out-of-2 x 2 logic. At this level the system will tolerate a "cannot trip" type of failure of one reactor trip component, or of the breaker associated with one reactor trip component without degrading the system's ability to trip all control rods. The failure analysis demonstrates that no single failure involving a reactor trip component will prevent its associated breakers from opening.

7.2.3.2 Redundancy

The design redundancy of the Reactor Protective System allows the loss of a single protective channel. If that protective channel is in the Trip state, the remaining components and protective channels are operational in a 1-out-of-3 system logic. If that protective channel is in Manual Bypass, the remaining components and protective channels are operational in a 2-out-of-3 system logic.

7.2.3.3 Electrical Isolation

For Units with the digital RPS not installed, all signals leaving the Reactor Protective System are isolated from the system either by the use of isolation amplifiers for analog signals, by relay contacts (in the case of digital signals), or by optical isolators for the BWNT STAR hardware and relay contacts. The effect of this isolation is to prevent faults occurring to signal lines outside of the Reactor Protective System cabinets from being reflected into more than one Protective channel. The isolation thus provided also assures that two or more protective channels cannot interact through the cross-coupling or faulting of related signal lines.

Faults such as short, open, or grounded circuits and cross-coupling of analog output signals from two or more channels have no effect upon the protective channels or their functions.

The isolation amplifier circuits have been prototype tested to assess their effectiveness to isolate the input signal from output circuit faults. They are capable of blocking a direct connection (i.e., a hot short) across their output of 410 vdc (300 v rms) without affecting the input source. The redundancy and coincidence logic of the system permits the system to tolerate failures and thus reduces the chance of an inadvertent reactor trip. The BWNT STAR hardware for the Flux/imbalance/flow trip string uses optical isolators rated at 500 VAC, ± 700 VDC galvanic isolation.

For Units with the digital RPS installed, electrical isolation is inherent in the use of fiber-optic data links. In order to maintain electrical independence when input signals are shared between channels, a TXS communication link module is used to convert the signal from hard wire to fiber optic. The fiber optic communication equipment is qualified as Class 1E isolation and provides the required electrical separation between each protective channel. Fiber optic communication equipment is also used between protective channels and the Monitoring and Service Interface (MSI). Fiber optic isolation prevents internal electrical faults from propagating from one protective channel to other redundant channels.

All signals leaving the RPS to non-qualified systems (such as ICS) utilize qualified signal isolators to protect against faults occurring external to RPS.

Each input/output interface type was tested in both differential (across input/output) and common (input/output to ground) modes. Fault signals of 600 VAC and 250 VDC were applied for 30 seconds. This testing verified the digital RPS operation was not affected by the simulated faults.

7.2.3.4 Periodic Testing and Reliability

For Units with the digital RPS not installed, the use of 2-out-of-4 logic between protective channels permits a channel to be tested on-line without initiating a reactor trip. Maintenance to the extent of removing and replacing any module within a protective channel may also be accomplished in the on-line state without a reactor trip.

To prevent either the on-line testing or maintenance features from creating a means for unintentionally negating protective action, a system of interlocks initiates a protective channel trip whenever a module is placed in the test mode or is removed from the system. However, provisions are made in each protective channel to supply an input signal which leaves the channel in a non-tripped condition for testing or maintenance.

The test scheme for the Reactor Protective System is based upon the use of comparative measurements between like variables in the four protective channels, and the substitution of externally introduced digital and analog signals as required, together with measurements of actual protective function trip points.

On-line testing may be performed at different intervals and levels within the system consistent with satisfactory system reliability characteristics. The reliability of the system for random failures has been assured by careful selection of components, failure testing of logic elements, environmental testing of the system's modules, and long-term prototype proof-testing with the Babcock and Wilcox Test Reactor (BAWTR).

The reliability of the system logic, primarily the relays and coincidence networks in the RT modules, has been made very high so as to eliminate the need for frequent tests of the logic. The logic relays are of two classes; one class designed for high speed, light electrical loads, and more than 10^7 operations under load; and the other class for switching electric loads of up to 10 amperes and more than 10^6 operations. Confirmation tests of operational reliability of these two types of relays, operated under load as they are used in the RPS, have been performed with no sign of failure or wear to 5×10^6 and 1.2×10^6 operations respectively.

The system test scheme includes frequent visual checks and comparisons within the system on a regular schedule in which all protective channels are checked at one time, together with less frequent electrical tests conducted on a rotational plan in which tests are conducted on different protective channels at different times.

A regular check of all Reactor Protective System indications is required. The check includes such things as comparing the value of the analog variables between protective channels and observing that the equipment status is normal. In addition, power-range protective channel readings are compared with a thermal calculation of reactor power. These checks are designed to detect the majority of failures that might occur in the analog portions of the system as well as the self-annunciating type of failure in the digital portions of the system. The electrical tests are designed to detect more subtle failures that are not self-evident or self-annunciating and are detectable only by testing.

Electrical tests are conducted on a rotational basis in accordance with a preliminary test scheme as follows:

1. Prior to startup (following a refueling outage), all Reactor Protective System channels, logic, and control rod drive power breakers are electrically trip tested to prove their operability. Testing is performed on a 45 day staggered test bases, for example:
2. 45 days after startup, protective channel A is electrically trip tested for every input up to and including the channel trip relay.
3. 90 days after startup, protective channel B is similarly tested.
4. 135 days after startup, protective channel C is similarly tested.

5. 180 days after startup, protective channel D is similarly tested.
6. 225 days after startup, protective channel A is similarly tested.

The rotational cycle is repeated so that a different protective channel is electrically trip tested every 45 days.

The control rod drive breaker associated with a reactor trip module is tested monthly.

Rotational testing has several advantages. It significantly reduces the probability of system failure as compared to testing all protective channels at one time. It also reduces the chance of systematic errors entering the system.

For Units with the digital RPS installed, the use of 2-out-of-4 logic between protective channels permits a channel to be tested online without initiating a reactor trip. Test circuits are supplied which utilize the redundant, independent, and coincidence features of the Protective Systems. This makes it possible to manually initiate online trip signals in any single protective channel in order to test trip capability in that channel without affecting the other protective channels. Surveillance requirements have been established for performance of protective channel calibrations and protective channel functional testing.

The digital RPS provides continual online automatic monitoring of each of the input signals in each channel, performs a signal online validation, and provides functional validation of hardware performance. The digital RPS has a Graphical Service Monitor (GSM) which supplies individual screens for monitoring and recording the analog and binary inputs during Protective Channel Calibration tests. To prevent adverse system actions, the analog or binary signals may be placed in Bypass using the GSM Trip/Bypass screens. There are also screens to exercise the reactor trip logic, statalarms, and events recorder. Each protective channel is provided with a key-operated Parameter Change Enable keyswitch. The system software controls access to the computer from each protective channel by controlling the operating modes of the computer. Under normal operating conditions, the computer is in the OPERATION mode. The PARAMETERIZATION Mode allows changes to specific parameters or performance of tests from the GSM screens. Permission to change from the OPERATION mode into the PARAMETERIZATION mode is provided by the Parameter Change Enable Keyswitch. After the permissive is provided from a system processor via its Keyswitch, communication from the Service Unit to that processor is allowed to change its operating mode. Placing the PROCESSOR into the FUNCTION TEST and DIAGNOSTIC modes requires first enabling the PARAMETERIZATION Mode with the keyswitch and then setting a separate parameter to enable these modes with the GSM. The FUNCTION TEST Mode allows disabling the application function and forcing the output signals (normally not used). The DIAGNOSTIC Mode allows download of new application software. The FUNCTION TEST and DIAGNOSTIC modes result in the processor ceasing its cyclic processing of the application functions. The Parameter Change Enable Keyswitches are administratively controlled (no hardware or software interlocks are provided). When a keyswitch is placed in the Parameter Change Enable Mode Position for any activity, the affected processor shall first be declared out of service. In addition to declaring the processor out of service (1) the affected RPS channel shall be bypassed and (2) either the affected ESPS input channel (A1, B1, or C1) shall be tripped OR the ESPS Set 1 voters shall be placed in Bypass for the following activities:

- Loading or revising the software in a processor.
- Changing parameters via the RPS High Flux Trip (Variable Setpoint) screen at the Service Unit.
- Changing parameters via the RPS Flux/Flow/Imbalance Parameters screen at the Service Unit.

Only one RPS channel at a time is allowed to be placed into Parameter Change Enable Mode Position for these activities. Parameter Change Enable Keyswitch status information is sent to a statalarm and is also sent to the OAC via the gateway.

The test scheme for the Reactor Protective System is based upon the use of comparative measurements between like variables in the four protective channels. Trip action is taken when the 2.MAX or 2.MIN value for analog signals or two out of four for binary inputs, based on the trip being tested, exceeds the actual protective function trip points. The alarms for the trip function for the channel under test will actuate when the trip condition for that channel's input is met.

The reliability of the system has been made very high so as to eliminate the need for frequent tests of the logic. The system software is not susceptible to transient, random, aging, or environmental related faults since it does not fail in the conventional sense. It can be reasonably expected to exhibit no degradation from these factors. The cyclic self-monitoring routine verifies that the code is not corrupted. The Mean Time Between Failure (MTBF) data for the Teleperm XS equipment calculates MTBF rates from 29 years to 267 years at 40°C (Reference 6).

All RPS protective channels, logic, and control rod drive power breakers are tested to demonstrate operability. Protective Channel Functional Testing, which is part of the Channel Calibration, is performed every refueling outage. The digital RPS software performs a continuous online automated cross Channel Check, separately for each protective channel, and continuous online signal error detection and validation. The combination of the self-testing features and the reliability of the TXS equipment support a protective channel functional test frequency of refueling outage. The setpoints in the software are manually verified every 92 days. The protective channel interposing relays are manually actuated every 92 days. Digital RPS logic is re-verified every refueling outage by rebooting the channel computer and checksums are verified at that time.

The control rod drive breaker associated with a reactor trip component is tested prior to startup from a refueling outage and monthly during the fuel cycle.

In addition, power range protective channel readings are compared with a thermal calculation of reactor power. This check, the Channel Checks, and the continuous online self-monitoring of the system are designed to detect the majority of failures that might occur in the analog portions of the system as well as the self-annunciating type of failure in the digital portions of the system.

The periodic electrical tests are designed to detect more subtle failures that are not self-evident or self-annunciating and are detectable only by testing.

7.2.3.5 Physical Isolation

The need for physical isolation has been met in the physical arrangement of the protective channels within separate cabinets and wiring within the cabinets separating power and signal wiring so as to reduce the possibility of some physical event impairing system functions. The systems sensors are separated from each other. There are four pressure taps for the reactor coolant pressure measurements to reduce the likelihood of a single event affecting more than one sensor. Outside the Reactor Protective System cabinets, vital signals and wiring are separated and physically protected to preserve protective channel independence and maintain system redundancy against physical hazards.

Redundant detectors and transmitter applied in the Reactor Protective System are located to provide physical separation. Redundant out of core nuclear detectors are located in separate quadrants around the reactor vessels. Two resistance thermometers assigned to the RPS are located on each reactor coolant outlet header. Cables approach redundant temperature detectors from opposite directions. Redundant pressure transmitters are located outside the secondary shield in four separate quadrants of the Reactor Buildings. Two reactor coolant pressure transmitters for RPS are connected to each of the two loops. Separate flow transmitters for each RPS channel are applied to sense the flow in each loop. This arrangement results in detectors and transmitters associated with one RPS channel being located in essentially (the reactor vessels are not in the center of the Reactor Buildings) the same quadrant of a Reactor Building, and with redundant detectors and transmitters located in another quadrant of the

Reactor Building. Since each RPS channel receives a flow signal from both loops, one of the flow transmitters for each channel is not located with the other RPS transmitters for that channel. Location and cable routing for these transmitters is such that separation of at least seven feet is provided between redundant channels inside the Reactor Buildings. Cables for redundant RPS and ES detectors and transmitters are routed in separate directions to four separate Reactor Building penetrations in trays carrying only nuclear instrumentation, RPS, ES, and accident monitoring instrumentation. These penetration assemblies are assigned to nuclear instrumentation, ES instrumentation, accident monitoring instrumentation, and RPS cables exclusively. Two of these penetration assemblies are located sixty feet apart in separate quadrants of each Reactor Building. One is used for RPS and ES channel A instrumentation; the other for RPS and ES channel B instrumentation. A penetration assembly for RPS and ES channel C instrumentation and one for RPS channel D are located on the opposite side of the Reactor Buildings thirty feet apart. Located under the control rooms between the outside of the Reactor Buildings and the cable and equipment rooms, four separate trays are provided per unit which carry nuclear, RPS, ES, and accident monitoring instrumentation cables. Three separate routes are followed by these trays. RPS channel C and RPS channel D follow the same route but are separated vertically by 1-1/2 feet. A detailed review of cable tray and pipe routing in this area indicates that no more than two RPS channels could be damaged by a single pipe failure or missile. Equipment locations in the Auxiliary Building provide the basis for vertical arrangement of trays following the same route from the Reactor Buildings. Switchgear for power equipment is located at lower elevations and instrumentation cabinets are located at higher elevations. Therefore, vertical separation of classes of cables in trays is as follows from top trays down:

1. Instrumentation cable trays
2. Control cable trays
3. Power and control cable trays
4. Power cable trays

Cables from each protective channel are routed in trays separate from those carrying cables from any other protective channel with the exception of fiber optic cables used for interchannel communication. Included in these trays are instrumentation cables from the Reactor Building, control and interconnecting cables associated with that protective channel, and non-protective instrumentation and control cables. Both protective and non-protective cables are individually armored, with the exception of fiber optic cables, and are flame retardant.

Reactor trip cables from the four RPS cabinets are routed separately to a reactor trip switch located on the main control board. From the trip switch, the cables follow four separate paths to the reactor trip breakers and the control rod drive cabinets.

Where overfill situations exist in the Unit 1, 2, and 3 Cable Rooms, and dedicated trays cannot be provided for individual channels, trays are allowed to carry protective and non-protective mutually redundant cable provided separation is maintained by distance (minimum of five inch air gap) or by barriers the continuous length where the cables are adjacent in the tray.

7.2.3.6 Primary Power

The primary source of 120V ac power for the Reactor Protective System comes from four vital buses, one for each protective channel, as described in Section 8.3.2.1.4.

7.2.3.7 Manual Trip

Manual trip may be accomplished from the control console by a trip switch. This trip is independent of the automatic trip system. Power to the control rod drive breakers' undervoltage coils comes from the

reactor trip components (digital output modules and Reactor Trip Relays for Units with the digital RPS installed and Reactor Trip Modules for Units with the digital RPS not installed). The manual trip switch contacts are between the reactor trip component output and the breaker undervoltage coils. Opening of the switch contacts opens the lines to the breakers' undervoltage coils, tripping them. There is a separate set of switch contacts in series with the output of each reactor trip component. All switch contacts are actuated through a mechanical linkage from a single pushbutton.

7.2.3.8 Bypassing

For Units with the digital RPS installed:

Each protective channel is provided with two key-operated bypass switches: Shutdown Bypass and Manual Bypass keyswitches. Software bypasses are available for the protective channels and individual input signals within a protective channel. These can be set via the Graphical Service Monitor (GSM) and the Change Enable keyswitch.

The RPS Shutdown Bypass feature allows the following RPS protective functions for a protective channel to be bypassed:

- Low RCS Pressure Trip

Variable Low RCS Pressure (based on RCS Temperature) Trip

- Flux/Flow/Imbalance Trip
- Reactor Coolant Pump/Power Monitor Trips

The RPS Shutdown Bypass function also initiates reductions to setpoints for the following RPS protective functions:

- Nuclear Overpower (High Neutron Flux)
- Reactor Coolant System High Pressure

This function provides the capability to perform control rod drive system testing after the reactor has been shut down and reactor coolant system pressure has been reduced. The RPS Shutdown Bypass keyswitches are administratively controlled (no hardware or software interlocks). All RPS Protective Channels may be placed in Shutdown Bypass as required. The RPS Shutdown Bypass keyswitch status information is sent to the Statalarm panels. Status information is also sent to the OAC via the Gateway.

The software bypass feature allows the following functions to be bypassed:

- Each of the protective channels as listed above
- Individual protective channels of Neutron Flux Power Range
- Individual protective channels of Reactor Coolant Hot leg Temperature
- Individual protective channels of Reactor Coolant Flow
- Individual protective channels of Reactor Coolant Pressure
- Individual protective channels of Reactor Building Pressure
- Individual protective channels of Main Feedwater Pump Turbine Trip
- Individual protective channels of Main Turbine Trip
- Individual protective channels of Reactor Coolant Pump/Power Monitor Trip

This function allows an individual input which has failed to be bypassed instead of bypassing an RPS channel. The system logic associated with the parameter which has one input bypassed would default to 2 out of 3 coincidence logic while the system logic associated with the remainder of the inputs would still maintain 2 out of 4 coincidence logic.

The Manual Bypass allows putting a complete RPS protective channel into bypass for maintenance activities. This includes the powerdown of the protective channel computer for each protective channel. If the Manual Bypass keyswitch is in the "ON" position, it provides 24V to the relays of the hardwired "2-out-of-4" trip logic in parallel to the output of the computer. This assures that the four output TRIP relays remain energized independent of the status of the TXS computer. It also sets the FAULT status of all input signals prior to sending input signal data to the other protective channels, via the fiber optic communication data links. Thus, during testing with an RPS channel in Manual Bypass, the system will operate in 2-out-of-3 coincidence logic. The Manual Bypass keyswitches are administratively controlled (no hardware or software interlocks are provided). Administrative control allows only one RPS Protective Channel in Manual Bypass at a time. Only one Manual Bypass key is available for each unit. Manual Bypass switch status information is sent to the Control Room Annunciators. Manual Bypass switch status information is also sent to the OAC via the Gateway.

For Units with the digital RPS not installed, each protective channel is provided with two key-operated bypass switches, a channel bypass switch and a shutdown bypass switch.

The channel bypass switch enables a protective channel to be bypassed without initiating a trip. Actuation of the switch initiates a visual alarm on the main console which remains in effect during any channel bypass. The key switch will be used to bypass one protective channel during on-line testing. Thus, during on-line testing, the system will operate in 2-out-of-3 coincidence. The use of the channel bypass key switch is under administrative control.

The shutdown bypass switch enables the power/imbalance/flow, power/RC pumps, low pressure, and pressure-temperature trips to be bypassed allowing control rod drive tests to be performed after the reactor has been shut down and depressurized below the low reactor coolant pressure trip point. Before the bypass may be initiated, a high pressure trip bistable, which is incorporated in the shutdown bypass circuitry, must be manually reset. The setpoint of the high pressure bistable (associated with shutdown bypass) is set below the low pressure trip point. If pressure is increased with the bypass initiated, the channel will trip when the high pressure bistable (associated with shutdown bypass) trips. The use of the shutdown bypass key switch is under administrative control.

For maintenance purposes, a bistable may be removed from the system and a dummy bistable inserted in its place, thus bypassing the original function. Installing a dummy bistable forces the protective channel into a trip state upon removal of the bistable. Thus, the removal and substitution cannot be performed without passing through a tripped condition. The installation of the BWNT STAR hardware in the flux/imbalance/flow (fif) trip string requires the use of jumpers to bypass the trip string. The installation of jumpers to bypass the fif trip does not require the removal of the STAR processor module, therefore, the protective channel is not forced into a tripped condition. The use of dummy bistable modules and jumpers is under administrative control.

7.2.3.9 Post Trip Review

Post trip review data and information capabilities are provided by use of time history and sequence of events recording equipment. Time history data is provided by the transient monitoring application of the Process Monitoring Computer system (PMC). Sequence of events is determined by data from the sequence of events recorder (SER), the OAC, and the PMC system. This equipment, along with OAC input and operator interviews, provides sufficient information on plant parameters to assure that the course of the reactor trip can be reconstructed as well as provide root cause determination. In the event of failure of the PMC system, information necessary to conduct a post-trip review or transient investigation

can be retrieved from other independent sources, such as the OAC and control room chart recorders. See Reference 1 and Section 7.7.2.

7.2.4 References

1. H. B. Tucker letter to H. R. Denton (NRC), November 4, 1983. Response to Generic Letter 83-28.
2. SER on GL 83-28, Item 1.1, Post Trip Review (Program Description and Procedure), May 15, 1985.
3. H. B. Tucker letter to J. F. Stolz (NRC), February 27, 1986. Response to GL 83-28, Item 1.2, Data and Information Capabilities.
4. SER on GL 83-28, Item 1.2, Post Trip Review (Data and Information Capability), September 11, 1986.
5. 10CFR50.59 USQ Evaluation, dated November 21, 2000, "Duke/ONS Commitment to GL 83-28…".
6. AREVA Document 32-5061241, Oconee Nuclear Station, Unit 1, 2, and 3 RPS/ESFAS TXS Upgrade Availability Analysis (OM 201.N-0028-007)
7. Safety Evaluation Report for RPS/ESPS Digital Upgrade dated January 28, 2010, by the Office of NRR related to Amendment Numbers 366, 368, and 367 to renew Facility Operating Licenses DPR-38, DPR-47, and DPR-55, Oconee Nuclear Station Units 1, 2, and 3 Docket Numbers 50-269, -270,-287

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.2.

7.3 Engineered Safeguards Protective System

Deleted Paragraph(s) per 2009 Update

The Engineered Safeguards Protective System (ESPS) monitors parameters to detect the failure of the Reactor Coolant System and initiates operation of the High and Low Pressure Injection Systems, the Building Isolation, the Reactor Building Cooling and the Reactor Building Spray Systems. In addition, the signal is used to start the standby power source and initiate a transfer to the standby power source when required as described in Section 8.3.1.1.3.

7.3.1 Design Bases

The design basis of the system includes the items of Section 7.1.2 with the following additions:

7.3.1.1 Loss of Power

For Units with the digital ESPS installed:

1. The loss of vital bus power to an ESPS protective channel will not cause an automatic trip.
2. A loss of power to an input module of an input channel results in the associated signals being faulted.
3. The ESPS voters require power to energize the associated protective relays therefore loss of power to either the ODD or EVEN voter cabinets would result in the inability to automatically actuate the associated ESPS ODD or EVEN train.

For Units with the digital ESPS not installed:

1. The loss of vital bus power to the instrument strings will, with the exception of Reactor Building Spray, initiate a trip of that portion of the logic associated with the affected instrument string.
2. The loss of vital bus power to the system logic will not initiate system actuation.

7.3.1.2 Equipment Removal

For Units with the digital ESPS installed:

1. Removal of an output card or computer card from the digital ESPS will result in an alarm but will not automatically initiate a protective channel trip.
2. Removal of a module in an ESPS protective channel while online does not inhibit the overall system functional design performance in other channels and will not initiate a system actuation.

For Units with the digital ESPS not installed:

1. Removing modules from an instrument string will, with exception of Reactor Building Spray, initiate a trip in that portion of the logic associated with the affected instrument string.
2. Removing logic modules from one protective channel does not affect any other protective channel and does not initiate system action.

7.3.1.3 Control Logic of ESF Systems

All systems receiving the ES signal remain in the emergency mode required by the ES actuation after the signal is reset. A separate deliberate action is required to shut off the ES systems and power supplies.

The following systems have been modified to conform to the above requirement of I.E. Bulletin 80-06:

1. HPI Pumps
2. Penetration room exhaust fans
3. Reactor Building Cooling Unit fans
4. Keowee Start

7.3.2 System Design

7.3.2.1 System Logic

For Units with the digital ESPS installed:

The ESPS is a digital protective system which employs 2-out-of-3 coincidence logic to actuate engineered safeguards functions in the event that Reactor Coolant System pressure or reactor building pressure setpoints are exceeded. The functions include signal acquisition, data-processing, and actuation signal voting. The digital ESPS processes both analog and contact signals from the field for input into the ESPS instrument input channels. The input processors perform software logic and parameter checks on the analog and contact input signals and provide software logic outputs to the other ESPS instrument input channels as well as to the actuation logic channels. Each input variable is measured by three process sensors; the three redundant signals are processed within the input channel and voter processors, which provide an ESPS channel actuation through a set of output Ro relays (Ro1 and Ro2). The eight actuation logic channels are split between ODD and EVEN voters as shown in Figure 7-5, pg. 2. Either of the two voters is independently capable of initiating the required protective action through redundant equipment. The 2.MAX or 2.MIN (depending on the analog trip) is selected to compare to the trip setpoint. For binary inputs a 2 out of 3 trip logic is used to actuate the trip.

The digital ESPS processes both analog and contact signals from the field for input into the three ESPS instrument input channels. These three input channels are shared by 2 redundant ESPS Subsystems. Subsystem 2 operates in the ESPS cabinets and is designated as A2, B2 and C2. Subsystem 1 is designated as A1, B1 and C1 and operates in the Reactor Protective System (RPS) channel cabinets A, B, and C. Each of the ESPS and RPS processors performs software logic and parameter checks on the same analog and contact input signals and provides software logic outputs to the other instrument input channels as well as to the ESPS voter subsystems.

The ESPS subsystems are interconnected via fiber-optic data links. This provides a means to exchange data between subsystem inputs , which are used for signal validation, fault and deviation detection, and trip actuation. Alarms are initiated when signals fail validation tests or when failures or abnormal deviations are detected. Analog signals are faulted when extremely low signals (significantly below off-scale) are detected, indicating transmitter failure or power supply failure. If inter-channel communications are lost, the associated signals are faulted as well. Faulted signals are eliminated from use in the signal selection logic. An additional level of reliability is provided through the utilization of second maximum (2.MAX) and second minimum (2.MIN) signal selection functions for analog inputs and 2-out-of-3 selection logic for contact inputs. These functions reduce the probability of using an erroneous signal for determining trip conditions.

Independence is maintained in the subsystem inputs which are interconnected via fiber-optic data links. If interchannel communications are lost, the associated signals are faulted as well. Faulted signals are eliminated from use in the signal selection logic. With only the hardwired signal as valid, the signal is passed directly to the subsequent logic, thus ensuring instrument input channel independence. The 2.MAX and 2.MIN signal selection functions are used for analog inputs, and 2-out-of-3 selection logic is used for contact inputs. The 2.MAX and 2.MIN functions remain until less than two valid signals are

present. The 2-out-of-3 logic function reduces to a 2-out-of-2 logic for any condition that causes an input signal fault, including loss of power.

The ODD/EVEN voter designation is associated with redundant actuation devices. The ODD1 and ODD2 voters provide output to ESPS actuation logic channels 1, 3, 5 and 7. The EVEN1 and EVEN2 voters provide output to ESPS actuation logic channels 2, 4, 6 and 8. There is an ODD/EVEN subsystem 1 and an ODD/EVEN subsystem 2, which correspond to the ESPS instrument input channels which provide signals to them. Voters ODD1 and EVEN1 receive input from ESPS instrument input channels A1, B1 and C1. Voters ODD2 and EVEN2 receive input from ESPS instrument input channels A2, B2 and C2. Either voter subsystem is capable of performing all required protective actions.

The instrument input channel trip signals are provided to the voters via fiber-optic data links. The voters use 2-out-of-3 logic on these trip signals for actuating the Ro relays.

The logic reduces to 2-out-of-2 for any condition that causes an input signal fault, including loss of power.

In addition, each voter (ODD1, EVEN1, ODD2 and EVEN2) is made up of a master and a checker processor, or 8 processors total. Each processor utilizes the same input information and executes the same software in performing an independent 2-out-of-3 logic for actuating the Ro relays (Ro1 and Ro2). At the end of each processing cycle, prior to sending output commands to redundant digital output boards that energize separate Ro relays, the master and checker processors compare results. If a calculation mismatch occurs between the Master and Checker processors, the respective subsystem automatically disables all of its output modules by shutting down the power supply to the output modules, generates an alarm, and initiates a reboot of the voter subsystem. This reduces the possibilities for inadvertently actuating the output Ro relays and subsequently energizing the Engineered Safeguards equipment when not required. Contacts from Ro1 and Ro2 are wired in series to prevent spurious actuation due to digital output board failure. Reference Figure 7-5 for trip logic diagrams.

The output Ro relays are normally de-energized. The contacts of the Ro relays are normally open within the control circuits of the individual Engineered Safeguards equipment. An ESPS actuation energizes the Ro relays and closes the Ro contacts which in turn energizes the control relays (CR) in each of the protective device (valve, pump, etc.) control circuits.

For Units with the digital ESPS not installed, the Engineered Safeguards Protective System is a basic 2-out-of-3 coincidence logic system. Each input variable is measured three times, the three redundant signals terminate in three bistables as shown in Figure7-5, pg. 1.

The Engineered Safeguards Protective System consists of eight 2-out-of-3 coincidence logic networks for actuating the equipment in four safeguards systems, thus each system is actuated by a pair of 2-out-of-3 logic and its outputs are referred to as an Engineered Safeguards Protective System channel. Each safeguards system is therefore actuated by two redundant coincidence logics or protective channels.

The coincidence logic output is normally de-energized. Trip action consists of closing the electrical path through the logic.

The output of the protective channel coincidence logic is connected to the channel's unit control module (UC modules). There is one UC module for every item, (pump, valve, etc.) controlled by the protective channel. A protective channel's UC modules are connected in parallel with the output of the coincidence logic.

The output of the coincidence logic follows a normally closed path in each UC module, finally terminating in an output relay, Ro, within each module. The Ro relays of a protective channel's UC modules are driven in parallel with the output of the protective channel coincidence logic.

The contacts of the Ro relay are normally open across a control line terminating in a control relay, CR, in the controller of the equipment assigned to the individual UC module. Power for operating the CR

relay is taken from the equipment controller in series with the Ro relay contacts. Trip action involves energizing the Ro relay, closing its contacts which in turn energizes the CR relay actuating the assigned equipment.

Each protective channel is equipped with a logic test module (LT module). The LT module, together with the UC module, provides the necessary circuitry to permit trip testing of an individual protective device without tripping an entire protective system or channel.

The UC module also provides a means whereby following a system trip, an individual protective device may be removed from the control of the Engineered Safeguards Protective System and returned to manual control. This block action cannot be initiated prior to a system trip.

The design of the system's logic can be summarized in terms of the systems operation as follows:

1. Each protective action is initiated by either of two protective channels with 2-out-of-3 coincidence between input signals.
2. Protective action is initiated by applying power from the protective channel logic to the individual Ro relays in the UC modules, which in turn energize the CR relays in each protective device controller.
3. There is a UC module for every safeguards system component (valve, pump, etc.)

7.3.2.2 High and Low Pressure Injection and Reactor Building Non-Essential Isolation Systems

For Units with the digital ESPS system installed, there are three independent reactor coolant pressure sensors and three independent reactor building pressure sensors which provide input to the ESPS. Reactor coolant pressure and the reactor building pressure inputs are monitored by two independent digital processing systems. The non-faulted inputs are combined within the ESPS into 2-out-of-3 coincidence logic for initiating High Pressure Injection (HPI) system, Low Pressure Injection (LPI) system and Reactor Building Non-Essential Isolation actions. System Logic for ESPS is described in Section 7.3.2.1 and is shown in Trips #1 and #2 of Figure 7-5.

The instrumentation, logic, and actuation of the High Pressure Injection (HPI) and Low Pressure Injection (LPI) Systems are identical in design. The systems differ only in their actuation setpoints.

During reactor operation, HPI and the Reactor Building Non-Essential Isolation will initiate if 2-out-of-3 of the reactor coolant pressure sensors indicate a decrease in pressure below the RCS Low pressure setpoint, or if 2-out-of-3 reactor building pressure sensors indicate an increase in pressure beyond setpoint. These ESPS functions start Keowee Hydro Units, provide permissives for emergency power, start the HPI pumps and align various valves. Two ESPS actuation output logic channels are initiated either of which is independently capable of initiating the required protective action.

During reactor operation, LPI and the Low Pressure Service Water System (LPSW) will initiate if 2-out-of-3 of the reactor coolant pressure sensors indicate a decrease in pressure below the RCS Low-Low pressure setpoint, or if 2-out-of-3 reactor building pressure sensors indicate an increase in pressure beyond setpoint. These ESPS functions initiate LPI and LPSW pumps and align various valves. Two ESPS actuation output logic channels are initiated either of which is independently capable of initiating the required protective action.

For Unit(s) with the digital ESPS system not installed, the instrumentation, logic, and actuation of the High and Low Pressure Injection Systems are identical in design. The systems differ only in their actuation set point.

There are three independent reactor coolant pressure sensors. The output of each sensor terminates in an isolation amplifier which provides individually isolated outputs. One output of each pressure

measurement goes to the plant computer for monitoring. One output goes to bistables, for initiating high pressure injection and Reactor Building non-essential isolation action and for low pressure injection action. The bistables are identical except for their set point. Bistable action is initiated when the low reactor coolant pressure set points are reached.

The output of the three high pressure injection and Reactor Building Non-Essential Isolation System bistables is combined in series with the trip outputs of three Reactor Building pressure bistables. The combination of reactor coolant pressure and Reactor Building pressure bistables outputs allows either variable to initiate high pressure injection and Reactor Building non-essential isolation.

The series outputs of the bistables are brought together in two identical 2-out-of-3 coincidence logics which form two Engineered Safeguards Protective System channels. Either of the two protective channels is independently capable of initiating the required protective action through redundant high pressure injection and Reactor Building Non-Essential Isolation System equipment.

The outputs of the three Low Pressure Injection System bistables are also combined in series with the independent trip outputs of the three Reactor Building pressure bistables. The combination functions in identically the same way as described for the High Pressure Injection System, with two 2-out-of-3 coincidence logics and protective channels.

7.3.2.3 Reactor Building Cooling and Reactor Building Essential Isolation System

For Units with the digital ESPS system installed, there are three independent reactor building pressure sensors which provide input to the ESPS. Reference Trip #3 of Figure 7-5 for trip logic diagram.

The non-faulted inputs are combined within the ESPS into a 2-out-of-3 coincidence logic for initiating Reactor Building Cooling (RBC) and Reactor Building Essential Isolation System actions. System Logic for ESPS is described above in Section 7.3.2.1.

RBC and the Reactor Building Essential Isolation System will initiate if 2-out-of-3 of the reactor building pressure sensors indicate an increase in building pressure above the high building pressure ESPS trip point. The second maximum of the sensor inputs is selected to compare to the trip setpoint. The three reactor building pressure inputs to ESPS are also utilized for HPI and LPI System initiations as previously discussed in Section 7.3.2.2. Two ESPS actuation output logic channels are initiated either of which is independently capable of initiating the required protective action.

This ESPS function starts RBC unit fans and penetration room fans as well as aligns certain component cooling water and LPSW valves when reactor building pressure increases above the ESPS setpoint. The Channel A Reactor Building Isolation signal is sent to the ICS to denote degraded containment conditions. The ICS is configured such that this signal is not utilized to initiate any action within the ICS.

For Unit(s) with the digital ESPS system not installed, there are three Reactor Building pressure sensors. The output of each sensor terminates in an input isolation amplifier, which provides individually isolated outputs. One isolated output of each pressure measurement goes to the plant computer for monitoring. One output of each pressure measurement goes to a bistable which initiates action when its high building pressure trip point is exceeded. Each input isolation amplifier module contains an analog meter for indicating the measured pressure. Each of the three bistables has contact outputs that are combined in series with the output of the High and Low Pressure Injection System bistables as previously described.

The outputs of the three bistables are brought together in two identical 2-out-of-3 coincidence logics which provide two Engineered Safeguards Protective System channels. Either of the two channels is independently capable of initiating the required protective action. Each protective channel uses redundant protective system devices. The bistable for Channel A Reactor Building Pressure Sensor provides a contact output to the ICS to denote degraded containment conditions.

7.3.2.4 Reactor Building Spray System

For Units with the digital ESPS system installed, reactor building pressure switch inputs are monitored by 6 pressure switches. Two sets of three switches feed two independent digital processing input channels. The non-faulted inputs are combined within the ESPS into 2-out-of-3 coincidence logic for initiating Reactor Building Spray (RBS) actions. System Logic for ESPS is described above in Section 7.3.2.1 and is shown in Trip #4 of Figure 7-5 for the trip logic diagram.

RBS will initiate if 2-out-of-3 of the reactor building pressure switches indicate an increase in building pressure above the High High building pressure ESPS trip setpoint. Two ESPS actuation output logic channels are initiated either of which is independently capable of initiating the required protective action

This ESPS function starts RBS pumps and aligns the RBS valves required for system operation.

For Units with the digital ESPS system not installed, the Engineered Safeguards Protective System channels of the Reactor Building Spray System are formed by two identical 2-out-of-3 logic networks with the active elements originating in six Reactor Building pressure sensing pressure switches.

Three independent pressure switches containing normally open contacts form one protective channel's 2-out-of-3 logic inputs. Three other identical pressure switches form the 2-out-of-3 logic inputs of the second protective channel. Either of the two protective channels is capable of initiating the required protective action.

7.3.2.5 Availability of Information

For Units with the digital ESPS installed, all system signals are monitored by the plant computer. ESPS device position status is indicated on the ES Status panels and also is monitored by the plant computer. Statalarm panel alarms provide the following ESPS conditions:

- HPI and LPI bypass permit,
- Input channel bypass for HPI and LPI,
- Input channel trip,
- Input channel trouble,
- Input channel in test,
- Manual bypass for each of voters ODD1, ODD2, EVEN1 and EVEN2,
- EVEN and ODD voter trouble,
- EVEN and ODD voter in test,
- EVEN and ODD voter in emergency override,
- Actuation output logic channel trip,

The digital ESPS provides automatic analog and binary process signal monitoring for signal failure (Fault) and for Channel Deviation, which are alarmed via the trouble alarms. If an instrument input channel fails the acceptance criteria, it is alarmed (OAC alarms & Statalarm windows) so that the Control Room Operator can take appropriate action. This feature allows automation of the channel check surveillance.

The digital ESPS system communicates with the plant through the Monitoring and Service Interface (MSI). The MSI has three communication functions which are to: provide unidirectional data to the OAC, provide bidirectional data to the Service Unit, and provide isolated communication between the safety related digital ESPS and the nonsafety plant systems such as annunciators and the ICS. The Graphical Service Monitor (GSM) resides on the Service Unit and provides an interface into the digital ESPS for

testing and maintenance. The OAC is sent unidirectional data through a gateway which provides real time information to the OAC. Reference Figure 7-1 for a diagram of the MSI.

Any time a test switch is in other than the operate position, a test annunciator will be lit and the associated protective channel must be administratively declared out of service.

For Units with the digital ESPS not installed, all system analog signals are indicated within the system cabinets and are monitored by the plant computer. All bistable outputs are indicated within the cabinets. Logic outputs are indicated within the cabinets and their state monitored by the plant computer.

Plant annunciators provide the operator with immediate indication of changes in the status of the ESPS. Included are all test switches, except those that are spring loaded to return to the operate position.

7.3.2.6 Summary of Protective Action

Actions initiated by the Engineered Safeguards Protection System are tabulated in Table 7-2. The devices actuated by the Engineered Safeguards Protection System are listed in Table 7-3. Channels indicated may be referred to applicable systems as shown in Figure 7-5. All actuated devices remain in their emergency modes after the reset of an engineered safeguards actuation signal until the devices are reset by operator action.

7.3.3 System Evaluation

The ESPS is a basic three-channel redundant system employing 2-out-of-3 coincidence between measured variables.

The system will tolerate the failure of one of three variables among either the reactor coolant pressure measurements or Reactor Building pressure measurements without losing its ability to perform its intended functions.

The High and Low Pressure Injection and Reactor Building Non-Essential Isolation Systems are actuated by either reactor coolant pressure or Reactor Building pressure, thus providing diversity in actuation. The system will tolerate single or multiple failures within one protective channel without affecting the operation of other protective channels. This is the result of keeping each of the protective channel logics independent of every other protective channel. The independence is carried through the protective channel logic and up to the final actuating CR control relay. This is best illustrated by considering the actuation arrangement for the high pressure injection pumps (Figure 7-5).

There are three High Pressure Injection System pumps which operate in the event of an accident. HP-P1A is under the control of protective channel 1, HP-P1C is under the control of protective channel 2, while HP-P1B is under the control of both channels. For Units with the digital ESPS not installed, within the motor controller of HP-PlA and HP-PlC there is a single CR control relay controlled by the Ro relay in the pump's associated Test and Block module. The operation of the protective channel logic, the Ro relay in relation to the CR relay, was described previously. For Units with the digital ESPS installed, there is a single CR control relay controlled by the Ro relays within the motor control logic for HP-PlA and HP-PlC. For Units with the digital ESPS installed or not installed, should any two of the three reactor coolant pressure variables drop below the RCS Low Pressure set point, both protective channel 1 and 2 logics will trip, energizing the appropriate CR relays, and start the pumps.

For Units with the digital ESPS not installed, within the motor controller of HP-P1B there are two independent CR relays, each controlled by separate Ro relays in separate Test and Block modules, one in channel 1 and one in channel 2. For Units with the digital ESPS installed, within the motor control logic for HP-P1B there are two independent CR relay strings, each controlled by separate Ro relays from ESPS (the Ro relays in output channel 1 and the Ro relays in output channel 2). For Units with the digital ESPS installed or not installed, the arrangement is identical to the way a

channel would control any device since all elements are independent and duplicated through the CR relay. The only common element is the power source for the CR relays which is common to the motor controller. Loss of this power prevents the motor control from operating as well as the pump. Relays that monitor actuator coils for each motor or valve control detect either an open coil or a loss of control power.

For Units with the digital ESPS installed, independence is maintained in the three instrument input channels which are interconnected via fiber-optic data links. These links provide the means to exchange data, which is used for signal validation, fault and deviation detection, and trip actuation; thus providing additional fault detection. If interchannel communications are lost, the associated signals are faulted as well. Faulted signals are eliminated from use in the signal selection logic. The 2.MAX and 2.MIN signal selection functions are used for analog inputs, and 2-out-of-3 selection logic is used for contact inputs. The 2.MAX and 2.MIN functions remain until less than two valid signals are present. When only the hardwired signal is valid, then the 2.MAX and 2.MIN functions directly pass the signal to the subsequent logic. The 2-out-of-3 logic function reduces to a 2-out-of-2 logic for any condition that causes an input signal fault, including loss of power.

The voters maintain their independence in the digital ESPS. The ODD/EVEN voter designation is associated with redundant actuation devices. The ODD1 and ODD2 voters provide output to ESPS actuation output logic channels 1, 3, 5 and 7. The EVEN1 and EVEN2 voters provide output to ESPS actuation output logic channels 2, 4, 6 and 8. There is an ODD/EVEN subsystem 1 and an ODD/EVEN subsystem 2, which correspond to the ESPS input channels which provide signals to them. Voters ODD1 and EVEN1 receive input from ESPS input channels A1, B1 and C1. Voters ODD2 and EVEN2 receive input from ESPS input channels A2, B2 and C2. Either voter subsystem is capable of performing all required protective actions. The instrument input channel trip signals are provided to the voters via fiber-optic data links. The voters use 2-out-of-3 logic on these input channel trip signals for actuating the output Ro relays. The redundant Ro relays mitigate failure modes of the voter outputs.

An Override switch has been installed on the unit board for the ESPS ODD and EVEN voters which allows operators to override the ESPS system in case of an ESPS actuation caused by a Software Common Mode Failure. Once the override is initiated, operators are able to manually position ESPS components.

For Units with the digital ESPS installed or not installed, the example just presented shows the independence and redundancy of the system. There is redundancy of sensors, logic, and equipment. The redundancy is preserved and kept effective by independence of sensors, instrument strings, logic, and control elements in the final actuator. These characteristics enable the system to tolerate single failures at all levels.

The system protective devices (pumps, valves, etc.) require electrical power in order to operate and perform their functions. The power for operating the CR relays is taken from the power source of the associated device. Loss of power to a CR relay or device does not impair the system functions since there is a second redundant device for each required function. The power for the R_o relays, logic, and instruments is taken from the plant's system of battery backed vital buses since loss of power at this level could affect the performance capability of the system. The system will tolerate the loss of one vital bus without loss of protective capability.

7.3.3.1 Redundancy and Diversity

The system as evaluated above is shown to have sufficient diversity and redundancy to withstand single failures at every level.

7.3.3.2 Electrical Isolation

The use of isolation amplifiers will effectively prevent any faults (shorts, grounds, or cross connection of signals) on any analog signal leaving the system from being reflected into or propagating through the system. The direct connection of any analog signal to a source of electrical power can, at worst, negate information from the measured variable involved. The use of individual R_o relays for each controlled device effectively preserves the isolation of each device and of elements of one protective channel from another. Faults in the control wiring between an R_o relay and its CR relay in the controller of a protective device will not affect any other device or protective channel action.

For Units with the digital ESPS installed, electrical isolation is inherent in the use of fiber-optic data links. In order to maintain electrical independence when input signals are shared between channels, a TXS communication link module is used to convert the signal from hard wire to fiber optic. The fiber optic communication equipment is qualified as Class 1E isolation and provides the required electrical separation between each protective channel. Fiber optic communication equipment is also used between protective channels and the Monitoring and Service Interface (MSI) and between the ESPS input channels and the Voters. Fiber optic isolation prevents internal electrical faults from propagating from one protective channel to other redundant protective channels

For Units with the digital ESPS installed or not installed, separation of redundant Engineered Safeguards (ES) functions is accomplished by assigning the eight actuation channels (Table 7-2) to three groups. Isolation for power, control, equipment location, and cable routing is maintained throughout. Channels l, 3, 5 and 7 are assigned to one group (odd actuation channels). Channels 2, 4, 6 and 8 are assigned to a second group (even actuation channels). Equipment which is actuated by both the even and odd actuation channels is assigned to a third group. All equipment required to perform a specific ES function is assigned to the same group. For example, a pump motor and all valves required for that pump to perform its function are assigned to the same group.

For Units with the digital ESPS installed or not installed, for Oconee 1, AC power for equipment controlled by the odd numbered actuation channels is supplied from Switchgear Group 1TC (4KV), motor control center 1XSl, 1XSF, and 1XS4 (600 and 208 volts), actuation power from Vital Power Panelboard 1KVIA and DC control power from DC Panelboard 1DIA. ES functions which are redundant to those controlled by the odd numbered actuation channels are controlled by the even numbered actuation channels. AC power for this equipment in Oconee 1 is supplied from Switchgear Group 1TD (4KV), Motor Control Center 1XS2 and 1XS5 (600 and 208 volts), from Vital Power Panelboard lKVIB, and DC control power from DC Panelboard 1DIB. Where a third unit of ES equipment is used to provide additional redundancy, it is actuated by both the even and odd actuation channels. AC power for this equipment in Oconee l is supplied from Switchgear Groups 1TE or 2TC (4KV), Motor Control Center 1XS3 (600 and 208 volts), actuation power from either Vital Power Panelboard 1KVIA for odd channel actuation or Vital Power Panelboard 1KVIB for even channel actuation, and DC power from DC Panelboard 1DIC. Similar arrangements are employed for ES equipment in Oconee 2 and 3 with different power and control sources for each unit. Motor Control Centers XS4, XS5 and XS6 are complements to Motor Control Centers XS1, XS2 and XS3 respectively. These are described in Section 8.3.

7.3.3.3 Physical Isolation

The arrangement of ESPS components within the system cabinets is designed to reduce the chance of physical events impairing system operation. Control wiring between the ESPS output components and the final actuating devices is physically separated and protected against damage which could impair system operation.

Separation between redundant channels of equipment, control cables, and power cables provides independence of redundant ES functions. The one exception to this separation are the fiber optic cables used for interchannel communication. Power and control cables for each group of ES equipment are

routed in cable trays that contain no cable for redundant equipment or meet current separation criteria. Cables for Reactor Building cooling units enter each Reactor Building through three separate penetrations located at least 25 feet apart and are routed in three different directions to the cooling units. The only other ES equipment located inside the Reactor Buildings are electric motor operated isolation valves which are all common to the odd numbered actuation group discussed above.

7.3.3.4 Periodic Testing and Reliability

For units with the digital ESPS installed, the ESPS input processors perform software logic and parameter checks on the analog and contact input signals and provide software logic outputs to the other input channels as well as to the voter output channels. Each input variable is measured by three process sensors. The 2.MAX and 2.MIN signal selection functions are used for analog inputs and 2-out-of-3 selection logic is used for contact inputs. Trip signals from the three input channels are processed within the voter processors which provide an ESPS output channel actuation through a set of Output Ro relays. The use of 2-out-of-3 logic between protective input channels and GO/NOGO (described below) testing of system outputs permits a protective channel to be tested online without initiating an output channel trip. The test circuits take advantage of the system redundancy, independence, and coincidence logic software to make it possible to manually initiate test signals in one protective channel without affecting the other channels. Surveillance requirements have been established for performance of protective channel calibrations and protective channel functional testing.

The digital ESPS provides continual online automatic monitoring of each of the input signals in each input channel, performs signal online validation, and provides functional validation of hardware performance.

The digital ESPS has a Graphical Service Monitor (GSM) which supplies individual screens for monitoring and recording the analog and binary inputs during Protective Channel Calibration tests. To prevent adverse system actions while performing these tests, the analog or binary signals under test may be placed in Bypass using the GSM Trip/Bypass screens. There are also screens to exercise the output channel trip logic, statalarms, and events recorder. Each protective channel can be tripped in a GO or NOGO test. A NOGO test will trip half of the output string and provide indication of a successful test on the GSM screen without moving the component. A GO test will trip both halves of the output string and provide indication of a successful test in the GSM and reposition the component to the ESPS position. Each protective channel is provided with a key-operated Parameter Change Enable keyswitch. The system software controls access to the computer from each protective channel by controlling the operating modes of the computer. Under normal operating conditions, the computer is in the OPERATION mode. The PARAMETERIZATION Mode allows changes to specific parameters or performance of tests from the GSM screens. Permission to change from the OPERATION mode into the PARAMETERIZATION mode is provided by the Parameter Change Enable Keyswitch. After the permissive is provided from a system processor via its Keyswitch, communication from the Service Unit to that processor is allowed to change its operating mode. Placing the PROCESSOR into the FUNCTION TEST and DIAGNOSTIC modes requires first enabling the PARAMETERIZATION Mode with the keyswitch and then setting a separate parameter to enable these modes with the GSM. The FUNCTION TEST Mode allows disabling the application function and forcing the output signals (normally not used). The DIAGNOSTIC Mode allows download of new application software. The FUNCTION TEST and DIAGNOSTIC modes result in the processor ceasing its cyclic processing of the application functions. The Parameter Change Enable Keyswitches are administratively controlled (no hardware or software interlocks are provided). When a keyswitch is placed in the Parameter Change Enable Mode Position for any activity, the affected processor shall first be declared out of service. In addition to declaring the processor out of service, when loading or revising software in an input channel processor, the affected ESPS inputs shall be tripped OR the associated ESPS voters shall be placed in Bypass. If this activity is being performed on an ES Input Channel in subsystem 1, the associated RPS channel shall also be placed in manual bypass. Only one

ESPS channel at a time is allowed to be placed into Parameter Change Enable Mode Position for software loading/revision. In addition to declaring the processor out of service, when loading or revising software in a voter processor, the affected ESPS voter (Set 1 or Set 2) shall be placed in Bypass. Only one ESPS voter at a time is allowed to be placed into Parameter Change Enable Mode Position for software loading/revision. Parameter Change Enable Keyswitch status information is sent to a statalarm and is also sent to the OAC via the gateway.

The reliability of the system has been made very high so as to eliminate the need for frequent tests of the logic. The system software is not susceptible to transient, random, aging, or environmental related faults since it does not fail in the conventional sense. It can be reasonably expected to exhibit no degradation from these factors. The cyclic self-monitoring routine verifies that the code is not corrupted. The Mean Time Between Failure (MTBF) data for the Teleperm XS equipment calculates MTBF rates from 29 years to 267 years at 40°C. See Reference 1.

Protective Channel Functional Testing, which is part of the Protective Channel Calibration, is performed every refueling outage. The digital ESPS software performs a continuous online automated cross channel input check, separately for each input channel, and continuous online signal error detection and validation. The combination of the self-testing features and the reliability of the TXS equipment support a protective channel functional test frequency of every refueling outage. The setpoints in the software are manually verified every 92 days. The output channel output relays are manually actuated every 92 days. Digital ESPS logic is re-verified every refueling outage by rebooting the channel computer and checksums are verified at that time.

For Units with the digital ESPS not installed, the number of elements which can fail in a single instrument string is small as the system coincidence logic is not complex. The redundancy of the logic and the division of protective devices between logics forms a system having two parallel protective channels either of which is capable of performing the required functions. These characteristics are basic to an inherently reliable system. Logic elements are relays which have been selected for reliability and subjected to confirming tests under loads identical to those encountered in the system. The resultant calculated probability of logic failure is several orders of magnitude less than the known or estimated probability of failure of all other system elements.

The built-in test facilities permit an electrical trip test of each analog instrument string by the substitution of signals at the isolation amplifiers.

When an analog instrument string is placed in test, all associated analog subsystem outputs go to the trip state. This assures that protective action cannot be defeated by placing analog instrument strings in test.

To avoid a full protective channel or system trip, the logic is tested in parts, one element at a time. The continuity of the electrical connections from the output of the coincidence logic up to each Ro relay is tested by means of the LT and UC modules. A LT module can neither prevent a trip of the associated protective channel when protective action is called for nor initiate a trip of the associated protective channel.

An individual protective device may be actuated by means of the UC module manual switch. Operating this switch energizes the Ro relay as if the protective channel has tripped actuating the associated final device. The module lamp confirms that the module test relay returned to its normal state upon release of the manual switch.

On-line checks of the system will confirm the normal state of the system, principally by comparative readings of similar analog indications between redundant measurements and by the status lamps on bistables and logic modules.

The set points of the pressure switches used for ESPS channels 7 and 8 may be checked by connecting a source of pressure and a pressure gauge to test connections provided. The design provides access for this check at all reactor power levels.

7.3.3.5 Manual Trip

For units with the digital ESPS system not installed, a manual trip switch is provided in each Engineered Safeguards Protective System channel. There are eight manual trip pushbuttons on the control console, one for each protective channel

For Units with the digital ESPS installed, each actuation channel (1 through 8) may be manually tripped from the Manual Trip pushbuttons on the Unit Board. This trip is independent of the software and may be initiated during any mode of operation. Each actuation channel (1 through 8) may be manually reset from the Reset pushbuttons on the Unit Board following either automatic or manual actuation of the channel. The ESPS manual actuation paths do not pass through the software, and therefore are not dependent on the correct functioning of the software.

7.3.3.6 Bypassing

The trip functions of the High and Low Pressure Injection and Reactor Building Non-Essential Isolation Systems are bypassed whenever the reactor is to be depressurized below the trip point of the systems. Bypassing must be initiated manually within a fixed pressure band above the protective system trip point. The High Pressure Injection and Reactor Building Non-Essential Isolation System may be bypassed only when the reactor pressure is 1,750 psi or less, and the Low Pressure Injection System may be bypassed only when the reactor pressure is 900 psi or less. The bypass is automatically removed when the reactor pressure exceeds the removal set point associated with the bypass values. This is in accordance with IEEE 279, Section 4.12 and for units with the digital ESPS installed, IEEE Std 603-1998 Section 6.6 and 7.4. The removal set points are above the trip points in order to obtain a pressure band in which the trips may be bypassed during a normal cooldown. The bypasses do not prevent actuation of the HP and LP Injection and Reactor Building Non-Essential Isolation Systems on high Reactor Building pressure. Bypassing is under administrative control. Since the ESPS incorporates triple redundancy in its analog input subsystems, there are three HP injection bypass switches and three LP injection bypass switches. Two of the three switches must be operated to initiate a bypass. Once a bypass has been initiated, the condition is indicated by the plant annunciator and by lamps associated with the bypass switches. For units with the digital ESPS system not installed the switches are backlighted. No provisions are made for manual removal of a bypass before its automatic removal set point is reached.

7.3.3.7 References

1. AREVA Document 32-5061241, Oconee Nuclear Station, Unit 1, 2, and 3 RPS/ESFAS TXS Upgrade Availability Analysis (OM 201.N-0028-007).
2. Safety Evaluation Report for RPS/ESPS Digital Upgrade dated January 28, 2010, by the Office of NRR related to Amendment Numbers 366, 368, and 367 to renew Facility Operating Licenses DPR-38, DPR-47, and DPR-55, Oconee Nuclear Station Units 1, 2, and 3 Docket Numbers 50-269, -270,-287.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.3.

THIS PAGE LEFT BLANK INTENTIONALLY.

7.4 Systems Required for Safe Shutdown

7.4.1 Nuclear Instrumentation

The nuclear instrumentation system is shown in Figure 7-6. The system meets the intent of the Proposed IEEE "Criteria for Nuclear Power Plant Protection Systems," dated August, 1968, (IEEE No. 279), for those elements associated with the Reactor Protective Systems.

7.4.1.1 Design Bases

The nuclear instrumentation (NI) system is designed to supply the reactor operator with neutron information over the full operating range of the reactor and to supply reactor power information to the RPS and to the Integrated Control System (ICS).

The system sensors and instrument strings are redundant in each range of measurement. Measurement ranges are designed to overlap to provide complete and continuous information over the full operating range of the reactor.

7.4.1.2 System Design

The nuclear instrumentation has nine (eight for Unit 1; eight for Unit 3) channels of neutron information divided into three ranges of sensitivity: source range, wide range, and power range. The three ranges combine to give a continuous measurement of reactor power from source level to approximately 200 percent of rated power or ten [1] decades of information. A minimum of one decade of overlapping information is provided between successive higher ranges of instrumentation. The relationship between instrument ranges is shown in Figure 7-7.

The source range instrumentation has four redundant count rate channels originating in four high sensitivity fission chambers. These channels are used over a counting range of 0.1 to 10^5 counts/sec as displayed on the operator's control console in terms of log counting rate. The channels also measure the rate of change of the neutron level as displayed for the operator in terms of startup rate from -1 to +7 decades/min.

The wide range instrumentation has four log N channels originating in four electrically identical fission chambers. Each channel provides ten+ decades of flux level information in terms of the log of chamber count rate and startup rate. The fission chamber/wide range monitor output range is from 10^{-8} to 200% power. The startup rate range is from -1 to +7 decades/min. A high startup rate of +2 decades/min. in any channel will initiate a control rod withdraw inhibit.

The power range channels have five (four for Unit 1; four for Unit 3) linear level channels originating in five (four for Unit 1; four for Unit 3) composite uncompensated ion chambers. The channels output is directly proportional to reactor power and covers the range from 0 to 125 percent of rated power. The gain of each channel is adjustable providing a means for calibrating the output against a reactor heat balance.

Power range channels NI-5, -6, -7, and -8 supply reactor power level information continuously to the RPS. Dual indicators on the control console provide the operator with both total reactor power information (ϕ), and reactor power imbalance information ($\Delta\phi$), from each of the four channels. The method of obtaining ϕ and $\Delta\phi$ is described in Section 7.4.1.2.1.

Reactor power information is provided to the ICS from NI-5, NI-6, NI-7 and NI-8. Isolation amplifiers are used to provide isolation of the power range signals leaving the RPS cabinets. Isolation amplifiers are used to buffer the signals leaving the RPS cabinets, preventing the reflection of faults on external signal lines back into the RPS. The ICS uses 2nd highest median select logic for selection of NI-5, NI-6, NI-7,

or NI-8 power range signal to be used for control and display on a recorder located on the control console above the power range indicators.

7.4.1.2.1 Neutron Detectors

The detectors used in the source range and wide range channels are fission chambers. The same detector/electronics string provides both source range and wide range outputs.

Uncompensated ion chambers are used in the power range channels. Power range detectors, except NI-9 (Unit 1 NI-9 abandoned in place) on Unit 1 which is a three section detector, consist of two nominally 70-inch sections with a single high voltage connection and two separate signal connections. The outputs of the two sections are summed and amplified by the linear amplifiers in the associated power range channel to obtain a signal proportional to total reactor power (ϕ). A signal proportional to the difference in percent full power between the top and bottom halves of the core, the reactor power imbalance or $\Delta\phi$, is derived from the difference in currents from the top and bottom sections of the detector. The difference signal is displayed on the control console to permit the operator to maintain proper axial power distribution. The manual test and calibration facilities provide a means for reading the output of the individual sections of the detector. Each detector has a combined sensitive volume extending approximately from the bottom to the top of the reactor core.

The physical locations of the neutron detectors are shown in Figure 7-8, Figure 7-9, and Figure 7-10. The power range detectors for channels NI-5, -6, -7, and -8 are positioned adjacent to each of the four quadrants of the core. The power range detector for channel NI-9 (Unit 1 NI-9 abandoned in place; Unit 3 NI-9 abandoned in place) is adjacent to the power range detector for channel NI-5. The source/wide range detectors are located adjacent to each of the four quadrants of the core.

Table 7-4 provides pertinent characteristics of the out-of-core neutron detectors. The flux ranges illustrated in Figure 7-7 are seen to be compatible with these characteristics. Nearly identical Westinghouse out-of-core detectors are presently in use at power reactors as follows:

Tube Type	Reactors	Utility
FC	Haddam Neck	Connecticut Yankee Power
	San Onofre	Southern California Edison
	Three Mile Island	GPU Nuclear
	Crystal River 3	Florida Power Corp.
UCIC	Haddam Neck	Connecticut Yankee Power

7.4.1.2.2 Test and Calibration

Test and calibration facilities are built into the system to permit an accurate calibration of the system and the detection of system failures in accordance with the requirements of Reactor Protective System design and IEEE No. 279. The digital RPS systems are also subject to IEEE Std 603-1998 "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations".

7.4.1.3 System Evaluation

The nuclear instrumentation will monitor the reactor over a minimum 10+decade range from source range to 200 percent of rated power. The full power neutron flux level at the power range detectors will be approximately 3.2×10^9 nv. The detectors employed will provide a linear response up to approximately 1.5×10^{10} nv before they are saturated.

The wide range channels fully overlap the source range and the power range channels as shown in Figure 7-7, providing the continuity of information needed during startup.

The steady-state radial flux distribution within the reactor core will be measured by the incore neutron detectors (Section 7.6.1). Both the out-of-core (NI-5, -6, -7, and -8) and incore detectors will be used to obtain the axial power distribution. The sum of the outputs from the two sections of each (out-of-core) power range detector will be calibrated to a heat balance. The sum will be recalibrated whenever it is determined that the sum disagrees with the heat balance by 2 percent or more. The signals from the two sections of the detector may be individually read and compared independent of the sum of the outputs. The operator, therefore, may correlate the difference signal against the core power distribution obtained from the incore system.

7.4.1.3.1 Primary Power

The nuclear instrumentation draws its primary power from vital buses and uninterruptable buses described in Section 8.3.2.1.4 and Section 8.3.2.1.5.

7.4.1.3.2 Reliability and Component Failure

The requirements established for the Reactor Protective System apply to the nuclear instrumentation. All channel functions are independent of every other channel, and where signals are used for safety and/or control, electrical isolation is employed to meet the criteria of Section 7.1.2.

7.4.1.3.3 Relationship to Reactor Protective System

The relation of the nuclear instrumentation to the RPS is described in Section 7.2. Power range channels NI-5, -6, -7, and -8 are associated with the Reactor Protective System. NI-5, NI-6, NI-7 and NI-8 also provide information for the Integrated Control System through Isolation Amplifiers.

The periodic test requirements of the Reactor Protective System are not dictated by the accuracy of the power range channels. The accuracy of the linear amplifiers is better than ±0.2 percent including drift.

7.4.2 Non-Nuclear Process Instrumentation

7.4.2.1 Design Bases

The non-nuclear process instrumentation provides the required input signals of process variables for the reactor protective, regulating, and auxiliary systems. It performs the required process control functions in response to those systems and provides instrumentation for startup, operation, and shutdown of the reactor system under normal and emergency conditions.

7.4.2.2 System Design

The non-nuclear instrumentation provides measurements used to indicate, record, alarm, interlock, and control process variables such as pressure, temperature, level, and flow in the reactor coolant, steam supply, and auxiliary reactor systems as shown in system drawings in Chapter 5, Chapter 9, Chapter 10 and Chapter 11. Process variables required on a continuous basis for the startup, operation, and shutdown of the unit are indicated, recorded, and controlled at the control rooms. Alternate essential indicators and controls are provided at other locations to maintain the reactor in a hot shutdown condition if the control rooms have to be evacuated. Other instrumentation is provided at auxiliary panels with alarm at the control rooms.

Response time and accuracy of measurements are adequate for reactor protective and regulating systems and other control functions to be performed.

7.4.2.2.1 Non-Nuclear Process Instrumentation in Protective Systems

Four independent measurement channels are provided for each process parameter for input to the Reactor Protective System.

Three independent measurement channels are provided for each process parameter and input to the Engineered Safeguards Protective System.

a. Reactor Outlet Temperature

Reactor outlet temperature inputs to the Reactor Protective System are provided by two fast-response resistance elements and associated transmitters in each loop.

b. Reactor Coolant Flow

Reactor coolant flow inputs to the Reactor Protective System are provided by eight high-accuracy differential pressure transmitters which measure flow through calibrated flow tubes welded into the reactor outlet pipe. The power/flow monitor of the reactor protective system utilizes this flow measurement to prevent reactor power from exceeding a permissible level for the measured flow. Operation of each reactor coolant pump breaker is also monitored as an indication of flow.

RPS Channel E, provides reactor coolant loop A and loop B flow information to the ICS. Channel E is in no way associated with Reactor Protective functions. Reactor coolant loop A and B flow information is also provided to the ICS from RPS Channel A and RPS Channel B. Optical Isolators are used to provide isolation from the RPS. Optical Isolators are used to buffer the signals leaving the RPS cabinets, preventing the reflection of faults on external signal lines back into the RPS. The ICS uses median select logic for selection of the reactor coolant loop A and B flow signal to be used for control.

c. Reactor Coolant Pressure

Reactor Protective System inputs of reactor coolant pressure are provided by two pressure transmitters in each loop.

RPS Channel E, provides reactor coolant pressure information to the ICS. Channel E is in no way associated with Reactor Protective functions. Reactor coolant pressure information is also provided to the ICS from RPS Channel A and RPS Channel B. Optical Isolators are used to provide isolation from the RPS. The Optical Isolators are used to buffer the signals leaving the RPS cabinets, preventing the reflection of faults on external signal lines back into the RPS. The ICS uses median select logic for selection of the reactor coolant pressure signal to be used for control and display on a recorder located on the control console.

Engineered Safeguards Protective System inputs of reactor coolant pressure in each loop are provided by redundant pressure transmitters. One pressure signal is utilized for recording, low pressure alarm, and interlock to decay heat removal return flow valve LP-1. This pressure signal can be supplied from either ES Channel A or B.

d. Reactor Building Pressure

Reactor Building pressure inputs to the Engineered Safeguards Protective System are provided by:

1) Three pressure transmitters which are located outside the Reactor Building. These provide inputs for initiation of Reactor Building isolation, high pressure injection, low pressure injection, and Reactor Building cooling.

2) Three groups of two pressure switches each are located outside the Reactor Building. These provide input signals of high Reactor Building pressure for initiation of Reactor Building spray by safeguards actuation.

Table 7-5 provides pertinent information concerning the NNI sensors supplying inputs to the RPS and ESPS, respectively.

7.4.2.2.2 Non-Nuclear Process Instrumentation in Regulating Systems

Selective reduntant measurements and input signals are provided for the process variables required for critical control functions. Selection between the redundant measurements and input signals is performed within the ICS utilizing two types of equipment. The "Control STAR" [TM] modules perform valid signal selection between certain redundant signals utilizing the median selection technique. Valid signal selection for the remaining critical control process variables is provided by a Smart Automatic Signal Selector (SASS). The SASS detects a rapid change in signal and automatically switches the SASS output signal to the remaining valid input signal.

The SASS instrumentation is located in ICS Cabinet 8 and provides automatic signal selection. The SASS instrumentation monitors the following process signals and selects the valid signal independent of the control board mounted key switch.

1. OTSG Operate Level Loop A
2. OTSG Operate Level Loop B
3. Pressurizer Level

The SASS can also detect a mismatch between the two input signals and provides indication of the mismatch on the SASS panel. The plant computer also receives the same signals as SASS and provides mismatch alarms to the operator via the plant computer.

The "Control STAR" modules are located in the ICS cabinets and provide automatic selection of the median signal for the following process parameters.

1. Reactor Coolant System Pressure
2. Reactor Coolant Flow Loop A
3. Reactor Coolant Flow Loop B
4. Power Range Neutron Flux
5. Feedwater Flow Loop A
6. Feedwater Flow Loop B
7. T-Hot Loop A
8. T-Hot Loop B
9. T-Cold Loop A
10. T-Cold Loop B
11. Turbine Header Pressure
12. OTSG Start-up Level Loop A
13. OTSG Start-up Level Loop B

TM - Control STAR is a trademark of Framatome Technologies.

The following inputs to the Integrated Control System are provided:

a. Reactor Outlet Temperature

Selected loop or unit average outlet temperature input is provided in each loop by two fast response resistance elements and associated transmitters.

b. Reactor Controlling Average Temperature

Loop or unit average temperature signals are selected for indication and input as controlling average temperature. Automatic selection determined by loop flows is provided for input of the appropriate signals.

Reactor inlet temperature signals required for loop, and unit average or differential temperatures are provided in each loop by two fast response resistance elements and associated transmitters.

c. Reactor Inlet Differential Temperature

Reactor inlet differential temperature is calculated, indicated and provided for input to the Integrated Control System.

d. Reactor Coolant Flow

Reactor coolant flow signals are provided for each loop and summed for total flow. Total flow is recorded and "low" total flow is alarmed.

Loop "low" flow signals provide the logic for automatic selection of reactor controlling average temperature.

Contacts from reactor coolant pump motor breakers provide fast indication to the ICS that a pump has tripped.

e. Feedwater Temperature

Feedwater temperature input is provided by three resistance elements and associated transmitters. The selected input also provides indication and feedwater flow temperature compensation.

f. Feedwater Flow

The main feedwater flow measurement in each loop is provided by three redundant differential pressure transmitters that measure flow through a flow nozzle. The automatically selected median feedwater flow signal for each loop is compensated by feedwater temperature. The compensated main feedwater flow signal for each loop is indicated, recorded and input to the ICS.

The start-up feedwater flow measurement in each loop is provided by a differential pressure transmitter that measures flow through a flow nozzle. The start-up feedwater flow signal for each loop is compensated by feedwater temperature. The start-up feedwater flow signal for each loop is indicated to the operator.

g. Feedwater Control Valves Differential Pressure

Pressure drop measurement across the valves is provided for input by redundant differential pressure transmitters. The selected input signal is also indicated.

h. Steam Generator Level

Selected "startup" level and "operate" level inputs are provided from each steam generator. Redundant measurements of each level are provided by differential pressure transmitters. Temperature compensation to augment the predetermined compensation for normal operating temperature is provided by two resistance elements and associated transmitters which measure steam generator lower downcomer temperature.

The selected "operate". level input is recorded and "high" level alarmed. The selected "startup" level input is indicated and "low" level alarmed.

A full range level measurement is provided for indication of each steam generator level but does not provide protective or regulating systems input.

i. Steam Generator Outlet Pressure

Selected outlet pressure input is provided from each steam generator. Measurement is made by pressure transmitters in both outlet lines of each steam generator. The selected input is also indicated.

j. Turbine Header Pressure

Turbine header pressure measurement is provided for input by a pressure transmitter in each header line from the steam generators. The selected pressure signal is also recorded, and high and low pressures alarmed. Additional redundant transmitters in each header line provide indication only.

7.4.2.2.3 Other Non-Nuclear Process Instrumentation

The following instrumentation is provided for measurement and control of process variables necessary for proper operation:

1. Pressurizer Temperature

   Pressurizer temperature is measured by three resistance elements and their associated transmitters. Two resistance elements provide temperature compensation of the Inadequate Core Cooling pressurizer level instrumentation. The third resistance element is used by the pressurizer heater controls to calculate reactor coolant system saturation pressure.

2. Pressurizer Level Control

   Pressurizer level is measured by three differential pressure transmitters. One temperature compensated signal is selected for indication, recording, interlock and level control. The selected level control signal provides alarms and interlock to de-energize the pressurizer electric heaters on low level. The level controller output positions the makeup control valve in the High Pressure Injection System to maintain a preset level. Pressurizer level is lowered by reactor coolant letdown or by manual control at the control room.

3. Reactor Coolant Pressure Control

   The reactor coolant pressure signal for control is provided by isolated signals from RPS Channel A, RPS Channel B and RPS Channel E (the fifth channel). The isolated RPS A, RPS B and the RPS E reactor coolant pressure signals are median selected within the ICS by the "Control Star" module to provide the selected RC Pressure control signal. The selected signal is used as an input to pressure switches which provide signals for automatic control of:

   a. Pressurizer electric heaters.

   b. Pressurizer spray control valve.

   c. Pressurizer electromatic relief valve.

   The heaters are grouped in banks which are energized below preset pressures.

   The selected signal also provides input to a pressure controller which automatically modulates the output of one bank of heaters to maintain a preset pressure.

   The spray and relief valve are opened at preset pressures above the desired reactor coolant system operating pressure.

   The selected signal is recorded and high and low pressures alarmed.

Reactor coolant pressure is recorded on a multi-channel recorder. One Channel has a range of 1700-2500 PSIG, and its input is the median selected reactor coolant pressure signal selected for control. The other channel has a range of 0-2500 PSIG, and its input is from a transmitter in the "A" loop.

Reactor coolant temperature is also recorded on a multi-channel recorder. One channel has a range of 50°F to 650°F and its input is selectable from either of four cold leg RTDs, two located in "A" loop cold legs and two located in "B" loop cold legs. A second channel indicating average temperature receives its imput from the reactor coolant average temperature selected for control and has a range of 520°F to 620°F. A third channel has a range of 520°F to 620°F and receives its input from the selected "A" loop THOT signal. A fourth channel has a range of 520°F to 620°F and receives its input form the selected "B" loop THOT signal. A fifth channel has a range of 520°F to 620°F and receives its input from the selected Average THOT signal.

4. Coolant Pump Control

   Interlock signals of reactor coolant inlet temperature are provided to each pump switching logic to prevent operation of more than three pumps during startup until a preset temperature is reached.

5. Feed and Bleed Control

   The feed and bleed control instrumentation in the High Pressure Injection System provides control and interlocks to permit adjustment of the reactor coolant boron concentration.

7.4.2.3 System Evaluation

The quantity and types of process instrumentation have been selected to provide assurance of safe and orderly operation of all systems and processes over the full operating range of the plant. Some of the criteria for design are:

1. Separate instrumentation and Engineered Safeguards Protective System, Reactor Protective System and Steam Generator Level Control System isolated output signals are used for vital control circuits.
2. Time of response and accuracy of measurements are adequate for protective and control functions to be performed.
3. Where wide process variable ranges are required and precise control is involved, both wide range and narrow range instrumentation are provided.
4. All electrical and electronic instrumentation required for operation is supplied form redundant vital and uninterruptable instrumentation buses.

7.4.2.3.1 Failure in RC Flow Tube Instrument Piping

7.4.2.3.1.1 Reactor Coolant Flow Indication

In each primary loop, reactor coolant flow is detected by measuring the ΔP developed across a flow tube that is an integral part of the outlet piping of the loop. Each flow tube has a high pressure (HP) tap and a low pressure (LP) tap. Connections to the taps are made with 1-inch lines. The 1-inch lines are terminated at root valves located inside the secondary shield wall to HP and LP headers. Five ΔP transmitters are connected between the two headers. Four are used to provide information to the Reactor Protective System. The fifth is used to provide input to the ICS. Isolated output signals from RPS Channel A, RPS Channel B and the fifth transmitter are input to the ICS "Control STAR" modules. The median selected signal provides alarms and indication as described in Section 7.4.2.2.2.

Each of the four Reactor Protective System channels receives a ΔP signal from a different one of the four ΔP transmitters. In other words, one transmitter is exclusively assigned to one protective channel. The

identical arrangement and assignment of transmitters is used for each of the two primary reactor coolant loops.

Within each Reactor Protective System channel, the square roots of the ΔP signals from each loop are extracted to obtain loop flow signals. The loop flow signals are summed to obtain a total reactor coolant flow signal. The three flow signals are displayed by connecting the STAR CTC to the channel's STAR module. The three signals are monitored by the plant computer.

The reactor operator can read the individual loop flows and total flow at the control console. The flow information is available to the operator on the plant computer for each unit.

7.4.2.3.1.2 Failures Considered

The following failures are considered:

1. Break in one of the 1-inch instrument lines.
2. Break in one of the 1/2-inch instrument lines.
3. A leak in one of the instrument lines.
4. Deleted per 2005 update.

7.4.2.3.1.2.1 Break in 1 Inch Instrument Lines

A break of a 1-inch instrument line will result in a reactor trip due to low RC pressure. If the break occurs in a HP line, the reactor will trip due to a high power/flow ratio if the power/flow limit is exceeded.

The operator will receive at least the following alarms and indications:

Alarms:

1. Break in 1-inch HP Instrument Line
   a. Low RC flow.
   b. Plant computer alarm and alarm log for low flow.
   c. Letdown storage low level.
   d. Pressurizer low level.
   e. Low reactor coolant pressure.
   f. Plant computer alarm and alarm log for low RC pressure.
2. Break in a 1-inch LP Instrument Line

   Identical alarms as listed for HP line break except RC flow is alarmed on high value.

Indication:

1. Break in a 1-inch HP Instrument Line
   a. Control room indication of the Reactor Building atmosphere particulate and gas radioactivities increases.
   b. Loop flow indication on console falls to zero.
   c. Loop flow indication in each RPS channel falls to zero. Flow is not displayed in the RPS channel cabinets unless STAR CTC is connected to channel.
   d. Total flow indication on console falls approximately 50 percent.

e. Total flow indication in each RPS channel falls approximately 50 percent. Flow is not displayed in the RPS channel cabinets unless STAR CTC is connected to channel.

f. Makeup flow goes to maximum value.

g. RC pressure falls on console indicators and with each RPS channel.

h. Reactor Building pressure and temperature indication rises.

2. Break in a 1-inch LP Instrument Line

   Identical indication as listed for HP line break except all loop flow indication goes full scale, total flow indication increases above normal.

7.4.2.3.1.2.2 Break in a ½-inch Instrument Line

A break of a ½-inch instrument line will result in a reactor trip due to low RC pressure. If the break occurs in a HP line, the reactor will trip due to a high power/flow ratio if the power/flow limit is exceeded.

The operator will receive the same alarms and indication as described for the 1-inch instrument line break.

7.4.2.3.1.2.3 Leak in One of the Instrument Lines

If the leak occurs in a HP line the operator will receive a low flow alarm for a 5 percent change in indication flow and a high flow alarm for a similar leak in the LP line. At this alarm Point, the leakage is in excess of 1 gallon per minute, hence Reactor Building radiation monitors will readily detect such a condition and result in leak evaluation, and subsequent action as required by Technical Specifications.

Depending on the size of the leak, alarms and indication described in Section 7.4.2.3.1.2.1, may occur. If the leak occurs on either of the ΔP transmitters associated with the RPS-A, RPS-B or the fifth channel input, the ICS "Control STAR" modules will select the median signal for control and indication as described in Section 7.4.2.2.2.

7.4.2.3.1.2.4 Deleted per 2005 Update

7.4.2.3.1.3 Conclusion

The conclusion of this analysis is that the operator has adequate indication and alarm facilities to quickly recognize a common mode failure in the flow instrumentation for the reactor protection system. Corrective action would therefore be positive and prompt.

7.4.2.3.2 Coincident LOCA and Systematic Failure of Low RCS Pressure Trip Signal.

Several break sizes and locations for the loss-of-coolant accident have been investigated with an assumed systematic failure of the low Reactor Coolant System pressure trip signal. Although this failure is not considered credible, the analysis has shown that either the void shutdown mechanism or the power/flow comparator should provide backup to shut down the reactor and render the Emergency Core Cooling System (ECCS) effective.

7.4.3 Emergency Feedwater Controls

7.4.3.1 Emergency Feedwater and Pump Controls

7.4.3.1.1 Design Basis

The Emergency Feedwater (EFW) System is designed to start the EFW pumps automatically in the event of loss of both main feedwater pumps or low water level in either steam generator.

The EFW control valves are designed to control steam generator level when the EFW System is supplying feedwater to the steam generators.

All automatic initiation logic and control functions are independent from the Integrated Control System (ICS).

7.4.3.1.2 System Design

Three EFW pumps powered from diverse power sources are provided. These include two independent motor driven pumps, each supplying feedwater to one steam generator; and one turbine driven pump, supplying feedwater to both steam generators.

Each of the EFW pumps is supplied with its own independent starting circuit which will start automatically as outlined below. Automatic initiation of the EFW pumps by ATWS Mitigation System Actuation Circuitry is described in Section 7.8. These independent control circuits are powered by the 125 VDC station batteries. Each pump is also provided with a control switch with which the operator may start the pump manually.

Discharge flow from the EFW pumps is normally aligned and controlled by discharge control valves located in the supply line to each steam generator's emergency feedwater connection. The control valves limit or increase emergency feedwater as necessary to maintain steam generator inventory and cooldown rate. These valves may be automatically controlled, or manually controlled by the operator.

Indication is provided in the control room to allow the operator to monitor EFW System parameters during a cooldown.

Alarms are provided to alert the operator of conditions exceeding normal limits. Essential plant parameters are annunciated or alarmed by the process computer in addition to specific EFW System alarms.

Motor Driven EFW Pumps (MDEFWP's):

Power for the motor driven pumps is normally provided by the normal station auxiliary power system. During loss of offsite power operation, these pumps are aligned to the Emergency Power System

Automatic starting of the MDEFWP's is determined by the position of the control room selector switch for each pump. The MDEFWP's are provided with a four position selector switch which allows the operator to select between OFF, AUTO 1, AUTO 2 and RUN. When the selector switch is in the AUTO 1 position, LOW STEAM GENERATOR WATER LEVEL in either steam generator (OTSG) will start the pump after a time delay to prevent spurious actuations. When the selector switch is in the AUTO 2 position, LOW STEAM GENERATOR WATER LEVEL or LOSS OF BOTH MAIN FEEDWATER PUMPS will start the pump. Loss of both main feedwater pumps is sensed by pressure switches which monitor feedwater pump turbine hydraulic oil pressure.

Automatic starts of the MDEFWPs are disabled if a main steam line break is sensed by the Automatic Feedwater Isolation System (AFIS). Upon an AFIS actuation, the MDEFWP aligned to the affected steam generator will automatically stop and be inhibited from any further automatic starts. Once automatically started, the MDEFWPs will continue to operate until manually secured by the operator or

disabled by an AFIS signal. The operator can manually start the MDEFWP by placing its selector switch to RUN.

Cooling water is initiated automatically, upon manual or automatic start of the MDEFWPs.

Turbine Driven EFW Pump (TDEFWP):

The steam supply for the TDEFWP turbine is provided from the main steam lines upstream of the main turbine stop valves and/or from the Auxiliary Steam System. Upon loss of station air, the supply is maintained by nitrogen bottle back-ups which are used on the pressure control valves. Should the nitrogen bottle back-ups fail, these control valves would fail to the open position.

The steam admission valve to the turbine, MS-93 is controlled by a normally energized solenoid valve. Upon receipt of a manual or automatic start signal, the solenoid valve will de-energize and immediately start the turbine by opening the steam admission valve. The steam admission valve will fail open upon loss of power to the normally energized solenoid valve or loss of supply air. The supply air is equipped with instrument air, auxiliary instrument air, and bottled Nitrogen backups. The EFW pump turbine speed is controlled by MS-95. The position of MS-95 is regulated by a hydraulic oil speed governing mechanism, with oil supplied from either the auxiliary oil pump or the shaft driven oil pump. MS-95 is designed to fail closed on loss of hydraulic oil pressure. An AFIS actuation will energize and close solenoid valve (TO-145) to isolate the hydraulic oil supply to close MS-95.

THE TDEFWP auxiliary oil pump is started automatically when the steam admission valve is opened, and provides hydraulic oil pressure for the operation of the TDEFWP governor control valve until the TDEFWP shaft driven oil pump is available. The TDEFWP auxiliary oil pump and its associated circuitry is required for automatic start of the TDEWFP. This equipment is powered from station batteries.

Automatic starting of the TDEFWP is determined by the position of the control room selector switch for the pump. The TDEFWP is provided with a three position-pull to lock selector switch. The operator can select between OFF, AUTO and RUN. When the selector switch is in the AUTO position, LOSS OF BOTH MAIN FEEDWATER PUMPS, with exception to loss due to the AFIS logic, will start the pump. Loss of both main feedwater pumps is sensed by pressure switches which monitor feedwater pump turbine hydraulic oil pressure. Automatic starts of the TDEFWP are disabled if a main steam line break is sensed by the AFIS circuitry. Upon an AFIS actuation, the TDEFWP will automatically stop and be inhibited from any further automatic starts. Once automatically started, the TDEFWP will continue to operate until manually secured by the operator or disabled by an AFIS (Unit 1) or MSLB (Units 2 and 3) signal. The operator can manually start the TDEFWP by placing the selector switch to RUN.

Once automatically started, the TDEFWP will continue to operate until manually secured by the operator or shutdown by the MSLB circuitry.

Control Valves:

Deleted paragraph(s) per 2002 Update.

Each emergency feedwater discharge line to each steam generator is provided with a control valve and a check valve. The air operated control valves receive an electric current signal that is converted to an air signal through an I/P converter. The converted signal is used for modulation of the valve in response to steam generator level, independent from the ICS. Each control valve has a Hand/Auto station mounted on the main control board. A pushbutton is provided on each Hand/Auto station to allow the individual EFW control valve to be placed in either an automatic level control mode or in a manual level control mode of operation. The Hand/Auto stations may be utilized to position the respective control valve when in the manual mode. Open/Closed valve position indication is provided for each control valve in the main control room. Power to the controller is battery backed DC converted to AC via the vital inverters.

The control valves are normally closed in the automatic mode due to steam generator level > setpoint. In automatic, an Auto/Manual relay for each control valve is de-energized, allowing the valve to be positioned automatically.

The control valves are arranged to fail to the automatic control mode upon loss of control power to the Hand/Auto station. If the selected train of automatic control experiences a loss of power, then the valve would fail open. Also, upon loss of station air, the valves will continue to control using the nitrogen supply. If the nitrogen supply fails the valve would fail open. These modes of operation show that Emergency Feedwater isolation will not result from valve control circuitry failure or motive force failure.

7.4.3.1.3 System Evaluation

Redundancy is provided with separate, full capacity, motor and turbine driven pump subsystems. Failure of either the motor driven pumps or the turbine driven pump will not reduce the EFW System below minimum required capacity. Pump controls, and instrumentation are separate and independent in design.

7.4.3.2 Steam Generator Level Control

7.4.3.2.1 Design Basis

The Steam Generator Level Control System (SGLCS) provides automatic Once Through Steam Generator (OTSG) water level control while the EFW System is supplying feedwater to the steam generators. SGLCS is designed to automatically control and modulate emergency feedwater supply to the steam generators during all initiating conditions for the EFW System (Section 7.4.3). Each OTSG has two independent level control systems each of which is capable of supplying a signal to the associated OTSG emergency feedwater level control valve.

The Steam Generator Level Control System (SGLCS) provides the automatic start signal for both MDEFWPs based on low level in either steam generator.

All automatic initiation logic and control functions are independent from the Integrated Control System (ICS).

7.4.3.2.2 System Design

Each OTSG is provided with two independent level control systems, each of which supplies a signal to that OTSG's emergency feedwater level control valve. The two systems provided for each OTSG monitor the 0-388 inch range (range at cold shutdown) of water in the OTSG. A signal deviation check between the two output signals is performed.

The SGLCS controls level higher than the normal ICS level setpoint to prevent control system conflict. Upon loss of all four reactor coolant pumps, such as during blackout conditions, the level control setpoint is automatically raised to promote natural circulation in the Reactor Coolant System.

Deleted paragraph(s) per 2002 Update.

The operator has a selector switch on the main control board, which is used to select either control channel on each OTSG. Also provided on the main control board is a Hand/Auto station, which may be utilized to override the automatic level control signal. A control switch is provided on the control board for each EFW control valve that can be selected to bypass the Hand/Auto station. When this switch is selected to the bypass or off position only the automatic level control signal is sent to the respective valve. The Hand/Auto stations have redundant QA-1 power sources to minimize the possibility of losing the manual control capability of these valves.

7.4.3.2.3 System Evaluation

Each level channel is separate and independently powered from its counterpart on each OTSG. Redundancy is provided with two trains/channels monitoring each steam generator. Each level channel per steam generator is capable of performing the necessary control and modulation of the feedwater control valves. In addition, sufficient alarms and indications are provided to alert the operator to a system failure and ensure correct manual operation of a level control valve.

7.4.4 Reactor Building LPSW Low Pressure Instrumentation Circuitry

7.4.4.1 Design Basis

Generic Letter 96-06 required consideration of effect inside containment due to the change in environment during a Loss of Coolant Accident (LOCA). This consideration identified the potential for waterhammers in cooling water systems serving containment following a Loss of Offsite Power (LOOP) concurrent with a LOCA or Main Steam Line Break (MSLB). Analysis and system testing in response to GL 96-06 concluded that waterhammers could occur in the Low Pressure Service Water (LPSW) system during all LOOP events (e.g. LOCA/LOOP, MSLB/LOOP). The LPSW piping supplies the Reactor Building Cooling Units (RBCU), the Reactor Building Auxiliary Coolers (RBAC), and the Reactor Coolant Pump Motor Coolers (RCPMC). During Loss of Offsite Power (LOOP) events or Loss of Coolant Accident (LOCA) events coupled with a LOOP it was possible to create a Column Closure Waterhammer (CCWH) or Condensation Induced Waterhammer (CIWH) in the LPSW piping and components inside containment. CCWH could have occured when the LPSW pumps restart following a LOOP and rapidly close vapor voids with the system. CIWH could have occurred when heated steam voids interact with sub-cooled water in long horizontal piping sections.

7.4.4.2 System Design

The Reactor Building LPSW Low Pressure Instrumentation Circuitry consists of four (4) analog channels each powered from a separate safety related battery backed power panel board and two (2) digital actuation channels each powered from a separate safety related battery backed power panel board. Portions of the analog and digital channels are shared with the RBAC LPSW Low Pressure Instrumentation Circuitry which isolates the LPSW supply and return flow to the Reactor Building Auxiliary Coolers (RBAC).

The design function of the instrumentation circuitry is to close the pneumatic discharge isolation valves (LPSW-1121, 1122, 1123, and 1124) and open controllable vacuum breakers (LPSW-1150 and LPSW-1151) any time a low pressure condition occurs in the LPSW supply header. Closure of LPSW-1121, 1122, 1123, and 1124 and the opening of controllable vacuum breakers LPSW-1150 and LPSW-1151 on low LPSW pressure will maintain the LPSW piping inside the Reactor Building water solid thereby avoiding water hammers in the RBCU LPSW piping.

7.4.4.2.1 Analog Channels

A pressure transmitter for each of the four (4) analog channels monitors LPSW supply header pressure. When pressure decreases to the design set point as sensed by a particular channel, a trip relay and alarm relay are actuated for each of the respective channels that sensed the low pressure condition.

The low pressure output from each of the four (4) analog channels provide input to the two redundant 2 out of 4 trip logic paths in each of the two (2) digital logic trip channels.

7.4.4.2.2 Digital Channels

The inputs from the four analog channels are arranged in such a way as to provide different paths within each of the two redundant 2 out of 4 logic circuits. This assures the Reactor Building LPSW flow does not terminate to the Reactor Building due to a single failure of one of the other analog channels during an analog channel test.

The two redundant digital logic trip channels provide a close command signal to the solenoid valves for pneumatic discharge isolation valves LPSW-1121, 1122, 1123, and 1124. The two redundant digital logic trip channels also provide a trip open command signal to the solenoid valves for controllable vacuum breakers LPSW-1150 and LPSW-1151 when a low LPSW pressure condition occurs.

7.4.4.2.3 System Actuation and Reset

Upon actuation of the system, power is removed from solenoid valves LPSW-1121, 1122, 1123 and 1124 to cause each of the normally open pneumatic discharge isolation valves LPSW-1121, 1122, 1123, and 1124 to "Trip" (go to the closed position).

Simultaneously, power is applied to solenoid Valves LPSSV-1150 and LPSSV-1151 which in turn cause the normally closed controllable vacuum breakers LPSW-1150 and LPSW-1151 to "Trip" (i.e., go to the open position). Controllable vacuum breakers LPSW-1150 and LPSW-1151 will "Reset" (i.e., go to the closed position) if both low pressure trips have returned to their normal state. If this should fail to reset the controllable vacuum breaker for a particular train, then, the controllable vacuum breakers for that train will still reset when the normal pressure reset logic for that train has been satisfied as described below.

The low pressure LPSW trips reset to provide a permissive for the resetting of the Waterhammer Protection System (WPS) and the controllable vacuum breakers following the return to normal LPSW system pressure.

However, as stated above, pneumatic discharge isolation valves for a particular train will not actually re-open (Reset) until the low pressure trip for that particular train has also reset, which should have already occured by the time that the normal pressure reset logic circuit has been actuated. Therefore, when the LPSW supply pressure is restored to a value greater than its normal set point value as sensed on two of the four analog input channels, then, power will be reapplied to the solenoid valves that control the pneumatic discharge isolation vlaves LPSW-1121, 1122, 1123, and 1124 results in the re-opening of these valves. Simultaneously, the power path will be interrupted to the solenoid valves that control the controllable vacuum breakers LPSW-1150 and 1151 resulting in the re-closing of these valves, if they have not already done so by the removal of the two trip signals from the digital trip logic.

7.4.4.2.4 RBAC

As stated above, portions fo the pneumatic discharge isolation valves instrumentation circuitry are shared with the RBAC LPSW Low Pressure Instrumentation Circuitry. After the LPSW supply pressure is restored, LPSW Valves LPSW-1054, 1055, 1061, and 1062 will remain closed until the control room operator resets the circuitry by depressing the respective channel reset pushbutton on the control room vertical board and initiates a slow ramp open circuit to restore flow back to the RBAC units.

7.4.4.2.5 Loss of Electrical Power

The pneumatic discharge isolation valves LPSW-1121, 1122, 1123, and 1124 are spring loaded to open and require air to close. The controllable vacuum breakers, LPSW-1150 and LPSW-1151, are spring loaded to close and require air to open. The pneumatic discharge isolation valves and the controllable vacuum breakers all fail closed on loss of electrical power to their respective control solenoid valves.

7.4.4.2.6 System Evaluation

Each analog channel is powered from a separate safety related battery backed power panel board. Likewise, each digital channel is also powered from a separate safety related battery backed power panel board. Redundancy is provided by two pressure transmitters/analog channels monitoring each LPSW supply header. The two-out-of-four logic prevents actuation from the failure of a single transmitter. The LPSW Waterhammer Prevention System is QA1. The system is capable of performing the necessary control and modulation of the LPSW system.

7.4.5 References

1. *Evaluation of Transient Nuclear Instrumentation Power Range Flux Error* - Duke Power Company - March 1981.
2. Qualification Testing of Protective System Instrumentation Babcock and Wilcox - *BAW - 10003 Rev. 3 - April, 1974 and BAW - 10003A Rev. 4 - January, 1976.*
3. *Evaluation of Reactor Protective System Grounding Concern* Babcock and Wilcox - March, 1978.
4. *177 FA Plants NI/RPS Ground Problem Discussion and Recommended Test Scheme* Babcock and Wilcox - March, 1978.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.4.

7.5 Display Instrumentation

7.5.1 Criteria And Requirements

7.5.1.1 Type A Variables

Type A variables are defined as those variables which are monitored to provide the primary information required to permit the Control Room operator to take specific manually controlled actions for which no automatic control is provided and that are required for safety systems to accomplish their safety functions for design basis accidents. Primary information is defined as that which is essential for the direct accomplishment of the specified safety functions; it does not include those variables associated with contingency actions which may also be identified in written procedures.

Emergency Procedures provide the lead guidance for selection of Type A variables. The following variables are those determined to be Type A for Oconee Nuclear Station, as defined above:

1. Reactor Coolant System Pressure
2. Core Exit (Thermocouples) Temperature
3. Pressurizer Level
4. Degrees of Subcooling
5. Steam Generator Level
6. Steam Generator Pressure
7. Borated Water Storage Tank Level
8. High Pressure Injection Flow
9. Low Pressure Injection Flow
10. Deleted per 2006 update
11. Deleted per 2005 update
12. Upper Surge Tank Level
13. Low Pressure Service Water (LPSW) Flow to Low Pressure Injection (LPI) Coolers.

7.5.1.2 Type B and C Variables

Type B and C variable selection is based on the Safety Parameter Display System (SPDS) Critical Safety Functions. The SPDS, which meets the requirements of NUREG 0737, Supplement 1,is provided as an aid to the Control Room operating crew in monitoring the status of the Critical Safety Functions. The Critical Safety Functions monitored are those defined in the SPDS Critical Safety Function Fault Trees. The SPDS provides continuous status updated at regular intervals of the Critical Safety Functions.

Since these Critical Safety Functions constitute the basis of the Oconee SPDS, it is Duke Power's position that they should also be identified as the plant safety functions for accident monitoring (i.e., the basis for Type B & C variable selection).

Using the SPDS Critical Safety Functions as the basis for defining the accident monitoring instrumentation incorporates the concept of monitoring the multiple barriers to the release of radioactive material. The Critical Safety Functions monitored are those which assure the integrity of these barriers. The Fault Tree provides an explicit, systematic mechanism for organizing the plant data required to

evaluate a Critical Safety Function. The prioritization of the Critical Safety Functions is consistent with the concept of multiple barriers to radiation release.

The Critical Safety Functions are:

1. Subcriticality

The subcriticality fault tree monitors the reactor core to assure that it is maintained in a subcritical condition following a successful reactor trip.

2. Inadequate Core Cooling

The inadequate core cooling fault tree monitors those variables necessary to evaluate the status of fuel clad heat removal.

3. Heat Sink

The heat sink fault tree monitors the ability to transfer energy from the reactor coolant to an ultimate heat sink.

4. Reactor Coolant System Integrity

The Reactor Coolant System integrity fault tree monitors those variables indicating a challenge to or a breach of the Reactor Coolant System pressure boundary.

5. Containment Integrity

The containment integrity fault tree monitors those variables which would indicate a threat to containment integrity or other undesirable conditions within containment.

6. Reactor Coolant System (RCS)

The RCS inventory fault tree monitors for indications of off-normal quantities of reactor coolant in the primary system.

7.5.1.3 System Operation Monitoring (Type D) and Effluent Release Monitoring (Type E) Instrumentation

7.5.1.3.1 Definitions

Type D: Those variables that provide information to indicate the operation of individual safety systems.

Type E: Those variables to be monitored as required for use in determining the magnitude of the release of radioactive materials and in continually assessing such releases.

The Type D and E variables are selected on the basis of individual plant specific system design requirements.

7.5.1.3.2 Operator Usage

The plant design has included variables and information display channels required to enable the Control Room operating personnel to:

1. Ascertain the operating status of each individual safety system to the extent necessary to determine if each system is operating or can be placed in operation to help mitigate the consequences of an accident. (Note: Type D and E are not always safety systems)
2. Monitor the effluent discharge paths to ascertain if there have been significant releases (planned or unplanned) of radioactive materials and to continually assess such releases.

3. Obtain required information through backup or diagnosis channel where a single channel may be likely to give ambiguous indication.

7.5.1.4 Design and Qualification Criteria

Design and qualification criteria used by Duke Power Company for plant instrumentation are provided below. The category designations are provided for reference to the Regulatory Guide 1.97 (Revision 2) document.

7.5.1.4.1 Design and Qualification Criteria - Category 1

Accident monitoring instrumentation which comprise this design and qualification category are considered by Duke Power to be Nuclear Safety Related and thus are classified as Quality Assurance Condition 1 (QA1).

1. QA1 instrumentation is environmentally qualified as described in the Oconee Nuclear Station IEB-79-01B Duke Power Company submittal and the Resolution of Safety Evaluation Reports for Environmental Qualification of Safety Related Electrical Equipment. Seismic qualification is in accordance with the Oconee Nuclear Station licensing basis as specified in Oconee FSAR Chapter 3 and the Duke Power Seismic Design Criteria (OSDC-0193.01-00-0001).

2. No single failure within either the accident monitoring instrumentation, its auxiliary supporting features, or its power sources, concurrent with the failures that are a condition or result of a specific accident, will prevent the operators from being presented the information necessary to determine the safety status of the plant and to bring the plant to and maintain it in a safe condition following that accident. Where failure of one accident-monitoring channel results in information ambiguity (i.e., the redundant displays disagree) that could lead operators to defeat or fail to accomplish a required safety function, additional information is provided to allow the operators to deduce the actual conditions in the plant. This is accomplished by providing additional independent channels of information of the, same variable (an identical channel) or by providing an independent channel to monitor a different variable that bear a known relationship to the multiple channels (a diverse channel). The information provided to the operator to eliminate ambiguity between redundant channels is needed only during a failure of one of the instrument loops. Therefore, it is considered acceptable to use installed instrumentation of equal design and qualification category, installed instrumentation of a lessor design and qualification category, temporary or portable instrumentation, or sampling to allow the operators to deduce the actual conditions in the plant. Redundant QA1 channels are electrically independent and physically separated from each other per the separation criteria described in Chapter 7 of the Oconee FSAR.

   At least one channel of QA1 instrumentation is displayed on a direct indicating or recording device. (Note: Within each redundant division of a safety system, redundant monitoring channels are not needed.)

3. The instrumentation is energized from the safety grade Emergency Power sources (as described in Chapter 8 of the Oconee FSAR) and is backed by batteries where momentary interruption is not tolerable.

4. The instrumentation channel will be available prior to an accident except as provided in Paragraph 4.11, "Exception" as defined in IEEE Standard 279-1971 or as specified in Technical Specifications. For the digital RPS/ESPS system, which includes the TXS cabinets and their associated hardware, the instrumentation channel will be available as defined in IEEE Std 603-1998 Sections 5.7, 6.7, 7.5 and 8.3.

5. The following documents pertaining to quality assurance are referenced:

a. Duke 1A, Duke Power Company Topical Report, "Quality Assurance Program"

b. Oconee FSAR Chapter 17

6. Continuous indication display is provided. Where two or more instruments are needed to cover a particular range, overlapping of instrument span is provided.

7. Recording of instrumentation readout information is provided for at least one of the redundant channels. Recorders which are utilized as the primary display device will be seismically qualified. Where direct and immediate trend or transient information is essential for operator information or action, the recording is continuously available on dedicated recorders. Otherwise, it may be displayed on non-seismically qualified recorders or continuously updated, stored in computer memory, and displayed on demand. Intermittent displays such as data loggers and scanning recorders may be used if no significant transient response information is likely to be lost by such devices. All analog variables which are wired to the plant computer may be trended upon demand and a hard-copy can be generated as needed.

7.5.1.4.2 Design and Qualification Criteria - Category 2

7.5.1.4.2.1 Nuclear Safety Related (QA1) Category 2 Instrumentation

For instrumentation loops that are installed as nuclear safety related (QA1), environmental qualification is provided per the methodology described in the Oconee Nuclear Station IEB 79-01B submittal and the Resolution of Safety Evaluation Reports for Environmental Qualification of Safety Related Electrical Equipment. Seismic qualification is in accordance with the Oconee Nuclear Station Licensing basis as specified in the Oconee FSAR and Duke Power Seismic Design Criteria (OSDC-0193.01-00-0001). Quality Assurance of these QA Condition 1 instrumentation systems is described in the Duke Power Company Topical Report "Duke 1A" and Oconee FSAR Chapter 17. These instruments are powered from the safety grade Emergency Power sources (as described in Chapter 8 of the Oconee FSAR) and are backed by batteries where a momentary power interruption is not tolerable.

7.5.1.4.2.2 Non Nuclear Safety Related (Non-QA1) Category 2 Instrumentation

For instrumentation loops of lesser importance which are not nuclear safety related, appropriate qualification is provided. Environmental qualification is provided per the methodology described in the Oconee Nuclear Station IEB 79-01B submittal and the Resolution of Safety Evaluation Reports for Environmental Qualification of Safety Related Electrical Equipment.

Category 2 instrumentation which is of primary use during one phase of an accident need not be qualified for all phases of the event. For example, an instrument of primary importance prior to attained the recirculation mode need not be demonstrated to withstand post-recirculation radiation.

For non-QA1 Category 2 instrumentation, seismic qualification is not required unless seismic induced failure of the instrumentation would unacceptably degrade a safety system.

These instrumentation systems are designed, procured, and installed per Duke Power Company standard practices. Duke Power considers that this is adequate to assure the quality of the subject instrumentation.

Isolation devices are provided to interface between Nuclear Safety Related (QA1) and Non Nuclear Safety Related (non QA1) portions of any of the subject instrumentation loops.

The instrumentation is energized from a highly reliable power source, not necessarily safety grade Emergency Power, and is backed by batteries where momentary interruption is not tolerable.

7.5.1.4.2.3 All Category 2 Instrumentation

For both Nuclear Safety Related and Non Nuclear Safety Related Category 2 instrumentation:

The out-of-service interval should be based on normal Technical Specification requirements for the system it serves where applicable or where specified by -other requirements.

The instrumentation signal may be displayed on an individual instrument or it may be processed for display on demand by CRT or by other appropriate means.

The method of display may be by dial, digital, CRT, or stripchart recorder indication. Effluent radioactivity monitors and meteorology monitors will be recorded. Where direct and immediate trend or transient information is essential for operation information or action, the recording is continuously available on dedicated recorders. Otherwise, it may be continuously updated, stored in computer memory, and displayed on demand.

7.5.1.4.3 Design and Qualification Criteria - Category 3

These instruments do not play a key role in the management of an accident but they do add depth to the Category 1 and 2 instrumentation to the extent that they remain operable. The instrumentation is of high quality commercial grade and is selected to withstand the normal power plant service environment.

The method of display may be by dial, digital, CRT, or stripchart recorder indication. Effluent radioactivity monitors and meteorology monitors will be recorded. Where direct and immediate trend or transient information is essential for operator information or action, the recording is continuously available on dedicated recorders. Otherwise, it may be continuously updated, stored in computer memory, and displayed on demand.

7.5.1.4.4 Additional Criteria for Categories 1 and 2

In addition to the criteria of Duke Position 7.5.1.4, the following criteria apply to Categories 1 and 2:

1. For Nuclear Safety Related (QA1) signals which are transmitted to non-safety related (non QA1) equipment, isolation devices are utilized.
2. Dedicated control board displays for the instruments designated as Types A, B, and C, Category 1 or 2 and qualified for use throughout all phases of an accident will be specifically identified on the control panels so that the operator can discern that they are available for use under accident conditions.

7.5.1.4.5 Additional Criteria for All Categories

In addition to the above criteria, the following criteria apply to all instruments identified in this document:

1. Servicing, testing, and calibration programs are specified to maintain the capability of the monitoring instrumentation. For those instruments where the required interval between tests will be less than the normal time interval between generating station shutdowns, the capability for testing during power operation is provided.
2. Whenever means for removing channels from service are included in the design, the design facilitates administrative control of the access to such removal means.
3. The monitoring instrumentation design minimizes the development of conditions that would cause meters, annunciators, recorders, alarms, etc., to give anomalous indications which are potentially confusing to the operator. Human factors guidelines are used in determining type and location of displays. The Duke Control Room Review Team made recommendations as to the type and location of displays, for added instrumentation.

4. To the extent practicable, the instrumentation is designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.
5. To the extent practicable, monitoring instrumentation inputs are from sensors that directly measure the desired variables.
6. To the extent practicable, the same instruments which are used for accident monitoring are used for the normal operations of the plant to enable the operators to use, during accident situations, instruments with which they are most familiar. However, where the required range of monitoring instrumentation results in a loss of necessary sensitivity in the normal operating range, separate instruments are used.
7. Periodic checking, testing, calibration, and calibration verification are in accordance with the applicable portions of the Oconee FSAR Chapter 7.

7.5.2 Description

Display instrumentation provided for Oconee operators is described below.

7.5.2.1 Reactor Coolant System Pressure

Three channels of Reactor Coolant System (RCS) Pressure indication are available through the plant operator computer (OAC), which receives the RCS Pressure signals through the Engineered Safety Features Actuation System (ESFAS) cabinets. This instrumentation is powered from a highly reliable battery backed source. These instrumentation channels monitor RCS pressure over the range 0 to 2500 psig. Two channels are recorded.

Two upgraded QA Condition 1 channels of Wide Range RCS Pressure indication are provided for post accident monitoring in response to Regulatory Guide 1.97. These instrumentation loops are seismically and environmentally qualified and are powered from safety grade emergency power sources. Signals to the Control Board readouts are processed through the Inadequate Core Cooling Monitoring (ICCM) system cabinets. The range for the readouts, 0-3000 psig, is in compliance with Regulatory Guide 1.97 specifications.

RCS pressure is a Type A Category 1 variable at Oconee, since the operator relies on this indication to determine when to switch from high pressure injection to low pressure injection.

Two upgraded QA Condition 1 channels of Low Range RCS Pressure indication are available via the Low Temperature Overpressure Protection (LTOP) System. These instrumentation loops are seismically and environmentally qualified and powered from safety grade emergency power sources. Although not required, the loops meet the RG 1.97 Category 1 instrumentation requirements of Section 7.5.1.4. The range for the readouts is 0-600 psig. The LTOP instrumentation loops are not credited in any design basis event. The instrumentation is classified as RG 1.97 Type D.

7.5.2.2 Inadequate Core Cooling Instruments

The Inadequate Core Cooling Monitor (ICCM) is of Westinghouse design. The ICCM system monitors hotleg level, reactor vessel head level, loop subcooling margin, core subcooling margin and core exit temperature and provides advanced warning of the approach to inadequate core cooling. The ICCM is a redundant two train Nuclear Safety-Related system powered by the vital instrumentation and control power system.

The microprocessor-based monitoring trains provide essential information to the control room operator so that conditions inherent to or leading to Inadequate Core Cooling (ICC) can be recognized and addressed.

The functions performed by the ICCM are as follows:

1. Assists in detecting a void or loss of level in the hotleg during natural circulation.
2. Indicates loss of subcooling margin.
3. Assists in detecting presence of a gas bubble or void in the reactor vessel head.
4. Assists in the detection of the approach to inadequate core cooling.

The ICCM system consists, on a per train basis of centrally located electronics/microprocessor cabinet, display electronics package, display selector key pad, and the plasma display unit on the main control board.

A description of each of the process sub-systems are described as follows.

7.5.2.2.1 Core Exit Temperature

There may be up to 52 Core Exit Thermocouples (CETs) per Oconee Unit. Twenty-four (12 per train) have been upgraded for accident monitoring and to meet seismic and environmental qualification requirements.

The plant computer is the primary display for up to 47 CETs of the 52. 5 CETs are displayed on the corresponding SSF unit console. The ICCM plasma displays (1 per train) located in the Control Room serve as safety related backup displays for the twenty-four nuclear safety qualified CETs. The range of the readouts is 50°F to 2300°F.

The ICCM CET function uses inputs from twelve incore thermocouples per train to calculate and display temperatures of the reactor coolant as it exits the core and to provide indication of thermal conditions across the core at the core exit.

Each of the twelve qualified thermocouples per train is displayed on a spatially oriented core map on the plasma display. The distribution of the monitored CETs in both trains assure minimum monitoring of at least four per core quadrant. Trending of CET temperature is available continuously on the plasma display. The average of the five hottest CETs is trendable for the past forty minutes.

Inputs to the plant computer for thermocouples used in the ICCM backup display is through qualified isolation devices. Power for the backup display is from safety grade emergency power sources, and power for the non-safety Operator Aid Computer (OAC) portion is from a highly reliable battery backed control bus. The plant computer and ICCM backup display are installed in a mild environment.

Core exit temperature is classified as a Type A Category 1 variable at Oconee because the operator relies on this information following a design basis event (LOCA) to secure HPI and throttle LPI, (SBLOCA) to throttle HPI and begin forced HPI cooling if needed, (MSLB, OTSG Tube Rupture) throttle HPI and isolate affected OTSG.

(RE: NSMs ON-1/2/32401)

7.5.2.2.2 Degrees of Subcooling Monitoring

The margin to saturation for the hotlegs and the reactor core are calculated from Reactor Coolant System (RCS) pressure and temperature measurements. The hotleg subcooling margin is calculated from wide range RCS pressure measurements and individual hotleg RTD temperature measurements. The hotleg subcooling margins are displayed in the Control Room on the ICCM plasma display unit. Train A displays the RCS Loop A hotleg subcooling margin while the Train B display provides RCS Loop B hotleg subcooling margin. Computer inputs are also provided for both hotlegs.

The reactor core subcooling margin is displayed in the Control Room in an identical manner. The core subcooling margin is calculated from the average of the five highest qualified Core Exit Thermocouples

(CET's) out of twelve inputs to each train of ICCM. This average value is then used with the RCS pressure measurement to calculate core subcooling margin.

The degrees of subcooling is also input to the plant computer through isolation buffers and is recorded on a recorder in the Control Room. The range of the degrees of subcooling readouts is 200°F subcooled to 50° superheat which envelopes the Regulatory Guide 1.97 range of 200°F subcooling to 35°F superheat.

Degrees of Subcooling Monitoring is classified as a Regulatory Guide 1.97, Rev. 2 Type A Category 1 variable at Oconee.

(RE: NSMs ON-1/2/32401)

7.5.2.2.3 Reactor Vessel Head and Hotleg Levels

The Reactor Vessel Head Level indicating system (RVHLIS) and Hotleg (HL) system are an adaptation of the Westinghouse RVLIS to the Babcock and Wilcox nuclear steam supply system. The HL and RVHLIS monitor the RCS for voids and loss of level conditions only under natural circulation.

The HL and RVHLIS uses two sets of two d/p (differential pressure) cells to measure both vessel and hot leg levels under natural circulation conditions. These cells are used to measure the pressure drop from the hot leg decay heat drop line connection to the top of the vessel, and from the hot leg decay heat drop line connection to the top of the candy cane on each hot leg. This differential pressure measuring system uses cells of differing ranges to cover natural circulation conditions.

This is a two train system containing Trains A and B which are physically separate and electrically isolated from each other. The trains perform the same function using identical but redundant inputs from differential pressure transmitters, impulse line temperature sensors, reactor coolant temperature sensors and wide range reactor coolant system pressure.

Software algorithms automatically perform compensation calculations required for variations in impulse line temperatures. Software also calculates and provides the necessary compensation for reactor coolant density.

Whenever the Reactor Coolant Pumps (RCPs) are running, the subcooling margin monitors and RCP monitor current meters are used to detect possible void conditions. Computer inputs are provided for both trains of level measurement. The Train A level measurements are recorded on a continuous recorder on the Main Control Board. The plasma displays for each train provide indication of both HL and RVHLIS in the Control Room.

Reactor Vessel Head and Hotleg Levels are classified as Regulatory Guide 1.97, Rev. 2 Type B Category 1 variables at Oconee.

7.5.2.3 Pressurizer Level

Two channels (2 level indications for Train “A” channel and 1 level indication for Train “B” channel)) of QA 1 instrumentation are provided for post accident monitoring the Pressurizer Level in response to Regulatory Guide 1.97, Revision 2. The indicated range is 0 to 400 inches which represents 11% to 84% level as a percentage of volume. Duke considers this range adequate for the intended monitoring function.

In order to determine the range or level that should be monitored for the pressurizer, it is important to understand how the pressurizer is sized and how the level taps are located. The pressurizer water volume is chosen such that the reactor coolant system can experience a reactor trip from full power without uncovering the level sensors in the lower shell and to maintain system pressure above the High Pressure Injection (HPI) system actuation setpoint. The steam volume is chosen such that the reactor coolant

system can experience a turbine trip without uncovering level sensors in the upper shell. Oconee has a 0 to 400 in range for pressurizer level based on these criteria. Although the installed range of instrumentation is not in complete compliance with the recommendation of Regulatory Guide 1.97, Revision 2, that pressurizer level be monitored from bottom to top, it is consistent with B&W NSSS requirements and is adequate for the intended monitoring function, including monitoring to ensure continued safe operation of pressurizer heaters.

The qualified instrument channels are powered by safety grade emergency power sources. Continuous recording is provided for one channel. The range for the instrumentation channels is 0 to 400 inches which Duke considers adequate for the intended monitoring function as referenced in the above paragraph.

Pressurizer level is classifed a Type A Category 1 variable at Oconee because the operator relies on this information following a design basis event (SBLOCA, OTSG Tube Rupture, MSLB) to throttle HPI.

(RE: NSMs ON-1/2/32448)

7.5.2.4 Steam Generator Level

Oconee has several different methods of Steam Generator level measurement and indication, as follows:

1. Start-up Range - Four transmitters (two per S/G) feed the ICS with signal ranges of 0" to 250". The four channels are used in the ICS for steam generator water level and feedwater control. The ICS employes median select between these signals and isolated signals from Item 4 below to control level and feedwater. The ICS displays the controlling level signal on a dual scale gage on the main control board.
2. Operate Range - Four transmitters (two per S/G) are combined with temperature compensation to feed two recorders with ranges of 0-100% (96"-388"). The four channels are switch selectable for feeding the recorders.
3. Full Range - Two transmitters (one per S/G) feed one dual gauge with ranges of 0 to 100% (0-650").
4. Extended Startup Range - Four transmitters (two per S/G) feed four gauges with ranges of 0" to 388".

Items 1 through 3 are used during normal plant operating conditions and are not required to meet Regulatory Guide 1.97, Type A, Category 1 Variable Requirements. These instruments may be used as backup verification for post accident monitoring to the extent they are available.

The instrumentation in Item 4 above is safety related and is used for post-accident monitoring. This instrumentation is powered by safety grade emergency power sources and the transmitters are seismically and environmentally qualified. Signal conditioning is provided by seismically and environmentally qualified equipment. Two transmitters, one per steam generator, provide electrically isolated level signals to the ICS for use in steam generator water level and feedwater control. The ICS will display these level signals if they have been selected for control on the control room indicator described in Item 1 above.

During accident conditions, the required range for a B&W once through steam generator is based on that level in the steam generator needed to recover from loss of subcooling margin conditions. The installed range of 0" to 388" ensures that the level required to restore subcooling margin as given in the emergency procedures can be measured.

Steam Generator Level is classified a Type A Category 1 variable at Oconee because the operator relies on this information following a design basis event (MSLB, OTSG Tube Rupture) to isolate affected OTSG.

(RE: NSMs ON-1/2/32447)

7.5.2.5 Steam Generator Pressure

Four QA Condition 1 channels, two channels per steam generator, are provided for post-accident monitoring steam generator outlet steam pressure in response to Regulatory Guide 1.97. Each instrument channel is seismically and environmentally qualified and powered from a safety grade source.

Each instrument channel inputs to the Inadequate Core Cooling Monitoring (ICCM) cabinets. The ICCM cabinets, Channel A and B respectively, provide safety inputs to two qualified indicators located on the Main Control Board in the Control Room. One channel per steam generator also provides an input to a recorder located in the Control Room. The ICCM system cabinets, channels A and B respectively, also provide non-safety inputs to the Operator Aid Computer (OAC). Safety train integrity is maintained by isolation buffers provided by the ICCM system cabinets. Additionally, each steam line has one QA Condition 1 channel of steam generator pressure instrumentation. These instrument channels along with corresponding ICCM steam generator instrumentation provide input signals into the Automatic Feedwater Isolation System (RE: NSM-ON-1/2/33053).

Each steam generator has two non-safety related channels of steam generator outlet pressure instrumentation (total of four) used for control by the ICS. In addition, two channels of QA-1 steam generator outlet pressure instrumentation used in the Automatic Feedwater Isolation System (AFIS) logic are electrically isolated and provided to the ICS for control. This makes a total of six pressure signals, three per steam generator, for use in the ICS for control. Each group of three pressure signals (3 - OTSG "A", 3 - OTSG "B") are used in median select strategy by the ICS for control. The control signal used in the ICS for each steam generator is provided for indication on the main control board. The indicated range is 0 - 1200 psig which corresponds to 14% above the lowest main steam safety relief valve setting and 8% above the highest safety valve setting. An additional channel of QA-steam generator outlet pressure instrumentation on each header is used in AFIS. All eight signals, four per steam generator, are also input to the plant computer (OAC) and trend recording is available to the control room operator if demanded. The non-safety related instrumentation is powered from highly reliable battery backed buses. The safety-related (QA-1) instrumentation is powered from the QA-1 vital instrumentation and control battery backed buses.

The main steam lines are provided with safety relief valves, atmospheric dump valves and condenser dump valves to prevent over pressurization of the lines as well as pressure control. Operability of the main steam safety valves ensures that the secondary system pressure will be limited to within its design pressure (1050 psig) during the most severe anticipated system operating transient. With an assumed 3% accumulation when these safety valves are operating, the maximum pressure while they are relieving will be less than 10% above design pressure. Also the Facility Operating License limit the plant power and thus steam flow in order to maintain that excess relief capacity. Therefore, based on the facts that the, highest safety valve setting is 1104 psig, the steam relief capacity is 17% above the expected steam flow rate and that excess relief capacity is maintained when safety valves are inoperable, the existing range of 0 to 1200 psig is sufficient for this variable.

Steam Generator Pressure is classified a Type A Category 1 variable at Oconee because the operator relies on this information following a design basis event (MSLB, OTSG Tube Rupture) to isolate affected OTSG.

(RE: NSMs ON-1/2/32447)

7.5.2.6 Borated Water Storage Tank Level

Three QA Condition 1 channels of level instrumentation are provided for normal and post accident monitoring the Borated Water Storage Tank (BWST) level. Each channel is seismically qualified. Two channels are powered from a safety grade source and the third channel has a safety and a non-safety grade power distribution. Signals to the Control Board are processed through the Inadequate Core Cooling

Monitoring (ICCM) system cabinets. The range for the readouts, 0 to 50 ft (13%-100% of volume), is in compliance with Regulatory Guide 1.97, Rev. 2.

Two of the three QA Condition 1 instrumentation channels provide inputs to the ICCM system cabinets, Train A and B respectively. The ICCM cabinets provides safety inputs to qualified indicators on the Control Board and non-safety inputs to the Operator Aid Computer (OAC). Safety train integrity is maintained through the use of isolation buffers provided by the ICCM system.

The third channel of qualified instrumentation provides a safety input from train B to a recorder (through a qualified isolator). This channel also provides input to the computer and various annunciators via an optical isolator which maintains safety train B integrity.

BWST level is classified a Type A Category 1 variable at Oconee because the operator relies on this information following a design basis event (LOCA, SB LOCA) to realign LPI to take suction from RB sump.

(RE: NSMs ON-1/2/32450)

7.5.2.7 High Pressure Injection System and Crossover Flows

Two channels of QA condition 1 instrumentation are provided for post accident monitoring of High Pressure Injection (HPI) flow in response to Regulatory Guide 1.97. Each channel is seismically and environmentally qualified and powered from a safety grade source. Each channel signal, A and B respectively, inputs to a recorder and qualified indicator via the Inadequate Core Cooling Monitoring (ICCM) system cabinets. Two channels of QA condition 1 instrumentation are also provided for monitoring HPI crossover flow. These instrument channel signals directly input to qualified indicators on the Control Board. HPI System and Crossover Flow instrumentation channels monitor flow over the range 0 - 750 gpm which envelopes the 0 to 110% design flow criteria of Regulatory Guide 1.97, Rev. 2.

The ICCM cabinets also provide non-safety inputs to the Operator Aid Computer (OAC) and annunciator points. Safety channel integrity is maintained through the use of isolation buffers provided in the ICCM.

HPI System flow is a Type A Category 1 variable at Oconee because the operator relies on this information following a design basis event (LOCA, SB LOCA, MSLP, OTSG Tube Rupture) to throttle HPI and initiate HPI bypass (if necessary).

(RE: NSMs ON-1/2/32589)

7.5.2.8 Low Pressure Injection System Flow

Two QA Condition 1 instrumentation channels are provided for normal and post accident monitoring Low Pressure Injection (LPI) flow in response to Regulatory Guide 1.97. Each channel is seismically and environmentally qualified and powered from a safety grade source. Each channel signal, train A and B respectively, inputs to a qualified indicator and a recorder via the Inadequate Core Cooling Monitoring (ICCM) system cabinets. These channels monitor LPI flow over the range 0-4000 gpm which envelopes the 0-110% of design flow criteria for Regulatory Guide 1.97.

The ICCM cabinets also provide non-safety inputs to the Operator Aid Computer (OAC) and annunciator points. Alarms generated in the ICCM cabinets provide high and low LPI flow and low Decay Heat removal flow for each train. Safety train integrity is maintained through the use of isolation buffers provided by the ICCM. Two non-qualified transmitters, one per train, also provide non-safety inputs to the OAC.

LPI System is a Type A Category 1 variable at Oconee because the operator relies on this information following a design basis event (LOCA, SB LOCA) to terminate HPI flow.

(RE: NSMs ON-1/2/32587)

(RE: NSMs ON-1/2/33093)

7.5.2.9 Reactor Building Spray Flow

Two QA Condition 1 instrumentation channels are provided for post accident monitoring Reactor Building Spray flow in response to Regulatory Guide 1.97. Each instrumentation channel is seismically and environmentally qualified and powered from a safety grade source. Each instrument channel signal, train A and B respectively, inputs to a qualified indicator and a recorder via the inadequate core cooling monitoring (ICCM) cabinets. These channels monitor Reactor Building Spray flow over the range 0-1500 gpm which envelopes the Regulatory Guide 1.97 range requirement of 0-110% of design flow.

The ICCM cabinets also provide non-safety inputs to the Operator Aid Computer (OAC), annunciator, and a non-safety indicator located in the Control Room. Safety train integrity is maintained through the use of isolation buffers provided by the ICCM system. Also provided is two non-safety instrument channels which provide non-safety inputs to the OAC.

For all units at Oconee, throttling is not required, and the RBS flow variable is classified as Type D Category 1 for indication of continued operation of the RBS system to support long term cooling requirements and iodine removal. However, this instrument is only required to meet Category 2 requirements.

(RE: NSMs ON-1/2/32588 and ON-1/2/33105)

7.5.2.10 Reactor Building Hydrogen Concentration

Two redundant channels of nuclear safety related instrumentation monitor reactor building hydrogen concentration. The reactor building hydrogen monitoring system meets the requirements of NUREG 0737, Item II.F.1.6, and is described in more detail in Section 9.3.7 of the UFSAR. The indicated range is from 0 to 10% concentration which envelopes the Regulatory Guide 1.97 range requirements.

Both channels are powered by safety grade emergency buses. Control of the sample line switching valves and sample selector solenoid valves is accomplished at the analyzer remote control panel. These instruments are seismically and environmentally qualified.

Reactor Building Hydrogen Concentration is classified as a Regulatory Guide 1.97, Rev. 2 Type E Category 3 variable at Oconee.

7.5.2.11 Upper Surge Tank and Hotwell Level

Oconee's Emergency Feedwater System (EFDW) draws condensate grade suction primarily from the Upper Surge Tanks and supplementarily from the Condenser Hotwell. Condensate may also be provided from the Condensate Storage Tank (CST) and the Makeup Demineralizers. Additional backup of the two normal condensate sources is provided by these same locations associated with the other two units. The level transmitters which monitor Upper Surge Tank and Hotwell level are located in the Turbine building which is a mild environment.

Instrumentation is available to monitor Hotwell level in the Control Room. The plant computer system is provided to display both current and past values of this variable. Hotwell level is not calssified as a Regulatory Guide 1.97 variable at Oconee.

Two QA Condition 1 instrumentation channels are provided for monitoring Upper Surge Tank (UST) level in response to Regulatory Guide 1.97. These instrument channels are seismically qualified and powered from a safety grade source. Each instrument channel, train A and B respectively, input to the Inadequate Core Cooling Monitoring (ICCM) system cabinets. The ICCM Train A cabinet provides safety inputs to a qualified indicator and to a recorder (through a qualified isolator), both located in the

Control Room to provide UST level indication. The ICCM Train B cabinet also provides a safety input to a qualified indicator located in the Control Room. The range of UST level indication is 0 - 12 feet.

The ICCM cabinets, Train A and B respectively, also provide non-safety inputs to two computer alarm points and one annunciator window. Safety train integrity is maintained through the use of isolation buffers provided by the ICCM system.

Upper Surge Tank level is a Type A Category 1 variable at Oconee because the operator relies on this information following a design basis event.

(RE: NSMs ON-1/2/32449)

7.5.2.12 Neutron Flux

Oconee has four channels of neutron flux for the source range, and four wide range QA Condition 1 channels of full range neutron flux instrumentation which are environmentally qualified for post-accident monitoring. Five (four for Unit 1; four for Unit 3) neutron flux channels exist for the power range. The indicated ranges are: Source Range 10^{-1} to 10^{5} cps, -1.0 to +7.0 decade/min. rate of change; Wide range (Post-Accident Monitoring channels) 10^{-8} to 200% power, -1 to +7 decade/min. rate of change; and Power Range, 0 to 125%.

NI-1,-2,-3, and -4 channels are environmentally qualified and powered from safety grade busses and encompass the 10^{-6} to 100% Full Power range in response to Regulatory Guide 1.97, Rev. 2. NI-1, -2, -3, and -4 channels are Type B Category 1 variables at Oconee. All other NI channels are designed for the normal Reactor Building Environment for the safety function of overpower reactor trip but they are not environmentally qualified for post-accident operation.

Operator information is provided as follows:

1. Thirteen (twelve for Unit 1; twelve for Unit 3) Control Room indicators (Four source, four wide, five [four for Unit 1; four for Unit 3] power)
2. Twenty-one (twenty for Unit 1; twenty for Unit 3) computer points (Eight source, eight wide range, and five [four for Unit 1; four for Unit 3] power)
3. Trend recording on demand
4. One QA Condition 1 Wide Range channel recorded on a recorder. One source range, wide range, and power range channel recorded, four (two power range) channels accessible on a Non-QA Condition recorder.

(RE: NSMs ON-1/2/32596 and 1/2/32909)

7.5.2.13 Control Rod Position

Each control rod's position is indicated on an analog display which has two switchable input modes for the full 0 to 139 inch range. In addition, separate Full In and Full Out indicating lights are provided for each control rod. Analog computer points are provided for each control rod's position. Analog computer points are also provided for control rod groups 5, 6, 7 and 8, for zero to 100% rod position corresponding to the full 0 to 139 inch range. This instrumentation is powered from a highly reliable battery backed source. Control Rod Position is classified as a Regulatory Guide 1.97, Rev. 2 Type B Category 3 variable at Oconee. (Re: FSAR 4.5.3).

Operator information is provided as follows:

1. Indicating lights for Full In or Not Full In for all control rods.
2. Analog display full range for all control rods.

3. Computer inputs for all control rods and all control rod groups 5, 6, 7, and 8. Trend recording on demand.

7.5.2.14 RCS Soluble Boron Concentration

This variable is monitored by sampling and laboratory analysis. Primary system boron concentration is controlled manually with the sampling frequency determined by plant conditions and operating procedures.

7.5.2.15 Reactor Coolant System Cold Leg Water Temperature

Oconee has indication of Reactor Coolant System (RCS) Cold Leg Temperature for each of the four cold legs. The instrumentation is powered from a highly reliable battery backed source. The indicated range is 50° to 650°F. Additional diversity is provided by the Hot Leg Water Temperature and Core Exit Temperature Instruments.

The RCS Cold Leg Water Temperature is used as a backup for the key variable of Hot Leg Temperature and Core Exit Temperature. Because the Hot Leg and Cold Leg RTD's are located in the RCS loops and not in the reactor vessel, either forced or natural circulation is required through the steam generators for their indication to be representative of actual core conditions. When circulation is present, the 650°F high end of the range provides 18% excess measurement capability based on a steam generator design pressure of 1050 psig and a saturation temperature of approximately 553°F for the Oconee design. Because the RCS Cold Leg Temperature is not used in the ATOG guidelines and functions as backup to the other two variables, it is appropriate to classify this variable as a Type B Category 3. The existing design is adequate for the intended monitoring function.

7.5.2.16 Reactor Coolant System (RCS) Hot Leg Water Temperature

Two qualified, QA condition 1 channels, are provided for post-accident monitoring Wide Range RCS Hotleg Water Temperature in response to Regulatory Guide 1.97 Rev. 2. These instrument channels are powered from safety grade emergency power sources. The indication readouts are located in the Control Room in a mild environment. This variable inputs to the plant computer through isolation buffers and is recorded on a recorder in the Control Room. (RE: NSMs ON-1/2/32401). The range of the readouts is 50 to 700°F which Duke considers adequate for the intended monitoring function. Also note, this range is in compliance with the recommendations of Revision 3 to RG 1.97. Control room display is through the inadequate Core Cooling Monitoring system. RCS Hot Leg Water Temperature is classified as a Regulatory Guide 1.97, Rev 2 Type A Category 1 variable at Oconee.

7.5.2.17 Reactor Building Sump Water Level Narrow Range

Two channels of instrumentation monitor both the Normal Sump Level (0 to 2 feet, approximately 350 gallons excluding embedded piping) and the Emergency Sump Level (0 to 3 feet, approximately 4000 gallons). This instrumentation is environmentally qualified and powered from safety grade emergency power buses. Qualified backup indication is provided by the Wide Range Sump Level instrumentation. Reactor Building Sump Water Level Narrow Range is classified as a Regulatory Guide 1.97, Rev. 2 Type B Category 2 variable at Oconee and, with the Reactor Building Sump Water Level instrument in Section 7.5.2.18 below, meets the requirements of NUREG 0737, Item II.F.1.5 as described in Section 5.2.3.10.5 of the UFSAR.

(Re: FSAR 3.4.1.1.2).

(RE: NSM ON-2248)

7.5.2.18 Reactor Building Sump Water Level

Two redundant QA Condition 1 channels of level instrumentation are provided for measuring reactor building sump water level from the bottom of the Reactor Building to approximately five feet above the maximum flood elevation which exceeds the 600,000 gallon level. The indicated range is 0 to 15 feet. Redundancy/diversity is provided by the Borated Water Storage Tank Level and the Narrow Range Sump Level indicators. The instrumentation channels are environmentally and seismically qualified and powered by safety grade emergency power buses. Reactor Building Sump Water level is classified as a Regulatory Guide 1.97, Rev. 2 Type B Category 1 variable at Oconee and, with the Reactor Building Sump Water Level Narrow Range instrument described in Section 7.5.2.17 above, meets the requirements of NUREG 0737, Item II.F.1.5 as described in Section 5.2.3.10.5 of the UFSAR.

(Re: FSAR 3.4.1.1.2).

7.5.2.19 Reactor Building Pressure

Two redundant QA Condition 1 channels of instrumentation are provided for monitoring Reactor Building Pressure in accordance with the requirements of NUREG 0737, Item II.F.1.4. The instrumentation channels are environmentally and seismically qualified and powered by safety grade emergency power buses. The indicated range is -5 to 175 psig with the reactor building design pressure being 59 psig. This instrumentation range covers nearly 99% of the recommended Regulatory Guide 1.97, Revision 2, range of 10 psig to 3 times the design pressure (177 psig). Duke considers the indicated range adequate for the intended accident monitoring function. Reactor Building Pressure is classified as a Regulatory Guide 1.97, Rev. 2 Type B Category 1 variable at Oconee.

7.5.2.20 Reactor Building Isolation Valve Position

All electrically controlled reactor building isolation valves that are active to close for containment isolation have control switches on the main control boards. Actual valve position is provided by QA Condition 1 limit switches on the valves which operate both Closed-Not Closed, and Open-Not Open control switch indicating lights. These valves are powered by safety grade emergency power buses. Additional indication is provided by the computer. Redundancy is not necessary on a per valve basis since redundant barriers are provided for all fluid penetrations as discussed in the Oconee FSAR Section 6.2.3.2. Environmental qualification of the limit switches is described in the Oconee FSAR section 3.10 and the Oconee Nuclear Station Seismic Design Criteria (OSDC-0193.01-00-00001). Reactor Building Isolation Valve Position is classified as a Regulatory Guide 1.97, Rev. 2 Type B Category 1 variable at Oconee.

7.5.2.21 Radiation Level in Primary Coolant

Oconee has one channel of primary coolant radiation level instrumentation which monitors the Reactor Coolant and Letdown Line and is isolated upon ESF actuation signal. The channel is powered from a highly reliable battery backed bus. The indicated range is 10^1 to 10^6 counts per minute which covers reactor coolant concentration of approximately 10^{-3} uCi/ml to 10^3 uCi/ml (see the Oconee FSAR, Section 11.5).

Deleted paragraph(s) per 2005 update

7.5.2.22 Accident Sampling Capability, Primary Coolant, Primary Coolant Sump, Containment Air

The existing design of the sampling system for the primary coolant, the Reactor Building sump and Reactor Building air allows samples to be taken for laboratory analysis. Samples from other plant

systems including various auxiliary building sumps can be obtained from sample points on system piping and/or storage tanks.

Deleted paragraph(s) per 2005 update

7.5.2.23 Reactor Building Area Radiation - High Range

Oconee has two redundant QA Condition 1 channels of Reactor Building high range radiation monitoring instrumentation. Each channel is powered by safety grade emergency power. The indicated range is 1 to 10^8 R/hr. Diversity is provided by portable instrumentation or by sampling and analysis. The instrumentation is seismically and environmentally qualified. Reactor Building high range radiation monitoring instrumentation is classified as a Regulatory Guide 1.97, Rev. 2 Type C Category 1 variable at Oconee.

7.5.2.24 Airborne Process Radiation Monitors

Airborne process radiation monitors exist for monitoring ventilation exhausts and the condenser air ejector exhaust (see Oconee FSAR, Section 11.5 and Table 11-7). However, in accordance with RG 1.97, Rev. 2 these individual airborne process radiation monitors are not required for accident monitoring due to the fact that ventilation systems and the condenser air ejector exhaust to the common unit vent (See Oconee FSAR, Section 7.5.2.52).

7.5.2.25 Area Radiation

Oconee has an extensive Area Radiation Monitoring System installed for personnel protection. Channel detector locations were selected based on areas normally having free access and low radiation dose rates with the potential of having abnormal radiation levels. These channels have an indicated range of 10^{-1} to 10^7 mr/hr. Redundant indication can be provided by portable instrumentation. The channels are powered by a highly reliable non load shed power bus capable of receiving power from the on-site emergency power sources. See the Oconee FSAR, Section 12.3.3.

The environmental qualification of some of the instrumentation is not in compliance with the recommendations of Regulatory Guide 1.97, Revision 2. However, the qualification is within the guidance provided for Type C Category 3 instrumentation which Duke considers adequate for the intended monitoring function. Also note, this is in compliance with the recommendations of RG 1.97, Rev. 3. Continuous recording is not required for the intended monitoring function.

7.5.2.26 Decay Heat Cooler Discharge Temperature

Each train of the Oconee LPI system contains instrumentation to monitor decay heat cooler discharge temperature which is referred to in Regulatory Guide 1.97, Revision 2, as RHR Heat Exchanger Outlet Temperature. The range for this instrumentation is 0 to 400°F, and the power supply is a highly reliable battery backed control bus. Each train is environmentally qualified per the IEB-79-01B submittal methodology and envelopes the Regulatory Guide 1.97, Rev. 2 range of 32° to 350°F. Decay Heat Cooler Discharge Temperature is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 2 variable at Oconee.

7.5.2.27 Core Flood Tank Level

Oconee has two channels of tank level instrumentation on each of the two core flood tanks. Power for these channels is provided by highly reliable battery backed buses. The indicated range for Units 1, 2 and 3 is 1.5 to 14 feet which corresponds to approximately 22% to 83% of the core flood tank volume. The equipment is located in a harsh environment.

The range and environmental qualification of this instrumentation is not in total compliance with the recommendations of RG 1.97, Rev. 2, which recommends a range of 10% to 90% volume and Category 2 classification.

The primary function of this instrumentation is to monitor the pre-accident status of the core flood tanks to assure that this passive safety system is prepared to serve its safety function. The indicated range envelopes the Technical Specification level requirements and Duke Power considers the range adequate to meet the intended monitoring function. This instrumentation plays no significant role in the subsequent management of an accident. Therefore, Core Flood Tank Level is not a key variable for accident monitoring and is considered to be Type D Category 3 instrumentation. The level of environmental qualification provided for the instrumentation in this system is consistent with the performance expectations of the system and meets the recommendations of Type D Category 3 in Duke's interpretation of RG 1.97, Rev. 2.

7.5.2.28 Core Flood Tank Pressure

Oconee has two channels of core flood tank pressure instrumentation on each of the two core flood tanks. Power for these channels is provided by highly reliable battery backed buses. The indicated range is 0 to 700 psig. The tanks are pressurized to 600 psig under normal operating conditions.

The primary function of this instrumentation is to monitor the pre-accident status of core flood tanks to assure that this passive safety system is prepared to serve its safety function. This instrumentation plays no significant role in the subsequent management of an accident. Therefore, Core Flood Tank Pressure is not a key variable for accident monitoring and is considered to be Category 3 instrumentation. The installed system meets the Duke interpretation of Type D Category 3 recommendations. Regulatory Guide 1.97, Revision 2, classifies this variable as Category 2.

The range of this instrumentation is not in total compliance with the recommended 0 to 750 psig range of Regulatory Guide 1.97, Revision 2. However, the indicated range covers approximately 0 to 117% of the operating pressure of the tanks. Because the purpose of this variable is to monitor and maintain Core Flood Tank pressure during normal operation to Technical Specification (TS) limits, the range of this variable should provide some margin above that TS limit. Since the Oconee TS limit is 600 ± 25 psig, a high range value of about 700 psig will provide greater than 10% excess range measurement capability and will therefore be sufficient. Duke Power considers the instrumentation adequate for the intended monitoring function.

7.5.2.29 Core Flood Tank Isolation Valve Position

The core flood tank isolation valves are provided with control switches on the main control board. During normal plant operation, power is removed from the valve operators to prevent a spurious signal from inadvertently closing the valves. The indicating lights are powered from a separate highly reliable battery backed bus and give actual valve position of both Closed-Not Closed and Open-Not Open. Environmentally qualified limit switches are provided for the core flood tank isolation valves.

Core Flood Tank Isolation Valve Position is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 2 variable at Oconee.

7.5.2.30 Boric Acid Charging Flow

Oconee NSSS does not include a charging system as part of the Emergency Core Cooling System (ECCS). Flow paths from the ECCS to the RCS include high pressure injection (HPI) and low pressure injection (LPI) with the BWST or the RB Sump as the suction source, and the Core Flood Tank injection. HPI and LPI flow rates are monitored, and BWST, Reactor Building Sump, and Core Flood Tank levels

are monitored by RG 1.97 variables. Therefore, Boric Acid Charging Flow monitoring is not applicable to the operation of the ECCS and is not a Type D variable for Oconee.

7.5.2.31 Reactor Coolant Pump Status

The indicated range for RCP motor current is from 0 to 1200 amps. The instrumentation derives power from the monitored source and is adequate for the intended monitoring function. The RCP motor current instrumentation is classified as a Regulatory Guide 1.97, Rev. 2 Type D Categroy 3 variable at Oconee.

7.5.2.32 Power Operated Relief Valves Status

An acoustical leak detection monitoring system is the primary instrumentation for determining PORV position. It is a single channel system powered from a highly reliable battery backed bus. It provides the operator with positive indication of valve position by indicating fractional flow through the valve in ten steps from 0.01 to 1.0. Backup indication of PORV position is provided by limit switch operated indicating lights and PORV outlet temperature indication. The system was specified and is rated to operate in all environmental conditions for its location. Power Operated Relief Valves status is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 2 variable at Oconee.

(RE: NSMs ON-1/2/32594)

7.5.2.33 Primary System Safety Relief Valve Positions (Code Valves)

Acoustical leak detection monitoring systems are the primary instrumentation for determining code valves position. Each code valve has a single channel system powered from highly reliable battery backed bus. It provides the operator with positive indication of valve position by indicating fractional flow through the valve in ten steps from 0.01 to 1.0. Backup indication of code valve position is provided by valve outlet temperature indication. The system was specified, and is rated to operate in all environmental conditions for its location. Primary System Safety Relief Valve Position is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 2 variable at Oconee.

(RE: NSMs ON-1/2/32594)

7.5.2.34 Pressurizer Heater Status

Control indicating lights are used for indication of the ON/OFF status of the pressurizer heater groups. Indicating lights are powered by highly reliable battery backed busses. This monitoring instrumentation is located in a mild environment.

ON/OFF status of the pressurizer heaters provides the operator adequate information for Design Basis events. Additionally, RCS pressure can be monitored to determine the effectiveness of the heaters to maintain system pressure. Duke feels that this is adequate for the intended monitoring function, and that monitoring of electric current per Regulatory Guide 1.97, Revision 2, recommendations is not necessary. Pressurizer Heater status is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 2 variable at Oconee.

7.5.2.35 Quench Tank Level

The indicated range of Quench Tank Level is from 0 to 125" corresponding to tank volume of approximately 15-96%. This range is not in complete compliance with RG 1.97, Rev. 2, which recommended top to bottom tank monitoring, however, the upper range meets the intended monitoring function. No useful information would be gained by measuring tank volume from 0-15%. Normal level (pre-accident) is maintained above 15% and post-accident condition will only increase tank level.

Therefore, the existing range is adequate for the intended monitoring function. Quench Tank Level is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 3 variable at Oconee.

7.5.2.36 Quench Tank Temperature

The indicated range of the Quench Tank temperature is from 50° to 350°F. The design temperature of the Quench Tank is 300°F which is approximately the maximum temperature reached in the tank during a design transient. The tank design pressure is 55 psig, and the rupture disc pressure is 55 psig. The saturation temperature for 55 psig is approximately 300°F. Thus, the indicated range of 50°F to 350°F will adequately measure the expected maximum temperature as well as saturation temperature for the Quench Tank. Quench Tank Temperature is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 3 variable at Oconee.

(RE: NSMs ON-1/2/32593)

7.5.2.37 Quench Tank Pressure

The indicated range of the Quench Tank pressure is from 0 to 60 psig. The tank rupture disc is designed to relieve at 55 psig, and the tank design pressure is 55 psig. Therefore, the installed instrumentation is adequate for the intended monitoring function. Quench Tank Pressure is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 3 variable at Oconee.

7.5.2.38 Main Steam Safety Valve Position

This variable is not monitored directly. The positions of the Main Steam Safety Valves (MSSV) are not required to mitigate the consequences of a design basis accident. Direct indication of safety valve position is not provided but indirect indication is provided via control room indication of steam generator pressure. During Duke's Control Room Design Review, a specific Task Analysis Evaluation of MSSV indication was undertaken. This evaluation dealt with steam leak transients with and without MSSV indication. As a result of this evaluation, direct MSSV indication was found not necessary. Also, sound emitted from the valves provides an audible indication to the operators when the valves lift. Duke feels that this is adequate indication for the intended monitoring function.

7.5.2.39 Main Feedwater Flow

Each feedwater line has three main feedwater flow transmitters. The indicated range for this variable is 0 to 6.0×10^6 lbs/HR which corresponds to 0 to 111% of design flow. Main Feedwater Flow is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 3 variable at Oconee.

7.5.2.40 Emergency Feedwater Flow

Oconee has four QA Condition 1 flow transmitters, two per steam generator monitoring Emergency Feedwater Flow from all EFDW pumps to each steam generator. The indicated range for this variable is 0 to 1200 GPM which corresponds to a range of 0 to 115% design flow. This instrumentation is powered from a safety grade emergency power source. The flow transmitters are located in a mild environment. Seismic qualification methodology for these transmitters is as described in the Oconee FSAR, Section 3.10. The indicators are located in the control room which is classified as a mild environment. Emergency Feedwater flow to each steam generator is recorded on separate recorders in the Control Room. Emergency Feedwater Flow is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 1 variable at Oconee.

7.5.2.41 Reactor Building Fan Heat Removal

The key variable for monitoring Reactor Building Cooler performance is Reactor Building Pressure instrumentation which is Type B Category 1. Backup instrumentation includes Nuclear Safety Related indication of each Reactor Building Cooler Fan motor starter status (high and low speed lights), each Fan motor starter status on the computer, indication of each Fan motor amperage, indication of inlet and outlet cooling water flow to each cooler, and inlet and outlet air temperature indication for each cooler. All of the above indications are provided in the Control Room. The installed instrumentation is adequate for the intended monitoring functions. For backup indications, the level of environmental qualification provided for the instrumentation is consistent with the performance expectations of the instrumentation and meets the recommendations of Type D Category 3 in Duke's interpretation of RG 1.97, Rev. 2.

7.5.2.42 Reactor Building Air Temperature

Thirteen dual element thermocouples are provided to measure Reactor Building air temperature on Units 1 & 2. Twelve dual element thermocouples are provided on Unit 3. One element of each T/C provides an input to the plant computer and the second element of each T/C, except for Unit 2, provides an input to a multi-channel recorder. On Units 1 and 3, the T/C input into the recorders is retransmitted to the OAC via an analog output card on board the recorders. Unit 2, for the present sends both T/C elements directly to the OAC. The plant computer and the recorders display a range of 0 to 400°F. The plant computer is powered by highly reliable battery backed busses.

The displayed ranges are adequate for the intended monitoring function. The worst case DBA temperature in the Reactor Building is 286°F. For accidents in which harsh RB environments are a result, pressure and temperature are coupled such that as RB pressure is reduced the temperature is also reduced. Therefore, RB pressure is considered the priority variable with temperature as a Category 3 backup variable. The level of environmental qualification provided for this instrumentation is consistent with its performance expectations and meets the recommendations of Type D Category 3 in Duke's interpretation of RG 1.97, Rev. 2.

7.5.2.43 Makeup Flow

The existing instrumentation for this variable provides continuous monitoring of reactor coolant makeup flow. The loop range is 0 to 160 gallons per minute which encompasses the Regulatory Guide 1.97, Rev.2 criteria of 0-110% of design flow. Design flow is 35 GPM. The instrumentation is located in a mild temperature environment.

The transmitter for this variable is not rated to withstand the anticipated maximum design basis accident radiation dose for the installed location. The installed instrumentation is adequate for the intended monitoring function. For accidents in which harsh environments are a result, the portion of the system containing this instrumentation is not required for the mitigation of these accidents and is automatically bypassed upon an ESF Actuation. Therefore, Makeup Flow is not a key variable for accident monitoring and is considered to be Category 3, instrumentation. The level of environmental qualification provided for the instrumentation in this system is consistent with the performance expectations of the system and meets the recommendations of Type D Category 3 in Duke's interpretation of RG 1.97, Rev. 2.

7.5.2.44 Letdown Flow

The existing instrumentation for this variable provides continuous monitoring of reactor coolant letdown flow. The loop range is 0 to 160 gallons per minute which envelopes the Regulatory Guide 1.97, Rev. 2 criteria of 0-110% of design flow. Design flow is 70 GPM. This instrument loop is powered from a highly reliable battery backed bus. The instrumentation is located in a mild temperature environment.

The transmitter for this variable is not rated to withstand the anticipated maximum design basis accident radiation dose for the installed location.

The installed instrumentation is adequate for the intended monitoring function. For accidents in which harsh environments are a result, the portion of the system containing this instrumentation is not required for the mitigation of these accidents and is automatically isolated upon an ESF Actuation. Therefore, Letdown Flow is not a key variable for accident monitoring and is considered to be Category 3 instrumentation. The level of environmental qualification provided for the instrumentation in this system is consistent with the performance expectations of the system and meets the recommendations of Type D Category 3 in Duke's interpretation of RG 1.97, Rev. 2.

7.5.2.45 Letdown Storage Tank Level

The existing instrumentation for this variable provides continuous monitoring of the letdown storage tank level. The loop range is 0 to 100 inches which covers the linear portion of the tank (approximately 16 to 84% of tank volume). This instrument loop is powered from a highly reliable battery backed bus. This instrumentation is located in a mild environment.

Minimum and maximum letdown storage tank levels are maintained within the range of the instrument. Extending the range into the domed portions of this tank would result in nonlinear readings at each extreme of the scale. The installed range is adequate for measuring letdown storage tank level. The installed instrumentation is adequate for the intended monitoring function. This tank is not required to be utilized during an accident. As a commitment to the NRC, Duke is voluntarily upgrading this LDST level instrumentation to Type D Category 2 Nuclear Safety Related (QA-1). This change was performed on Unit 3 during the 3EOC17 refueling outage, and will be implemented on the other units in subsequent outages. This upgraded instrumentation is also adequate to perform the intended monitoring function. (Ref NSM x-2885)

7.5.2.46 Low Pressure Service Water Temperature to ESF System

The Oconee system for providing cooling water to ESF components is the Low Pressure Service Water System (LPSW). The temperature of LPSW is essentially the same as the temperature of Lake Keowee at the CCW pump suction. There is no control over the temperature of the LPSW; therefore, there is no need to indicate the LPSW temperature in the control room since no operator action is taken based on this temperature and, by design, no useful information would be provided to the operator by such instrumentation.

7.5.2.47 Low Pressure Service Water Flow to ESF Systems (Pressure)

The Oconee system for providing cooling water to ESF components is the Low Pressure Service Water System (LPSW). Primary indication of proper LPSW system and pump operation is line pressure measured in each of the two LPSW headers. The indicated range is 0 to 100 psig for a system design pressure of 100 psig. These instruments are located in a mild environment and powered by a highly reliable battery backed source which meets Type D Category 2 requirements. LPSW header pressure is a valid measurement of system and pump operation and Duke considers the existing indications to meet the intent of Regulatory Guide 1.97, Rev. 2.

Additional instrument loops provide backup indication in the Control Room of proper system operation. These include LPSW pump motor amperage, valve position indication on valves operated in the control room, inlet and/or outlet cooling water flow for certain ESF coolers, and flow and pressure alarms. For backup variables, a design qualification of Type D Category 3 is adequate for the intended monitoring functions and consistent with the performance expectations of the instrumentation.

(RE: NSMs ON-1/32590)

7.5.2.48 RC Bleed Holdup Tank Level

The indicated range for this variable is 0 to 180 inches for the RC Bleed Holdup tank. This level indication corresponds to a tank volume of approximately 1% to 99%. Although the range is not in complete compliance with the recommendation for a RG 1.97, Rev. 2 Type D Category 3 variable (top to bottom), the tap to tap range of the installed instruments is adequate to provide tank level information for all design basis events. Duke considers the installed instrumentation adequate for the intended monitoring function.

7.5.2.49 Waste Gas Decay Tank Pressure

Oconee utilizes two tanks per unit for radioactive waste gas storage. The maximum operating pressure for these tanks is approximately 100 psig (per Oconee FSAR, Section 11.3). The indicated range is 0 to 150 psig for each tank, which is adequate for the intended monitoring function. Waste Gas Decay Tank Pressure is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 3 variable at Oconee.

7.5.2.50 Emergency Ventilation Valve Position

There are three Emergency Ventilation Systems at Oconee; Reactor Building Purge, Penetration Room Ventilation, and Reactor Building Cooling. Each system has indication that the required emergency alignment has been achieved in the control room. (Penetration Room Ventilation is no longer required due to adoption of alternate source term.)

For the Reactor Building Purge System direct indication of containment isolation valves position is provided. The in-containment isolation valves (PR-1, 6) are MOVs whose position indication is provided by internal limit switches. These valves are not in the EQ program because they are racked-out during normal operation and are not required to function during a design basis event. This instrumentation is powered from safety grade emergency power. The out-of-containment isolation valves (PR-2, 5) are AOVs and positive indication is provided by limit switches. Positive indication of these valves is required per RG 1.97 (PAM). Therefore environmental qualification is provided for these limit switches. This instrumentation is powered from safety grade emergency power. Reactor Building Purge is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 2 variable at Oconee.

For the Penetration Room Ventilation System, positive indication of system operation is provided by the Penetration Room Pressure Instrumentation. This instrumentation is pneumatic and is supplied by normal Station Air System. The Unit 1 and 2 instruments are located in mild environments; however, the Unit 3 instrumentation is located in a harsh environment. Penetration Room Ventilation System is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 2 variable at Oconee.

For a description of the instrumentation required to determine proper operation of the Reactor Building Cooling System see UFSAR Section 7.5.2.41.

7.5.2.51 Emergency Power System Status

All safety-grade emergency or battery backed control busses have undervoltage alarms in the Control Room with local diagnostic capabilities to enable an expedient assessment of abnormal situations. In addition, the 125 VDC distribution centers have analog indicators of voltage level in the Control Room. All of the Control Room alarms are on highly reliable battery backed busses. All of the sensing relays and alarm electronics are located in a mild environment. See FSAR Chapter 8. Emergency Power System Status is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 2 variable at Oconee.

7.5.2.52 Unit Vent Radioactive Discharge Monitors

Oconee has a normal range, high range and high-high range channel of unit vent radioactivity instrumentation. These channels are powered from a highly reliable non load shed power bus. The indicated range is 1 to 10^8 R/hr gross gamma for the high-high range monitor which envelopes the upper end of the recommended range. The indicated range is 10 to $1E^7$ cpm for the high range channel and 10 to $1E^7$ cpm for the normal range channel. The combined ranges of these monitors meet the requirements of Regulatory Guide 1.97, Rev. 2 Type C Category 2 variable. This instrumentation is installed in a mild environment.

7.5.2.53 Unit Vent Flow

The installed instrumentation indicates flow in the unit vent stack over the range of 0 to 110% of design flow. The design flow for the Unit 1 stack is 97,262 SCFM (98,880 for Unit 2; 114,506 for Unit 3). The indicator and recorder, Units 1, 2 and 3 respectively, actual dual ranges are the following:

Unit 1&2	-	0 to 60 x 10^3 SCFM
		0 to 120 x 10^3 SCFM
Unit 3	-	0 to 65 x 10^3 SCFM
		0 to 130 x 10^3 SCFM

The primary instrument loop which contains the transmitter, the plant computer and the retransmitter is powered by a highly reliable battery backed bus. The secondary instrument loop contains the retransmitter, indicator and recorder. The retransmitter and indicator are powered by a highly reliable auxiliary bus. The instrumentation is located in a mild environment and envelopes the Regulatory Guide 1.97, Rev. 2 Type E Category 2 variable range criteria of 0 to 110% of design flow.

7.5.2.54 Main Steam Line Radiation Monitors

Area radiation monitors are located adjacent to the main steam lines to detect radioactivity emitted from main steam. The monitors for all 3 units are located upstream of the main steam relief valves. Correlation curves allow conversion of the monitor readings in mR/hr to μCi/cc. The indicated range for the monitors is 10^{-2} to 10^7 mR/hr. The monitors are powered from a highly reliable non load shed power bus capable of receiving power from the on-site emergency power sources. This instrumentation is rated to withstand the environmental conditions that would exist during accidents in which it is intended to operate. A steam line break in the vicinity of this instrumentation may cause the environment to exceed the rated temperature, however, the instrument is not required to remain operational for this event. Main Steam Line Radiation Monitors are classified as a Regulatory Guide 1.97, Rev. 2 Type E Category 2 variable at Oconee.

7.5.2.55 Wind Direction

Oconee has two channels of wind direction instrumentation. The indicated range is 0 to 540°. Wind direction is a Regulatory Guide 1.97 Category 3 Type E Variable. The range and accuracy of the installed instrumentation is adequate for its intended purpose.

7.5.2.56 Wind Speed

Oconee has two channels of wind speed instrumentation. The indicated range is 0 - 60 mph. Wind Speed is a Regulatory Guide 1.97 Category 3 Type E Variable. The range and accuracy of the installed instrumentation is adequate for its intended purpose.

7.5.2.57 Atmospheric Stability

The indicated range for atmospheric stability is -4° to 8°C for 44.7 meter interval. Loop accuracy is at least +0.15°C. This range is adequate for Oconee site meteorological conditions. Atmospheric Stability is classified as a Regulatory Guide 1.97, Rev. 2 Type E Category 3 variable at Oconee.

7.5.2.58 Low Pressure Service Water Flow to Low Pressure Injection Coolers

Two QA Condition 1 instrumentation channels are provided (one per train) for post accident monitoring of Low Pressure Service Water (LPSW) flow to the Low Pressure Injection (LPI) coolers in response to Regulatory Guide 1.97. Each instrument channel is seismically qualified and powered from a safety grade power source. Each instrument channel signal inputs to a qualified indicator and to the plant computer via a qualified signal isolator. These channels monitor LPSW flow to the LPI Coolers over a range of 0-8000 gpm which envelopes the 0-110% of design flow criteria for Regulatory Guide 1.97.

Two non-safety instrument channels are provided, one per train, for indication of LPSW flow to LPI Cooler and control of valves LPSW-251 and 252. Each instrument signal inputs to a controller which monitors flow and valve control. These channels monitor LPSW flow to the LPI Cooler over a range of 0-6000 gpm. These instrument channels are not required for Regulatory Guide 1.97 and are used for normal operation.

LPSW flow to LPI Coolers is a Type A Category 1 variable at Oconee because the operator relies on this information following a design basis event (LOCA) to throttle LPSW flow to LPI Coolers to maintain proper flow balance in the LPSW System.

7.5.2.59 Essential Siphon Vacuum Tank Pressure (Vacuum)

The instrumentation for this variable provides continuous display of Essential Siphon Vacuum (ESV) Tank Pressure. One instrument channel is provided for each train of ESV tank. The ESV system on a per unit basis consists of three pumps and two tanks. Each train consists of one tank and one pump. The third ESV pump serves as an in-place spare pump which can be aligned to either train. The instrumentation provides control room indication of tank vacuum from 30 In Hg to 0 In Hg. The instrumentation is seismically qualified in accordance with the Oconee licensing basis as specified in the Oconee UFSAR and Duke Power Seismic Design Criteria (OCSD-0193.01-00-0001). The instrumentation is located in the ESV building which is considered a Mild Environment. The installed equipment meets the requirements of RG 1.97, Rev 2 for Type D, Category 2 nuclear safety related (QA-1) instrumentation as described in Section 7.5.

This instrumentation monitors the Essential Siphon Vacuum Tanks for operation to provide information (two indicators, two computer alarms, and two annunciator alarms, all one per tank) to indicate the operation of the system in the event it is needed to mitigate the consequences of the design basis accident (LOCA/LOOP).

7.5.2.60 Essential Siphon Vacuum Tank Water Level

The instrumentation for this variable provides continuous local display of Essential Siphon Vacuum Tank Water level. One instrument is provided on each train of ESV tank. The level gage is physically located on the tank. The ESV system for each unit consists of three full capacity pumps and two tanks. Each train consists of one tank and one pump. The instrumentation range (0-24 inches) provides local indication of any accumulated water in the ESV Tanks. Manual action can be taken to drain the tanks as required. The instrumentation is seismically qualified in accordance with the Oconee licensing basis as specified in the Oconee UFSAR and Duke Power Seismic Design Criteria (OCSD-0193.01-00-0001). The instrumentation is located in the ESV building which is considered a Mild Environment. The installed equipment is adequate for its intended monitoring function and meets the requirements of RG 1.97, Rev.

2 for Type D, Category 2 nuclear safety related (QA-1) variables instrumentation as described in Section 7.5.

This variable monitors the Essential Siphon Vacuum Tanks for operation to provide local indication regarding the operation of the system in the event it is needed for continued post accident mitigation of the consequences of the design basis accident (LOCA/LOOP).

7.5.2.61 Siphon Seal Water Flow to Essential Siphon Vacuum Pumps

The instrumentation for this variable provides continuous local display of Siphon Seal Water (SSW) flow to the Essential Siphon Vacuum pumps as well as a signal to the plant computer for display in the control room. One instrument is provided on each SSW supply to an ESV pump. There are three ESV pumps per unit. A total of nine instruments are provided for the nine ESV pumps. A bargraph indicator is located on the local panel in the ESV Building for each Unit's three pumps. The ESV system consists of three pumps and two tanks. Each ESV train consists of one tank and one pump. The third pump is an installed spare. The instrumentation is seismically qualified in accordance with the Oconee licensing basis as specified in the Oconee UFSAR and Duke Power Seismic Design Criteria (OCSD-0193.01-00-0001). The instrumentation is located in a Mild environment. The installed equipment meets the requirements of RG 1.97, Rev. 2, Type D, Category 2 nuclear safety related (QA-1) instrumentation as described in Section 7.5.

The range (0 to 15 Gallons per Minute (GPM)) and the qualification requirements of the SSW flow to ESV pumps instrumentation is in compliance with the recommendations of RG 1.97, Rev. 2 for Type D variables. This variable monitors the Siphon Seal Water flow to the Essential Siphon Vacuum Pumps to provide information relative to the operation of the ESV system in the event it is needed for continued post accident mitigation of the consequences of the design basis accident (LOCA/LOOP).

7.5.2.62 Low Pressure Service Water Reactor Building Waterhammer Prevention System Valve Position

The Low Pressure Service Water (LPSW) Reactor Building (RB) Waterhammer Prevention System (WPS) is designed to maintain the LPSW piping inside containment water solid during events which cause a loss of LPSW such as LOOP, LOCA/LOOP, or MSLB/LOOP. The system's major components consist of check valves in the suply headers (LPSW-1111, 1116), pneumatic discharge isolation valves (LPSW-1121, 1122, 1123, 1124), pneumatic vent valves (a.k.a. controllable vacuum breakers) (LPSW-1150, 1151), and associated acutation circuitry.

The installed instrumentation provides valve position indication for the pneumatic discharge isolation valves (LPSW-1121, 1122, 1123, 1124). Position indication is provided by QA-1 indicating lamps at the control switches on the control board for the four pneumatic discharge isolation valves. These LPSW valve position indications associated with LPSW RB Waterhammer Prevention System are considered to be Regulatory Guide 1.97, Rev. 2, Type D Category 3 instrumentation.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.5.

THIS PAGE LEFT BLANK INTENTIONALLY.

7.6 Control Systems Not Required for Safety

7.6.1 Regulation Systems

Reactor output is regulated by the use of movable control rod assemblies and soluble boron dissolved in the coolant. Control of relatively fast reactivity effects, including Doppler, xenon, and moderator temperature effects, is accomplished by the control rods. The control response speed is designed to overcome these reactivity effects. Relatively slow reactivity effects, such as fuel burnup, fission product buildup, samarium buildup, and hot-to-cold moderator reactivity deficit, are controlled by soluble boron.

Control rods are normally used for control of xenon transients associated with normal reactor power changes. Chemical shim shall be used in conjunction with control rods to compensate for equilibrium xenon conditions. Reactivity control may be exchanged between rods and soluble boron consistent with limitations on power peaking.

Reactor regulation is a composite function of the Integrated Control System and Control Rod Drive System. Design data for these subsystems are given in the following sections.

7.6.1.1 Control Rod Drive System

The Control Rod Drive System (CRD) includes drive controls, power supplies, position indicators, operating panels and indicators, safety devices, and enclosures.

7.6.1.1.1 Design Basis

The Control Rod Drive System design bases are categorized into safety considerations, reactivity rate limits, startup considerations, and operational considerations.

7.6.1.1.2 Safety Considerations

The control rod assemblies (CRA) are inserted into the core upon receipt of protective system trip signals. Trip command has priority over all other commands.

No single failure shall inhibit the protective action of the Control Rod Drive System.

7.6.1.1.3 Reactivity Rate Limits

The speed of the mechanism and group rod worth provide the reactivity change rates required. For design purposes, the maximum rate of change of reactivity that can be inserted by any group of rods has been set at a conservative value used within the Chapter 15 Section 15.3 and Section 15.2. The drive controls, i.e., the drive mechanism and rods combination, have an inherent speed-limiting feature.

7.6.1.1.4 Startup Considerations

The Control Rod Drive System design bases for startup are as follows:

Reactor regulation during startup is a manual operation.

Control rod "out" motion is inhibited when a high startup rate in the wide range is detected.

7.6.1.1.5 Operational Considerations

For operation of the reactor, functional criteria related to the control rod drive system are:

CRA Positioning

The Control Rod Drive System provides for controlled withdrawal, controlled insertion, and holding of the control rod assemblies (CRA) to establish and maintain the power level required for a given reactor coolant boron concentration.

Position Indication

Continuous rod position indication, as well as full-in and full-out position indication, are provided for each control rod drive.

System Monitoring

The Control Rod Drive System design includes provisions for routinely monitoring conditions that are important to safety and reliability.

7.6.1.1.6 System Design

The Control Rod Drive System provides for withdrawal and insertion of the control rod assemblies to maintain the desired reactor output. This is achieved either through automatic control by the Integrated Control System discussed in Section 7.6.1.2 or through manual control by the operator. As noted previously, this control compensates for short term reactivity changes. It is achieved through the positioning in the core of sixty-one control rod assemblies and eight axial power-shaping rod assemblies. The sixty-one rods are grouped for control and safety purposes into seven groups. Four groups function as safety rods, and three groups serve as regulating rods. An eighth group serves to regulate axial power peaking due to xenon poisoning. Seven of the eight groups may be assigned from four to twelve control rod assemblies. Eight rod assemblies are used in Group 8.

Control rods are arranged into symmetric (by core quadrant) groups by utilizing the Engineering Work Station (EWS) to edit a data base contained in the PLC software which defines the desired rod group patterns. Typically, thirty-six rods, including the axial power shaping rods, are assigned to the regulating groups, and thirty-three rods are assigned to the safety rod groups. A typical rod grouping arrangement is shown below:

Safety Rods	Regulating Rods	Axial Power Shaping Rods
Group 1 - 8	Group 5 - 12	Group 8 - 8
Group 2 - 8	Group 6 - 8	
Group 3 - 8	Group 7 - 8	
Group 4 - 9		

During startup, the safety rod groups are withdrawn first, enabling withdrawal of the regulating control groups. The sequence allows operation of only one regulating rod group at a time except where reactivity insertion rates are low (first and last 25 percent of stroke), at which time two adjacent groups are operated simultaneously in overlapped fashion. These insertion rates are shown in Figure 7-11.

As fuel is used, dilution of soluble boron in the reactor coolant is necessary. When Group 6 is more than 95 percent withdrawn, interlocks permit dilution. The reactor controls insert Group 6 to compensate for the reduction in boron concentration by dilution. The dilution is automatically terminated by a pre-set volume measuring device. Interlocks are also provided on Group 6 rod position to terminate dilution at a pre-set insertion limit.

7.6.1.1.7 System Equipment

The Control Rod Drive System consists of three basic components: (1) control rod drive motor power supplies; (2) system logic; and (3) trip breakers. The power supplies consist of 138 Single Rod Power

Supply (SRPS) modules, with two identical wired as a redundant pair and connected to each CRDM. Each SRPS uses a six-phase half-wave (SCR) rectifier design. See Figure 7-4, Figure 7-12 and Figure 7-13.

SRPS, rectification and switching of power is accomplished through the use of Silicon Controlled Rectifiers (SCRs). This switching sequentially energizes first two, then three, then two of the six CRA motor stator windings in stepping motor fashion, to produce a rotating magnetic field for the control rod assembly motor to position the CRA. Switching is achieved by gating the six SCRs on for the period each winding must be energized. As each of the six windings utilize SCRs to supply power, six gating signals are required.

Deleted Paragraph(s) per 2009 Update

Gating signals for the SRPS are generated by a Programmable Logic Controller (PLC) using software containing logic to accept automatic commands from the ICS, or direct manual commands from the Operator Control Panel (OCP). These commands are converted to sequential digital outputs which cause the mechanism motors to step at the proper speed and direction to provide a 3-2 hold control, which ensures two-coils are energized when there are no commands. If one coil becomes de-energized the control rod position will be maintained, but cannot be exercised. A second PLC is devoted exclusively to processing absolute and relative control rod position indication signals.

Deleted Paragraph(s) per 2009 Update

The PLC is also known as a Triple Modular Redundant (TMR) Controller using a triplicated processor running in parallel, with redundant and automatic selection of the "good" signal in the event of failure or malfunction of the controlling "slice". An auctioneering network determines if any anomalies exist and selects the most credible (via a two-out-of-three voting network) of the three available signals. Each processor executes the application program simultaneously and independently. Redundant power supplies are used for all CRD mechanisms, and each is capable of carrying the full load and each is fed from separate power sources with a common SCR gating signal control source.

Deleted Paragraph(s) per 2009 Update

Major components of the system are the RPS interface Trip Breakers, Position Indication (PI) Panel, OCP, TMR Controllers, Engineering Work Station (EWS) – for software control inputs, and the SRPS.

Switches are provided at the operators control panel for selection of desired rod control mode. Control modes are: (1) Automatic mode--where rod motion is commanded by the Integrated Control System; and (2) Manual mode--where rod motion is commanded by the operator. Manual control permits operation of a single rod or a group of rods. Alarm lamps on the CRD panel alert the operator to the systems status at all times. The Group 8 control rods can only be controlled manually even when the remainder of the system is in automatic control.

The sequence section of the logic system utilizes rod position signals to generate control interlocks which regulate rod group withdrawal and insertion. Sequence logic applies in both automatic and manual modes of reactor control, and controls the regulating groups only. When operating in the "sequence mode" mode, the PLC controls sequential withdrawal and insertion of numerically adjacent regulating groups. Two adjacent groups are enabled coincidentally within 25% overlap regions, in order to minimize effects of lower rod worth at their upper and lower extremes in travel.

The automatic sequence logic can control only rod Groups 5, 6, and 7. The safety rod groups, Groups 1 through 4, are controlled manually, one group at a time. There is no way in which the automatic sequence logic can affect the operations required to move the safety rods.

In addition to the sequence logic, logic is also provided which prohibits out of sequence conditions. The selection of manual control mode and sequence bypass mode functions permit intentional out-of-sequence

conditions. This condition is indicated to the operator. If automatic control is selected, "sequence" operation cannot be bypassed.

"Sequence bypass" operation permits selection of any rod group or any single rod for control. It will not permit selection of more than one rod group at any given time. Motion of more than one group at any given time is also not possible when this operation is selected.

Inputs to the system logic from the Nuclear Instrumentation and the Integrated Control System provide interlock control over rod motion. These interlocks cause rod motion command lines and control mode selection to be inhibited.

Under certain conditions, the nuclear instrumentation generates an "out inhibit" signal. When this signal is received by the Control Rod Drive System, all out command circuits are disabled, thus preventing withdrawal of all rods in either automatic or manual control.

Automatic operation of rods can only be commanded by the ICS when the Control Rod Drive System is in the automatic mode. These commands can only affect rod Groups 5, 6, and 7.

In the Control Rod Drive System, two methods of position indication are provided: an absolute position indicator and a relative position indicator. Either position signal is available to the control board indicator through a selector switch. The absolute position transducer consists of a series of magnetically operated reed switches mounted in a tube parallel to the motor tube extension. Each switch is hermetically sealed. Switch contacts close when a permanent magnet mounted on the upper end of the lead screw extension comes in close proximity.

As the lead screw (and the control rod assembly) moves, the switches operate sequentially, producing an analog voltage proportional to position. Other reed switches included in the same tube with the position indicator matrix provide full-in and full-out limit indications.

The relative position indication is calculated by the TMR processor. Control Rod Drive System trip breakers are provided to interrupt power to the control rod drive mechanisms. When power is removed, the roller nuts disengage from the lead screw allowing a gravity trip of the CRA.

The Group 8 drive mechanisms are modified to prevent rod drop into the core when power is removed from the stators. In this type of mechanism, the roller nuts are mechanically restrained to remain engaged with the lead screw at all times. Thus, the mechanical "trip" action has been removed from these APSR's, and they remain at the position they occupied immediately before trip was initiated.

Deleted Paragraph(s) per 2009 Update

The CRD Trip Breakers are of the three-pole, stored energy type and are equipped with instantaneous undervoltage and shunt trip coils. Each of the four breakers is housed in separate metal-clad enclosures with two vertical breakers housed in the middle two compartments of each of two adjacent and integral seismically-qualified Class 1E breaker cabinets. Two other compartments in each cabinet are utilized for ancillary equipment (Reactor Trip Confirm Signals and Source Interruption Device Signals via the AC Power Interface equipment in top and 15 KVA Control Transformer in bottom). All breakers have motor-driven reset features to provide remote reset capability.

7.6.1.1.8 System Evaluation

Safety Considerations

A reactor trip occurs whenever power has been removed from the rod drive motors. The design provides stored energy breakers which do not require power to interrupt the electrical feeds to control rod drive power supplies.

Deleted Paragraph(s) per 2009 Update

The system ensures that power is removed from all of the CRDM's by utilyzing a 1 out of 2 taken twice power design. This design uses 2 qualified breakers located in the "A" power feed into the system and 2 qualified breakers located in the "B" power feed into the system. Therefore a single failure in the distribution system for the control rods does not prevent a plant shutdown.

The minimum voltage required to hold a drive in a withdrawn position is 42 volt DC per coil (2 coil "hold" mode). The probability of an external DC source being applied to the control rod drive mechanisms downstream from the reactor trip points such that the CRA are held in their withdrawn positions after a trip is not considered credible for the following reasons:

1. The trip devices in the Control Rod Drive System remove all DC power from the drives.
2. Control rod drive power cables are terminated at only three points between the Control Rod Drive System cabinets and the drive mechanisms.

   Two of these terminations are made outside and inside the Reactor Building electrical penetrations inside junction boxes containing only control rod drive power cables. The third termination is made in bulkhead connectors (one per drive) in the area of the reactor. The only other cables terminated in this area are the control rod drive instrumentation cables. The instrumentation cables are terminated in bulkhead connectors of a different size and configuration, therefore mismating of connectors could not be accomplished.
3. No cable splices are permitted between termination points described.
4. DC systems from the batteries at Oconee are not grounded and are equipped with ground detecting circuitry.

In summary, series redundant trip devices having adequate rating, testability and a 1 out of 2 taken twice power design arrangement insure safety of reactor trip circuits.

Reactivity Rate Limits

The desired rate of change of CRA reactivity insertion and uniform reactivity distribution over the core are provided for by the control rod drive and power supply design, and the selection of rods in a group. The CRA motor, lead screw, and power supply designs are fixed to provide a uniform rate of speed of 30 in./min. The speed is determined by the CRD PLC, which digitally controls speed. The reactivity change is then controlled by the rod group size. To insure flexibility in this area, rod group assignments are entered off-line at the EWS into password-protected software. This determines desired rod group worth distribution to coordinate with varying core reload design. Any rod may be assigned to any group, with the exception of group 8, so long as the same group pattern exists in each core quadrant. Rod groups may vary from a minimum of four to a maximum of 12, which translates into five possible rod groupings of 4, 5, 8, 9, and 12 – where the odd-numbered group would contain the center rod at core grid H-8. APSR rod assignments are fixed at two near the center of each quadrant.

Deleted Paragraph(s) per 2009 Update

Uniform and symmetrical reactivity addition rate is provided by synchronous withdrawal of all rods assigned to that group. All rods in any one group will have the same CRD motor stator windings simultaneously energized. Such synchronous withdrawal is achieved by phase trigger pulses from the Pulse Generator/Monitor (PG/M) modules in response to rod movement command signals generated by the TMR Controller. The TMR architecture employs a highly synchronized triplicated processor set running in parallel. Each processor "slice" executes the application program simultaneously and independently, verifying data, control, clock, and synchronization signals. These signals are partitioned and down-loaded in such a manner as to optimize execution times of the algorithms controlling synchronous motion of the entire group.

Each control rod is provided with rod position indicator logic to sense asymmetric rod patterns by comparing the individual rod position with its group average position. When the rod moves out-of-step from its group by a preset amount, this condition is alarmed to the operator, the plant computer, and the ICS. Depending on the power setting and the control mode, action is initiated by the ICS to insert rods and reduce power.

Startup Considerations

The rod drive controls receive interlock signals from the ICS and nuclear instrumentation (NI). These inputs are used to inhibit automatic mode selection when a large error exists in the ICS reactor control subsystem and to inhibit out motion for high startup rates, respectively.

In addition to the startup considerations, dilution controls, to permit removal of reactor shutdown concentrations of boron in the reactor coolant, are provided. This control bypasses the normal reactor coolant dilution controls, described in Section 7.6.1.1.6, provided all safety rods are withdrawn from the core and the operator initiates a continuous feed and bleed cycle. An additional interlock on rod Group 5 inhibits the use of this circuit when rod Group 5 is more than 80 percent withdrawn.

Operational Considerations

The control rod assembly positioning system provides the ability to move any rod to any position required consistent with reactor safety. As noted in Section 7.6.1.1.8, a uniform speed is provided by the drive system. A fixed rod position when motion is not required is obtained by the power supply ability to energize two adjacent windings of the CRA motor stator. This static energizing of the windings maintain a latched stator and fixed rod position.

Position Indication

As previously described, two separate position indication signals are provided. The absolute position sensing system produces signals proportional to CRD position from the reed switch matrix located on each CRD mechanism. The relative position indication system produces a signal proportional to the number of electrical pulses sent to the CRD motor stator windings, as determined through processing of these signals by a separate programmable logic (TMR) controller whose sole function is the processing of absolute and relative position indication signals.

Position indicating readout devices mounted on the operator's console consist of 69 single rod position meters. The operation of a selector switch permits either relative or absolute position information to be displayed on the single rod meters.

Indicator lights are provided on the position indication panel to indicate when each rod is (1) fully inserted, (2) fully withdrawn, (3) under control, and (4) whether a fault is present. Indicators on the operator control panel show full insertion, full withdrawal, under control, and fault indication for each of the eight control rod groups.

Failures which could result in unplanned control rod withdrawal are continuously monitored by fault detection logic. When failures are detected, indicator lights and alarms alert the operator. Fault indicator lights remain on until the fault condition is cleared by the operator. A list of indicated faults is shown below:

1. Asymmetric rod patterns (indicator and alarm).
2. Sequence faults (indicator and alarm).
3. Trip status (indicator and alarm).
4. Safety rods not withdrawn (indicator only).
5. Rod position sensor faults.

Faults serious enough to warrant immediate action produce automatic correction commands from the fault detection logic, and manual bypass is not possible. Status indicators on the operator's console provide monitoring of control modes.

A description of each fault detector follows:

Asymmetric Rod Monitor

Design Basis - To detect and alarm if any rod deviates from its group reference position by more than a maximum of nine inches true position.

Operation - There are 69 asymmetric rod pattern monitors, one assigned to each control rod. This logic continuously compares the individual rod absolute position signal with the absolute group reference (average) signal. The absolute value of the difference between the two signals is computed, and if this difference is less than the maximum value allowed by the software configuration, no output results. If, however, the difference is greater than the setpoint, the system alarms the asymmetric condition. Two alarm channels are provided which are identical except for the setpoints. One setpoint allows a maximum 7-inch true position separation before initiating an alarm. The other setpoint allows a maximum 9-inch true position separating before initiating the action described below.

Corrective Action - Action taken upon detection of an asymmetric rod fault depends upon the control mode and the power level in effect at the time the fault is detected. Corrective action is the same for any asymmetric condition including "stuck-in," "stuck-out," or dropped control rods.

Detection of a 7-inch position separation is defined as an "asymmetric rods alarm." Actuation of this alarm causes the fault indicator lamp for that rod to be energized and an alarm signal to be sent to the plant computer and annunciator.

If the condition is not corrected and the separation increases to a 9-inch position separation, the following actions occur:

"Asymmetric fault" lamp on the operator's console is energized. If operation is in the manual control mode, operator action is required by administrative control.

If operation is in the automatic mode, a "runback fault" signal is sent to the Integrated Control System. The ICS will impose a maximum reactor power demand of 55 percent of rated power if power is initially less than 55 percent.

When an asymmetric fault occurs, the Control Rod Drive Control System generates an "Out Inhibit" which prevents automatic rod motion that would increase reactor power. Below 60 percent reactor power the ICS generates a bypass signal for the out inhibit, which allows normal automatic rod control.

Reactor power demand remains limited to 55 percent maximum in automatic control until the fault is corrected.

Sequence Monitor

Design Basis - To detect any motion of the regulating rod groups outside of the predetermined automatic sequence patterns, and to prevent further automatic motion when such conditions occur.

Operation - The sequence logic continuously compares the group average (reference) signals for each regulating rod group with the allowable sequence patterns. In addition, the rod group "enable" logic determines if a group is enabled for motion out-of-turn. The safety rod groups' out limit signals serve as a permissive to automatic sequencing: the sequence monitor prevents automatic control until the safety rods are fully withdrawn.

Corrective Action - When an out-of-sequence condition is detected and operation is in the automatic control mode, the automatic mode disengages and an alarm lamp alerts the operator to the malfunction.

Control reverts to manual and remains in manual until the fault is corrected and the system is reset by the operator.

Trip Status

Design Basis - To sense the status of trip devices and trip channels.

Operation - The circuit contains elements, which sense the state of each trip device as well as the state of each of the four trip channels. If a trip device or a trip channel is in a trip state, its associated annunciator will alarm. The annunciators are used by operations to detect faults that may affect operation of the trip circuits, such as one trip breaker in the tripped position during normal operation.

Corrective Action - Alarms are provided.

Safety Rods Not Withdrawn

Design Basis - To prevent, on plant startup, withdrawal of the regulating rods until the safety rods are fully withdrawn.

Operation - Continuously monitors the group "out" limit for the four safety rod groups. When the four groups are all fully withdrawn, automatic control is permitted.

Corrective Action - Alarms are provided.

Rod Position Sensor Faults

All rod position sensor faults lead to false asymmetric, stuck, or dropped rod symptoms which are acted upon by the Asymmetric Rod Monitor previously described.

7.6.1.2 Integrated Control System

7.6.1.2.1 Design Basis

The Integrated Control System (ICS) provides the proper coordination of the reactor, feedwater control, and turbine under all operating conditions. Proper coordination consists of producing the best load response to the Core Thermal Power demand while recognizing the capabilities and limitations of the reactor, steam-generator feedwater system, and turbine. When any single portion of the plant is at an operating limit or control selection is on manual, the Integrated Control System design uses the limited or manual section as a load reference.

The Integrated Control System maintains constant average reactor coolant temperature between 15 and 100 percent rated power, and constant steam pressure at all loads. Optimum unit performance is maintained by limiting steam pressure variations; by limiting the unbalance between the steam generator, the turbine, and the reactor; and by limiting the Core Thermal Power demand upon loss of capability of the steam generator feed system, the reactor, or the turbine generator. The control system provides limiting actions to assure proper relationships between the generated load, turbine valves, feedwater flow, and reactor power.

The response of the Reactor Coolant System to increasing and decreasing power transients is limited by the Integrated Control System as indicated in Table 7-6. The Turbine Bypass System permits a load drop of 40 percent or a turbine trip from 40 percent load without safety valve operation.

7.6.1.2.2 Description

The Integrated Control System includes four independent subsystems as shown in Figure 7-14. The four subsystems are: the Core Thermal Power Demand; the Integrated Master; the Feedwater Control; and the Reactor Control. The system philosophy is that control of the plant is achieved through feed-forward control from the Core Thermal Power Demand. The Core Thermal Power Demand produces demands for

parallel control of the turbine, reactor, and Steam Generator Feedwater System through respective subsystems.

The Feedwater Control is capable of automatic or manual feedwater control from a startup to full power. The Integrated Master Control is capable of automatic or manual turbine valve control from minimum turbine load to full output, and of manual control below minimum turbine load. The Reactor Control is designed for automatic or manual operation above 2 percent power, and for manual operation below 2 percent power.

The basic function of the Integrated Control System is matching Turbine and Reactor Power to Core Thermal Power demand. The Integrated Control System does this by coordinating the steam flow to the turbine with the rate of steam generation. To accomplish this efficiently, the following basic reactor/steam-generator requirements are satisfied:

The ratios of feedwater flow and BTU input to the steam generator are balanced as required to obtain desired steam conditions.

BTU input and feedwater flow are controlled:

1. To compensate for changes in fluid and energy inventory requirements at each load.
2. To compensate for temporary deviations in feedwater temperature resulting from load change, feedwater heating system upsets or final steam pressure changes.

7.6.1.2.2.1 Unit Load Demand

The Core Thermal Power Demand Subsystem provides the operator with a means of establishing the desired operating power load from the plant. The demand signal produced by this subsystem is called the Core Thermal Power Demand (CTPD), and is the principle independent demand signal in the ICS. Other subsystems receive the CTPD and establish final control element positions in order to meet this demand.

The CTPD subsystem obtains a load demand signal, manually set by the operator, from the Load Control Panel. The Load Control Panel is the primary operator interface to the ICS for Integrated Mode operation. Pushbutton switches, digital meters, a digital thumb switch and status lamps are provided for manipulation of Core Thermal Power Demand Set, the Demand Rate Set, turbine Load and Unload, Maximum Runback function and status for various Load Limit and Tracking conditions. The CTPD substytem initiates load limiting and runback functions to restrict operation within prescribed limits. Figure 7-15 illustrates the functions incorporated in the subsystem.

The CTPD is restrained by a maximum load limiter, a minimum load limiter, a rate limiter and a runback limiter.

Rate limiting is designed as a function of load, so transients are limited as shown in Table 7-6.

The limiter acts to runback and/or limit the CTPD under any of the following conditions:

1. Loss of one or more reactor coolant pumps.
2. CTPD vs reactor coolant flow, variable limit.
3. Low suction pressure (FDW or Condensate)
4. Loss of one feedwater pump.
5. Asymmetric rod patterns exists in reactor.
6. The generator separates from the bus.
7. A reactor trip occurs.

The output of the limiters is a CTPD signal which is applied to the turbine control, feedwater control, and reactor control in parallel.

The controlling subsystems of the ICS (turbine control, feedwater control, and reactor control) normally operate in the automatic mode in response to a demand signal from the CTPD. The subsystems control function is kept within pre-established bounds under other than normal automatic operation by a "load tracking" feature built into the ICS. The ICS will switch to the load tracking mode if either of the following conditions exists:

One or more of the subsystems are in manual.

Errors greater than preset limits develop between the demand and the variable.

In this mode, the CTPD is made to follow the manual or limited control subsystem. Load tracking continues until the limiting condition is brought back to within the pre-established deadband or the subsystem is returned to automatic operation.

7.6.1.2.2.2 The Integrated Master

The Integrated Master has been designed to receive the Core Thermal Power Demand (CTPD) from the Core Thermal Power Demand Subsystem and utilize this signal as a demand for the feedwater, turbine and reactor control. A functional diagram of the Integrated Master Control is shown in Figure 7-16. The Integrated Master subsystem produces demand signals for the reactor control, feedwater control and turbine control (steam valves), to meet the CTPD, while providing coordination between the primary system, feedwater and turbine to maintain heat balance. The subsystem produces demands for total feedwater flow, reactor power and steam valve position to ensure that heat balance indicating parameters are kept within operating limits. The demands are modified during plant limited operation in accordance with the Control Priority. The ICS Control Priority for the four main heat balance variables is as follows:

Tave

Steam Header Pressure

Reactor Power

Cold Leg Temperature Difference (delta - Tc)

Three major control Hand/Automatic (H/A) stations are provided to give the operator a means of manually setting the integrated master demand outputs. The reactor master control station allows the operator to manually establish a demand for reactor NI-Flux and to set the controlling reactor coolant system Tave set point. The steam generator master H/A station allows the operator to manually establish the total feedwater flow demand. The turbine control H/A station allows the operator to establish the EHC load reference signal and to set the controlling turbine header pressure set point.

Turbine Control

Control of the turbine is accomplished by a pressure controller. The turbine header pressure is compared to a set point (set by the operator from the turbine H/A station) and this error drives an analog signal. The resulting analog signal is sent to the load reference logic where it is integrated into a steam valve position demand. The ICS will continue to generate a demand for turbine valve movement until the pressure error is reduced to zero.

The turbine control H/A station gives the operator the option of letting the turbine control pressure or, by transferring the turbine control station to manual, allowing the operator to establish the amount of electrical load generation.

The "LOAD" and "UNLOAD" push buttons on the "Load Control Panel" provide the operator interface with the turbine load and unload system. The turbine load and unload system enables the operator to

smoothly introduce and remove the main turbine into/from the plant control process. The system is necessary because the reactor may be operated in automatic at a power level significantly below the normal minimum load of the turbine.

Turbine Bypass

The Turbine Bypass System operates from the turbine header pressure error or individual steam generator pressures as an overpressure relief for the turbine header. The turbine bypass valves receive control inputs from their respective OTSG outlet pressure , unless the main turbine is in automatic. If the main turbine is in automatic, the bypass valves use the turbine header pressure error signal, which is the same signal controlling the main turbine controller.

The turbine bypass valves serve four functions:

1. Provide pressure control at low loads before the turbine can be placed in automatic.
2. Provide a high pressure relief if the turbine header pressure exceeds its set point (normally 885 psig) by 50 psig.
3. Provide an independent high pressure relief that operates proportionally to steam generator pressure above 1035 psig.
4. Provide pressure control after a reactor trip at 125 psi above normal set point to prevent excessive cooling of the reactor coolant fluid.

Once the main turbine is placed in automatic control, and loaded, the turbine bypass valves assume over pressure control at set point plus 50 psi.

7.6.1.2.2.3 Feedwater Control

The Feedwater Control Subsystem has been designed to receive the total feedwater demand signal from the Integrated Master Subsystem and utilize this signal to develop demand signals for control of the feedwater pumps and the feedwater valves for each steam generator. A functional diagram of the Feedwater Control Subsystem is shown in Figure 7-17.

The total feedwater demand signal developed in the Integrated Master Subsystem is corrected for feedwater temperature in the Feedwater Control Subsystem. A proportional correction is also applied to the feedwater demand when RC Pressure is greater than 2250 psig. The feedwater demand signal is limited when Neutron Error exceeds +/- 5%.

The corrected total feedwater demand signal is modified to provide a feedwater demand signal for each steam generator. Under normal conditions, each steam generator will produce one-half of the total load. The steam generator load ratio control (delta Tc control) is provided to balance reactor inlet coolant temperatures during operation with more reactor coolant pumps in one loop than in the other. The steam generator load ratio control (delta Tc control) signal is modified by an anticipatory delta Tc error circuit which is based upon a ratio of the measured RC flow.

A Feedwater Master Hand/Automatic control station for each steam generator enables manual control by the operator or operation in automatic. In the automatic mode of operation, feedwater flow is controlled by either level control or flow control. Each steam generator may independently operate on level or flow control.

Level control ("Low Level Limits", LLL) exists when loop Tave is less than the Tave set point and the steam generator level is equal to or less than the steam generator low level set point. During this mode, steam generator startup level provides a demand signal to the feedwater valves for control of feedwater flow to the steam generator.

Flow control exists when Tave is equal to or greater than the Tave set point and steam generator level is greater than the low level limit.

During the flow control mode, the loop feedwater master demand is compared to steam generator feedwater flow and to a maximum steam generator operate level set point. The resultant feedwater error signal is utilized to develop the position demand signal for the feedwater valves. The feedwater error signal drives the feedwater valves to make feedwater flow match loop feedwater flow demand, or to limit the maximum steam generator level.

Feedwater flow to each steam generator is controlled by two valves, a startup valve and a main valve. The startup feedwater control valve provides feedwater flow control from startup to approximately 15 percent reactor power. The main feedwater control valve provides feedwater flow control from approximately 15 percent to 100 percent power. Each feedwater valve has a Hand/Automatic control station which enables automatic control or the operator to manually establish a valve position demand.

Feedwater flow to both steam generators is provided from two turbine driven main feedwater pumps. The speed of both feedwater pumps is controlled by a single automatic controller to maintain a constant differential pressure across the feedwater valves. Feedwater valve differential pressure is compared to set point and the resultant error is the controller demand signal. The loop A and loop B feedwater master demand signals are input to the controller as a feed forward signal to reduce the amount of feedwater valve differential pressure change during load changes. Each main feedwater pump has a Hand/Automatic control station which enables automatic control or the operator to manually establish a pump speed demand.

Feedwater Control - Reactor Coolant Pumps tripped

Upon loss of all reactor coolant pumps, the ICS positions valves to direct main feedwater flow to the auxiliary feedwater header in each steam generator. The steam generator operate level is used as a demand signal to the startup feedwater valve to establish "natural circulation" cooling of the reactor coolant system.

Steam Generator Overfill Protection

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 10CFR 50.54(f)," on September 20, 1989. This generic letter required PWR licensees to provide a description of their steam generator overfill protection (SGOP) 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 Oconee overfill protection system is provided by the Integrated Control System (ICS) and is initiated on high water level in anyone steam generator, based on non-safety grade hardware with a 2-out-of-2 initiating logic. When the high level setpoint is reached, the ICS terminates feedwater by tripping the main feedwater pumps. The Steam Generator Overfill Protection system also added an alternate non-safety grade trip device, SV6, to assure trip of the main feedwater pump turbine in the event of a loss of control power. The NRC SER (see section 10.4.9, Reference II) concluded that this addition minimized the potential for common mode failure such that the overall design of Steam Generator Overfill Protection sufficiently satisfies the single-failure criterion of Generic Letter 89-19.

7.6.1.2.2.4 Reactor Control

The reactor control is designed to maintain a constant average reactor coolant temperature over the load range from 15 to 100 percent of rated power. The steam system operates on constant pressure at all loads. The average reactor coolant temperature decreases over the range from 15 percent to zero load. Figure 7-18 shows the reactor coolant and steam temperatures and the steam pressure over the entire load range.

The Reactor Control Subsystem controls the neutron flux production of the reactor. The subsystem varies the neutron flux such that primary temperature and pressure requirements are maintained, while the heat drawn from the primary system meets the CTPD.

The reactor control subsystem controller receives inputs from core thermal power demand, reactor coolant pressure and reactor coolant average temperature. The output of the controller is an error signal that causes the control rod drives to be positioned until the error signal is within a deadband. A block diagram of the reactor control is shown on Figure 7-19.

A reactor power demand can be established in two ways. The operator can manually establish a reactor power demand using the reactor master hand/automatic control station. The second method of establishing a reactor power demand is with the reactor master control station in automatic. In this mode of operation, the reactor demand becomes a function of CTPD with a modification from Tave, steam pressure and transient RC pressure control.

Cross limits are employed between the reactor control and feedwater control subsystems to help ensure that the basic demand relationships between the reactor and feedwater are preserved during transients. In addition to cross limits, the controller also incorporates a high limit on reactor power level demand.

The reactor power level demand is compared with the reactor power level (neutron flux). The resultant error signal is the reactor power level error (neutron error) signal.

When the reactor power level error signal exceeds the deadband settings, the control rod drive receives a command that withdraws or inserts rods depending upon the polarity of the power error signal.

The reactor controls incorporate automatic or manual rod control above 2 percent of rated power and manual control below 2 percent of rated power.

7.6.1.2.3 System Evaluation

Redundant sensors for major system parameters are available to the Integrated Control System. The list of redundant major system parameters is contained in Section 7.4.2.2.2.

Automatic signal selection between the redundant sensors is provided as described in Section 7.4.2.2.2. The operator can manually select between the redundant sensors which are monitored by SASS; however, if a failure occurs the automatic signal selector (SASS) will transfer the output signal from the failed device to the valid input. The SASS also will not allow the operator to select the failed sensor if the failure occurred on the non-selected sensor. The "Control STAR" uses the median signal selection technique to select between redundant sensors. If a sensor failure occurs the "Control STAR" automatically transfers to the valid redundant sensor. The operator does not have manual selection capability between the redundant sensors which input to "Control STAR"; however, specific sensors can be selected by special maintenance techniques.

Manual reactivity control is available at all power levels. Loss of electrical power to the ICS Automatic control reverts the control system to manual.

Maloperation or failure of any ICS subsystem places no automatic limitations on reactor operation because the ICS reverts to the manual mode. Therefore other ICS subsystems follow the limited subsystem.

The design of the NNI/ICS System in conjunction with procedures and training allow the operator to cope with various loss of power situations. Also, alarm indications provide information to the operator of various instrument and control functions. Emergency procedures provide assurance of positive responses by the operator.

Failure of the ICS does not diminish the safety of the reactor. None of the functions provided by the ICS are required for reactor protection or for actuation of the ESPS. The reactor protection criteria, used in the analysis of accidents presented in Chapter 15 can be met irrespective of ICS action.

7.6.1.2.3.1 Modes of Control

The Integrated Control System is designed to revert to a "Tracking" mode to tie the unit to the subsystem on manual or to the subsystem being limited. In the startup control mode, the reactor is prevented from automatic rod withdrawal below 1.5 percent power.

The controls will limit steam bypass to the condenser when condenser vacuum is inadequate.

7.6.1.2.3.2 Loss-of-Load Considerations

The nuclear unit is designed to accept 10 percent step load rejection without safety valve action or turbine bypass valve action. The combined actions of the control system and the turbine bypass valve permit a load reduction from 40 percent load without safety valve action. The controls will limit steam dump to the condenser when condenser vacuum is inadequate, in which case the steam safety valves may operate. The combined actions of the control system, the turbine bypass valves and the steam safety valves permit separation from the external transmission system without a reactor trip for power levels less than 50 percent.

The features that permit continued operation under load rejection conditions include:

Integrated Control System

During normal operations, the Integrated Control System controls the unit load in response to the core thermal power demand (CTPD) set by the operator. During loss of load, the CTPD is limited to a maximum 20 percent. The ICS will control reactor power, feedwater flow and bypass valve position to maintain the CTPD, Tave and steam pressure. The turbine governor takes control to regulate frequency.

100 Percent Relief Capacity in the Steam System

This provision acts to reduce the effect of large load drops on the Reactor System.

Consider, for example, a sudden load rejection from a power level above 20 percent. When the turbine-generator starts accelerating, the governor valves and the intercept valves close to maintain set frequency. As the governor valves close, steam pressure rises, forcing reduced energy transfer from the primary system and causing reactor coolant average temperature to rise. At the same time, a power demand runback is initiated to 20 percent power by the CTPD, causing reduction in the feedwater and reactor demand signals. The rise in reactor coolant temperature will help initially reduce reactor power along with the reduction in demand. The bypass valves will open in response to the increased steam pressure to reject the excess steam flow to the condenser. In addition, when the load rejection is of sufficient magnitude, the safety valves open to exhaust steam to the atmosphere. If transient conditions warrant, the feedwater system will increase feedwater flow to mitigate the undercooling condition caused by the sudden reduction in steam flow from the loss of load.

As operation continues with the turbine- generator carrying the in-house electrical loads, the turbine control will operate in the frequency control mode, the reactor and feedwater will operate to maintain proper reactor conditions at reduced demand and the bypass system will reject the excess steam flow to the condenser to control steam pressure.

7.6.1.2.3.3 Loss of Power Supply Considerations

The ICS/NNI system power supply is arranged such that it is normally powered from a dedicated static inverter system, which receives a DC input from the Vital I & C batteries, and is backed by an AC input

from one of the plants regulated non-load shed buses (Chapter 8). Both automatic and manual transfer switching is provided to select between these supplies.

In addition to the power supply reliability for the ICS, essential plant parameters necessary for shutdown have been arranged with their power supplies independent of the ICS source. Also, a "display group" has been developed and defined on the plant operator aid computer such that upon a loss of ICS power, the operator may quickly have full and complete information on key primary and secondary system parameters. Emergency procedures have also been developed to designate alternate sources of information on key plant parameters if the computer is unavailable, thus assuring the operator can obtain sufficient systems information. The reliable ICS power supply and the development of operator information are consistent with NRC Bulletin 79-27, "Loss of Non-Class IE I&C Power System Bus During Operation," as described in Reference 1.

If a loss of power event occurs, the ICS/NNI is designed to send the plant to a "Known Safe State" (KSS) by initiating a trip of both main feedwater pumps via the failsafe design of the high steam generator level monitoring circuits. These circuits are designed such that upon a loss of both "hand" and "auto" power they will initiate a trip of the main feedwater pumps and main turbine which will also trip the reactor via the Anticipatory Reactor Trip System (ARTS) circuitry. Emergency feedwater is also initiated upon loss of both feedwater pumps as described in Section 7.4.3. Upon loss of either "hand" or "Auto" power, steady state operation is maintained.

7.6.2 Incore Monitoring System

The Incore Monitoring System has been upgraded to meet the requirements of NUREG 0737 Item II.F.2.

7.6.2.1 Description

The Incore Monitoring System provides neutron flux detectors to monitor core performance. Incore self-powered neutron detectors measure the neutron flux in the core to provide a history of power distributions during power operation. Data obtained provides power distribution information and fuel burnup data to assist in fuel management decisions. The plant computer provides normal system readout and a backup readout system is provided for selected detectors.

7.6.2.2 System Design

The Incore Monitoring System consists of assemblies of self-powered neutron detectors and temperature detectors located at preselected positions within the core. Each core can contain up to 52 incore assemblies. The incore monitoring locations are shown on Figure 7-20. In this arrangement, an incore detector assembly consisting of seven local flux detectors, one background detector, one thermocouple and a calibration tube is installed in an instrumentation guide tube. The local detectors are positioned at seven different axial elevations to indicate the axial flux gradient. The outputs of the local flux detectors are referenced to the background detector output so that the differential signal is a true measure of neutron flux. The temperature detectors located just above the top of the active fuel in the fuel assemblies measure core outlet temperature.

Multi-point recorder readouts of selected detectors are provided independent of the computer.

When the reactor is depressurized, the incore detector assemblies can be inserted or withdrawn through guide tubes which originate at a shielded area in the Reactor Building as shown in Figure 7-21. These guide tubes enter the bottom head of the reactor vessel where internal guides extend up to the instrumentation tubes of 52 selected fuel assemblies. The instrumentation tube serves as the guide for the incore detector assembly. During refueling operations, the incore detector assemblies are withdrawn approximately 13 feet to allow free transfer of the fuel assemblies. After the fuel assemblies are placed in their new location, the incore detector assemblies are returned to their fully inserted positions.

7.6.2.3 Calibration Techniques

The nature of the detectors permits the manufacture of nearly identical detectors which produces a high relative accuracy between individual detectors. The detector signals are compensated continuously for burnup of the neutron-sensitive material.

Calibration of detectors is not required. The incore self-powered detectors are controlled to precise levels of initial sensitivity by quality control during the manufacturing stage. The sensitivity of the detector changes over its lifetime due to such factors as detector burnup, control rod position, fuel burnup, etc. The results of experimental programs to determine the magnitude of these factors have been incorporated into calculations and are used to correct the output of the incore detectors for these factors. Operation of these detectors in both power and test reactors has demonstrated that this compensation program, when coupled with the initial sensitivity, provides detector readout accuracies sufficient to eliminate the need for a calibration system.

7.6.2.4 System Evaluation

7.6.2.4.1 Operational Experience

Self-powered incore neutron detectors have been operated since 1962. Such detectors have been assembled and irradiated in a Babcock & Wilcox development program that began in 1964.

The B&W Development Program included these tests:

1. Parametric studies of the self-powered detector.
2. Detector ability to withstand PWR environment.
3. Multiple detector assembly irradiation tests.
4. Background effects.
5. Readout system tests.
6. Mechanical withdrawal-insertion tests.
7. Mechanical high pressure seal tests.
8. Relationship of flux measurement to power distribution experiments.

Conclusions drawn from the results of the test programs are as follows:

1. The detector sensitivity, resistivity, and temperature effects are satisfactory for use.
2. A multiple detector assembly can provide axial flux data in a single channel and can withstand reactor environment.
3. Background effects will not prevent satisfactory operation in a PWR environment.
4. Plant computer systems are successful as read-out system for in-core monitors.

For Incore Monitoring System development program results and conclusions, refer to B&W Topical Report BAW-10001A; "Incore Instrumentation Test Program."

7.6.2.4.2 Deleted Per 1997 Update

7.6.2.5 Detection and Control of Xenon Oscillations

Under normal operating conditions, the incore detectors supply information to the operator in the control room.

Each individual detector measures the neutron flux at its locality and is used to determine the local power density. The individual power densities are then averaged and a peak-to-average power ratio calculated. This information can be used to indicate possible power oscillations.

7.6.3 References

1. NRC Letter to Duke dated December 7, 1989, Oconee: Audit for Verification of Resolution of IE Bulletin 79-27 concerns

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.6.

THIS PAGE LEFT BLANK INTENTIONALLY

7.7 Operating Control Stations

Following proven power station design philosophy, all control station, switches, controllers, and indicators necessary to start up, operate, and shut down Oconee l and 2 are located in one control room. Controls for Oconee 3 are located in a separate control room. Control functions necessary to maintain safe conditions after a loss-of-coolant accident are initiated from the centrally located control rooms. Controls for certain auxiliary systems are located at remote control stations when the system controlled does not involve unit control or emergency functions.

7.7.1 General Layout

The control room for Oconee 1 and 2 is designed so that one man can supervise operation of both units during normal steady state conditions. During other than normal operating conditions, other operators are available to assist the control operator. Figure 7-26 shows the control room layout for Oconee l and 2. Oconee 3 has similar accessibility to the various controls. The control boards are subdivided to show the location of control stations and to display information pertaining to various sub-systems.

7.7.2 Information Display and Control Functions

Consideration is given in the control board layout to the fact that certain systems normally require more attention from the operator. The Integrated Control System is therefore located nearest the center line of the boards (Section l on Figure 7-26).

On Section 2 of the control board, one indicator will be provided for each control rod. Fault detectors in the Rod Drive Control System are used to alert the operator should an abnormal condition exist for any individual control rod. Displayed in this same area are limit lights for each control rod group and all nuclear instrumentation information required to start up and operate the reactor. Control rods are manipulated from the Section 2 bench position. Plant computer readout facilities for alarm monitoring and sequence monitoring are located here to aid the operator.

A plant computer is used on each unit to provide fuel management measurements and calculations. These computers also provide for alarm monitoring, performance monitoring, data logging, and sequence monitoring during start-up and shut-down of the turbine-generator. Monitoring and display functions of the plant computer which audit Nuclear Steam Supply System parameters of major interest are duplicated elsewhere in the control rooms. This type of computer application has been successfully applied to units presently in operation on the Duke system.

Variables associated with operation of the secondary side of the station are displayed and controlled from Section 1 and 3 of the control board. These variables include steam pressure and temperature, feedwater flow and temperature, electrical load, and other signals involved in the Integrated Control System. Section 3 of the control board also contains indication and controls of the Reactor Coolant System parameters.

The Engineered Safeguards System is controlled and monitored from Sections 3 and 4 unit boards and Section 8 of the vertical boards. Indicating lights are provided as a means of verifying the proper operation of the Engineered Safeguards System. Control switches located on these panels allow manual operation of equipment that is not controlled elsewhere in the control room or test of individual units.

Control and display equipment for station auxiliary systems are located on Section 6 of the control board.

Reactor coolant pump controls located on Section 5 of the control boards consists of the pump controls and auxiliary instrumentation required for pump operation. Also mounted on this section are the Auxiliary Electrical System controls required for manual switching between the various power sources described in Section 8.2 and Section 8.3.

Controls and indications for all normal ventilation systems are located on Section 7 of the control boards.

In order to maintain the desired accessibility for control of the station, miscellaneous recorders not required for station control are located on the vertical recorder boards where they are visible to the operator. Radiation monitoring information is also indicated there.

Radiation monitoring display and transient monitoring system are combined in the process monitoring computer (PMC). The radiation monitoring display provides supervisory control and display of information from field mounted radiation monitoring equipment. The transient monitoring system automatically records pre-selected plant parameters (temperatures, pressures, flowrates, etc.) for analysis and diagnoses of plant transients or reactor trip. Like the OAC, most of the information provided by the PMC is either duplicated elsewhere in the control room, or deemed not significant enough to have a dedicated display device. The PMC is not QA-1, redundant, or single failure proof. The PMC is independent of the OAC. The PMC is not relied upon to initiate a reactor trip, mitigate an accident, or actuate a safety system, and performs only supervisory control to field mounted radiation monitoring and sampling equipment.

A description and results of the Unit 1, 2, and 3 control room review (per Generic Letter 82-33) were provided in the document "Response to Supplement 1 to NUREG-0737" which was submitted on April 14, 1983 by letter from H. B. Tucker to H. R. Denton.

7.7.3 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 Reactor Building 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. Alarms are provided to warn security of unauthorized entry into vital areas.

7.7.4 Communications

7.7.4.1 Control Room to Inside Station

The telephones for the site are connected to a Private Automatic Branch Exchange (PABX) located inside the Oconee Office Building. The PABX has capability of up to 10,000 lines and provides access for communications and paging. The equipment provides 4-digit dialing, dial tone, ring-back tone and busy tone. The PABX is powered by 48VDC batteries, which are charged through an inverter/charger combination, fed by a 480VAC supply. Upon loss of normal AC power, the system batteries will provide required power for a minimum of four (4) hours. Alternate power is automatically provided from the emergency diesel generator provided for the building.

The public address system is accessible through plant telephones by dialing a access code. In the event of PABX failure, the PA system is operable through eleven handsets installed at strategic locations within the station.

A radio transmitter/receiver communication system is provided between the control room and the rest of the station. This system is used during normal plant operation and during outage, security or fire situations. Radio transmission is only available in a reactor building when an antenna is activated by the unit 1 & 2 control room. Usage of the radio communication system in the reactor building is limited to times when the unit is open for access.

A sound powered telephone system was supplied during original plant design, but radio utilization allows this system to be an available but nonessential system. This system consists of a network of conductor

pairs converted to jacks throughout the plant. Sound powered handsets are plugged into the jacks to form talking paths with separate talking paths available for each unit. The system is completely independent from any other telephone system and involves no external power supply.

7.7.4.2 Control Room to Outside Station

The commercial telephone network and the Duke Power fiber optic network provide communication to outside the station area. An interface is provided between the PABX and the commercial telephone lines and another interface is provided between the PABX and the Duke Power fiber optic network which includes access to the General Office at Charlotte, Transmission Control Center, System Operating Center, and Lee Steam Station. Ringdown phone service (independent of the PABX) is also provided through the fiber optic network to the Transmission Control Center, System Operating Center, and Lee Steam Station.

The control room is also equipped with a transmitter-receiver which operates at 800 megahertz to provide communication between the control room and the System Operating Center, Transmission Control Center, and Bad Creek, Jocassee, and Keowee Hydro Stations.

7.7.4.3 Deleted per 1998 Revision

7.7.5 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 rooms for maximum hypothetical accident conditions. Each Control Room Ventilation System is provided with radiation detectors and appropriate alarms. See Section 9.4.1 for control room ventilation systems description. Emergency lighting is provided.

The potential magnitude of a fire in either 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 IEEE 383-1974. (Reference IPCEA S-19-81 & ASTMD 2220-68)
3. Qualified trained personnel, adequate extinguishers, and accessibility to all control room areas are provided.

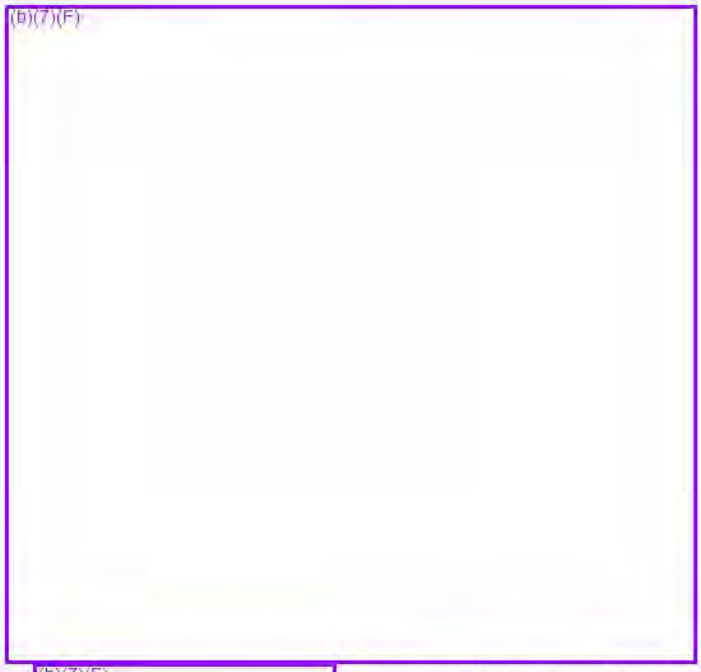
A fire, if started, would be of such a small magnitude that it could be extinguished by the operator using a hand fire extinguisher. The resulting smoke and vapors would be removed by the ventilation system in the case of Unit 3. For Units 1 & 2, the control room would be purged with portable equipment.

Essential auxiliary equipment is controlled by either stored energy, closing-type, air circuit breakers which are accessible and can be manually closed in the event DC control power is lost, or by AC motor starters which have individual control transformers.

7.7.5.1 Emergency (Auxiliary) Shutdown Panel

If temporary evacuation of the control room is required while operating at any power, the operator will trip the control rods and start the Keowee hydro units prior to evacuating the control room. (b)(7)(F) (b)(7)(F) . After evacuation, the operator can establish and maintain a hot shutdown condition from the emergency shutdown panel located (b)(7)(F) The following instrumentation and controls are available on the emergency shutdown panel:

(b)(7)(F)



If (b)(7)(F) is in operation, it can be tripped from the 4.16 KV switchgear located on elevation 796' + 6". The operator has control of (b)(7)(F) at the emergency shutdown panel. Makeup to the letdown storage tank can be obtained, if desired, from one of the following sources:

1. RC Bleed Holdup Tank
2. Concentrated Boric Acid Storage Tank
3. Boric Acid Mix Tank

The necessary pumps can be controlled from the waste disposal control panel.

7.7.5.2 Standby Shutdown Facility

The Standby Shutdown Facility (SSF) provides a secondary alternate and independent means to achieve and maintain a hot shutdown condition for scenarios in which the Control Room is unavailable or equipment it controls is unavailable. The SSF was designed for safe shutdown during postulated fire, Turbine Building flooding, and physical security events. The following instrumentation and controls are available on the SSF:

SSF DIESEL GENERATOR AND STATION RELATED CONTROLS AND INSTRUMENTATION

1. Diesel Generator Annunciator Panel
2. Diesel Generator Controls
3. Diesel Generator Metering
4. Diesel Generator Syncroscope
5. SSF Power Systems Breaker Controls and Indicating Lights
6. SSF Power Systems Metering
7. SSF Diesel Engine Service Water Pump Control
8. SSF Diesel Engine Service Water Pump Discharge Flow Meter
9. SSF Auxiliary Service Water Pump Control

10. SSF Auxiliary Service Water Pump Discharge Flow Meter
11. SSF Sump Pump Controls

SSF UNIT RELATED CONTROLS AND INSTRUMENTATION

1. Unit Annunciator
2. Unit Recorder
3. (b)(7)(F)
4. Unit Process Indicators
   a. Pressurizer Level
   b. Pressurizer Pressure
   c. RC Loop A and B Hot Leg Temperatures
   d. RC Loop A and B Cold Leg Temperatures
   e. RC Loop A and B Pressure
   f. Steam Generator Level A and B
   g. Steam Generator Auxiliary Service Water Flow
5. (b)(7)(F)
6. Power Systems Alignment Indicating Lights

7.7.6 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. The control functions initiated from local control stations do not directly involve either the Engineered Safeguards System if actuated or the Reactor Control System. Sufficient indicators and alarms are provided so that the Oconee control room operator is made aware of abnormal conditions involving remote control stations.

7.7.7 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 safeguards section 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 7.7.

7.8 Anticipated Transients Without SCRAM (ATWS) Mitigation System

7.8.1 Design Basis

The ATWS system that is installed at the Oconee Nuclear Station is based upon the B&WOG Generic ATWS Design Basis Document 47-1159091-00 dated October 9, 1985, subsequent B&WOG ATWS Committee submittal dated December 1, 1987, the Safety Evaluation Report on B&WOG 47-1159091-00 contained in the NRC letter to DPCo dated July 26, 1988, and the September 7, 1988 letter G. Holohan (NRC) to L. Stalter (B&WOG). The ATWS system was installed as required by the ATWS Rule, 10CFR50.62, "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants."

7.8.2 Systems Design

The ATWS Mitigation System is composed of two parts, the ATWS Mitigating Systems Actuation Circuitry (AMSAC) and the Diverse SCRAM System (DSS).

The ATWS Mitigation System Actuation Circuitry (AMSAC) and Diverse Scram System (DSS) consist of two Programmable Logic Controllers (PLC's) for the logic control circuits and two Uninterruptible Power Sources (UPS) connected to offsite power. Inputs from the field sensors are wired to the PLC's and outputs to the final actuation devices are wired using interfacing relays housed with the ATWS equipment cabinets and powered from the UPS. The UPS's are powered from a 120 VAC local panelboard backed by the Oconee Station emergency source (Keowee Hydroelectric Generating Station). The 2 UPS's are isolated from the emergency source by individual fuses coordinated with the panelboard circuit breakers and the upstream distribution network.

The AMSAC/DSS System consists of a two channel energize-to-trip design with the AMSAC portion actuated on low Feedwater Pump Turbine (FDWPT) control oil pressure or low Feedwater Pump (FDWP) discharge pressure while the DSS portion is actuated upon high Reactor Coolant System (RCS) Pressure.

All AMSAC/DSS PLC's and UPS power supplies are located in a stand-alone cabinet located above the Control Room in what is called the Ventilation Room. This location is convenient to the Control Room and allows easy access for testing and maintenance. This location is a Mild Environment.

All AMSAC/DSS process monitoring inputs are provided by existing Oconee instrumentation and control systems. RCS pressure inputs to the DSS which are analog signals are currently displayed on the Main Control Boards. Annunciator alarms are provided in the Control Room to alert the operator that one channel for either AMSAC or DSS has actuated.

7.8.2.1 AMSAC

Each channel of AMSAC uses existing inputs from the Feedwater System which monitor FDWPTA(B) hydraulic control oil pressure and FDWPA(B) discharge pressure signals (one per pump to each channel) from pressure switches which are part of the original Oconee feedwater system design.

These signals are multiplied using relays to provide the contact inputs which will be wired directly to the PLC's. These signals are processed using programmable logic resident in the PLC to provide the outputs to the Main Turbine and the Emergency Feedwater System.

AMSAC interfaces with the following systems and devices:

FROM	TO	ISOLATION
AMSAC PLC Interfacing Relays	Main Turbine Trip Solenoid	NE to NE
AMSAC PLC Interfacing Relays	EFDW Pump Start Circuits	NE to 1E
AMSAC Channels Actuation	Control Room Annunciator	NE to NE
NE = Non-Class 1E	1E = Class 1E	

Feedwater Pump Turbine Oil Pressure is sensed by pressure switches in the Feedwater Pump Turbine Control Console on the turbine standard. These switches are then multiplied using control relays for output to various plant control, monitoring and alarm circuits. AMSAC will be one of the end users of these signals.

Feedwater Pump Discharge Pressure is sensed by pressure switches in the discharge lines of each individual pump. These switches are then multiplied using control relays for output to various plant control, monitoring and alarm circuits. AMSAC will be one of the end users of these signals.

7.8.2.2 DSS

Each channel of DSS uses a Wide Range RCS Pressure signal supplied via an analog isolator from the Westinghouse supplied Reactor Vessel Level Indication System (RVLIS). These signal loops also provide the Regulatory Guide 1.97 wide range RCS pressure indications on the main control board. The DSS utilizes the signal conditioning equipment which is resident in the RVLIS cabinet through an isolation device that separates the Class 1E RVLIS from the Non-Class 1E DSS. DSS trip actuation is initiated at a setpoint of 2450 ± 25 psig using the logic in the PLC. Outputs from both channels of the PLC's are combined to make the required two-out-of-two logic. DSS provides two digital inputs (one per channel) to the CRD system. Upon actuation of both channels of DSS, the CRD system opens a normally-closed solid-state relay contact in each of the 138 Single Rod Power Supply (SRPS) modules. This interrupts power to the CRDM's causing all control rods (except the captured APSR's) to fall into the core resulting in a reactor trip. DSS also signals the ICS to raise the Turbine Bypass Valve pressure setpoint to ensure shutdown margin requirements are maintained.

DSS interfaces with the following systems and devices:

FROM	TO	ISOLATION
DSS Interfacing Relays	Single Rod Power Supplies	NE to NE
DSS Interfacing Relays	TBV's Control Setpoint	NE to NE
Deleted Row(s) per 2009 Update		
DSS Channel Actuation	Control Room Annunciator	NE to NE
WR RCS Pressure (RVLIS)	DSS PLC Channels	1E to NE
NE = Non-Class 1E	1E = Class 1E	

The Control Rod Drive (CRD) System also provides an input from the CRD Diamond panel located in the main Control Room into the DSS logic for reset of the CRD SRPS modules.

7.8.2.3 Testing

Inputs are also provided from the ATWS test panel. The panel is resident in the PLC cabinet along with other ATWS equipment.

Periodic testing will use a Bypass/Enable switch located on the test panel for testing each channel of AMSAC and DSS logic in the PLC. Whenever this switch is not in the ENABLE position, a continuous indicator in the Control Room will be illuminated and a computer alarm will be generated for display in the Control Room on a CRT. Status indication of all inputs and outputs are on the test panel.

These systems are designed so that both are two out of two logic actuated systems, and provisions are incorporated which allow disabling of the system output when one of the channels is placed in test. This prevents accidental initiation of the systems during individual channel testing.

7.8.2.4 AMSAC and DSS I/O

Each input to the AMSAC and DSS logic is provided with complete indications and alarms that alert the operator to an off-normal status that might preclude proper response to an ATWS event. Each plant variable that inputs into the AMSAC and DSS is monitored as part of the existing plant indications and provide the operator with information relevant to the status of each variable prior to reaching the AMSAC or DSS set point.

Outputs from the PLC's are provided through interfacing relays located in the ATWS equipment cabinets. These relays provide the outputs to the Main Turbine, Turbine Bypass Valve Set Point, the Emergency Feedwater Pumps, and the Control Rod Drive System for Single Rod Power Supplies via the CRD system PLC. The relays used are powered by the UPS. Each PLC channel output relays will be wired to the above devices in a manner such that both channels of AMSAC/DSS are required for the devices to trip, start, or drop. The relays also provide output status information to the operator.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.8.

THIS PAGE LEFT BLANK INTENTIONALLY.

7.9 Automatic Feedwater Isolation System (AFIS)

7.9.1 Design Basis

The Automatic Feedwater Isolation System (AFIS) circuitry is designed to address containment over-pressurization concerns, unacceptable thermal stresses to the steam generator tubes, and significant core overcooling by isolating main and emergency feedwater to the faulted steam generator during a Main Steam Line Break event. AFIS is credited in the steam line break containment response analysis (Section 6.2.1.4) and the steam line break tube stress analysis (Section 5.2.3.4). AFIS is not credited for the steam line break core response analyses (Sections 15.13 and 15.17). The design basis of the system includes the items of Section 7.1.2 with the following additions:

7.9.1.1 Loss of Power

1. The loss of vital bus power to an analog channel will cause a loss of signal to that analog channel creating a 1-out-of-4 coincidence without AFIS actuation.
2. The loss of vital bus power to a digital channel will not initiate system actuation.

7.9.1.2 Equipment Removal

1. Removal of an isolation module from the AFIS system will require a bypass on 2 analog channels (for AFIS and Trip Confirm modules) in both digital channels or AFIS system actuation will occur.
2. Removal of a logic module from one protective digital channel does not affect the other protective digital channel and does not initiate system action.

7.9.1.3 Control Logic of AFIS System

AFIS has priority over the automatic actuation/operation of systems affected. All systems receiving the AFIS signal remain controlled by AFIS unless manual control is taken. The affected EFW pumps can be operated manually to override the AFIS actuation. A separate deliberate action is required to place the affected systems in manual prior to performing a reset of the AFIS functions.

7.9.2 System Design

7.9.2.1 System Logic

The AFIS instrumentation is designed to provide automatic termination of feedwater and emergency feedwater flow to the affected steam generator. The AFIS instrumentation automatically terminates Main Feedwater (MFW) by tripping both MFW pumps and closing the affected steam generator's main and startup feedwater control valves (MFCV and SFCV) and block valves. Although the main and startup feedwater block valves are automatically closed, their closure is not credited for mitigation of a MSLB. The AFIS logic automatically terminates emergency feedwater (EFW) by stopping the turbine-driven emergency feedwater pump (TDEFWP) and tripping the motor-driven emergency feedwater pump (MDEFWP) aligned to the affected steam generator. Manual overrides for the TDEFWP and MDEFWPs are provided to allow the operator to subsequently start the EFW pumps if necessary.

In addition, AFIS actuation limits EFW pump runout in the event of a MSLB and certain large break MFW line breaks with the pump in the automatic mode of operation.

Main Steam header pressures are used as input signals to the AFIS circuitry. There are four QA-1 pressure transmitters per header with each feeding a steam pressure signal to a signal isolator. The output

of the signal isolator provides an analog signal to a processor module that actuates isolation functions at desired setpoints. One pressure transmitter per header and associated cabling and resistors constitute an AFIS detection analog channel.

The four AFIS analog channels per header feed two redundant AFIS digital channels. Each digital channel provides independent circuit functions to isolate each steam generator. If the logic is satisfied, a trip output is energized. The use of an energized-to-trip processor module ensures that a loss of power to the digital channel will not result in inadvertent feedwater isolation. If either digital channel is actuated, feedwater is isolated to the affected steam generator. Energizing the trip outputs results in the actuation of contacts in various control circuits for systems and components used for the MSLB and feedwater line break mitigation. Therefore, when the trip outputs are actuated, the systems and components perform their isolation functions. Other features of the digital channels include header specific manual initiation pushbuttons, a header specific ENABLE/OFF switch, and redundant "trip confirm" modules for each digital channel. The AFIS digital channel is defined as the analog isolation modules, the (4) digital 2-out-of-4 logic modules (Framatome STAR), the ENABLE/OFF pushbutton, the manual initiation pushbutton, the associated trip relays, the trip relay outputs to the feedwater pumps, the switchgear trips for the MDEFWP, the solenoid valves for the MFCV and SFCV, the trip solenoid valves for the feedwater pumps, and the TDEFWP trip function. While AFIS provides isolation of the feedwater block valves, this is not a credited function and is not a requirement for digital channel operability.

The AFIS digital channels are enabled and disabled administratively rather than automatically. Appropriate operating procedures contain provisions to enable/disable the digital channels.

7.9.2.2 Trip Setpoints

Trip setpoints are the nominal values that are user defined in AFIS software. An AFIS analog channel is considered to be properly adjusted when the AS LEFT value is within the band for channel calibration accuracy.

The trip setpoints used in the AFIS software are selected such that adequate protection is provided when all sensor and processing time delays are taken into account. The trip setpoints are set for low main steam pressure and a high rate of depressurization associated with a specific steam generator. To allow for calibration tolerances, instrumentation uncertainties, instrument drift, the allowable values specified are conservatively adjusted with respect to the analytical limits. The actual nominal trip setpoint entered into the software is controlled procedurally.

7.9.2.3 Availability of Information

All system analog signals are indicated within the system cabinets and are monitored by the plant computer. All BWNT STAR module outputs are indicated within the cabinets and their state monitored by the plant computer. Plant annunciators provide the operator with immediate indication of changes in the status of the processor module inputs and outputs. The following conditions are annunciated for the AFIS system:

1. Digital Channel 1 Test/Disable
2. Digital Channel 2 Test/Disable
3. AFIS Initiate Header A
4. AFIS Initiate Header B
5. AFIS Analog Channel Trip

Initiation of Header A (3) or Header B (4) requires simultaneous detection by both the "primary" and "trip confirm" modules of either of the Digital Channels for the Low Pressure Trip. Inadvertent actuation

of the "primary" low pressure trip without confirmation from the "trip confirm" function or actuation of the "trip confirm" by itself will not result in an AFIS system actuation but will be annunciate on the appropriate "trouble" annunciator (1 or 2). The STAR modules indicate when any "one out of four" analog channel trip occurs, which the annunciator (5) will be illuminated.

7.9.2.4 Summary of Protective Action

The AFIS circuitry is designed to address containment over-pressurization concerns and thermal stresses on steam generator tubes by isolating feedwater to the faulted steam generator during a Main Steam Line Break event. Two conditions apply for AFIS actuation:

1. Low main steam pressure
2. Low main steam pressure and a high rate of depressurization

In response to the first condition of low main steam pressure, the AFIS circuitry trips the main feedwater pumps and trips or prevents the turbine driven emergency feedwater pump from automatically starting by redundantly and independently closing valves, MS-93 and MS-95. The AFIS circuitry also closes the main and startup feedwater control and block valves on the affected header.

In response to the second condition, AFIS circuitry performs the same actions as in the first condition with the addition of redundant trip signals to the motor driven emergency feedwater pump associated with the faulted steam generator.

7.9.3 System Evaluation

The four AFIS analog channels per steam generator feed two redundant feedwater digital channels. Each digital channel provides independent circuit functions to isolate each steam generator. If the logic is satisfied, a trip output is energized. The use of an energized-to-trip processor module ensures that a loss of power to the digital channels will not result in inadvertent feedwater isolation. If either digital channel is actuated, feedwater to the affected steam generator is isolated. Energizing the trip outputs results in actuation of contacts in various control circuits for systems and components used for the MSLB and feedwater line break mitigation. Therefore, when the trip outputs are actuated, the systems and components perform their isolation functions. While AFIS provides isolation of the feedwater block valves, this is not a credited function and is not a requirement for digital channel operability.

There is redundancy of sensors, logic, and equipment, excluding the main feedwater equipment. The redundancy is preserved and kept effective by independence of sensors, instrument strings, logic, and control elements in the final actuator. These characteristics enable the system to tolerate single failures at all levels.

To prevent a single-failure from causing loss of feedwater flow to one or both headers inadvertently, a redundant trip confirm function is provided that must also detect the low pressure trip condition in order to create an AFIS low pressure trip.

The system protective devices require electrical power in order to operate and perform their functions. The power for the STAR modules is taken from the plant's system of battery-backed vital buses since loss of power at this level could affect the performance capability of the system. The system will tolerate the loss of one vital bus without loss of protective capability.

7.9.3.1 Redundancy and Diversity

The system as evaluated above is shown to have sufficient diversity and redundancy to withstand single failures at every level, excluding the main feedwater components associated with AFIS.

7.9.3.2 Electrical Isolation

The use of analog isolation will effectively prevent adverse affects of faults (shorts, grounds, or cross connection of signals) on any analog signal leaving the system from being reflected into or propagating through the system. The isolation amplifier circuits have been qualified to isolate the output signal from input circuit faults. The STAR module employs diverse software to mitigate common mode failures.

Separation of redundant AFIS functions is accomplished by maintaining isolation for the power, control, equipment location, and cable routing between channels.

AC power for AFIS channels is supplied from independent vital power panels. Analog channel 1 is supplied from Vital Power Panelboard KVIA. Analog channel 2 is supplied from Vital Power Panelboard KVIB. Analog channel 3 is supplied from Vital Power Panelboard KVIC. Analog channel 4 is supplied from Vital Power Panelboard KVID. The digital channels, 1 and 2, are supplied from AC panelboards, KVIC and KVID, respectively. The devices controlled by the digital channels are supplied by redundant and independent QA-1 sources of power. These are described in Section 8.3.

7.9.3.3 Physical Separation

The arrangement of modules within the system cabinets is designed to reduce the chance of physical events impairing system operation. Channel specific control wiring between the STAR modules and the final actuating devices is physically separated and protected against damage, which could impair system operation. The equipment is separated to limit the possibility of spurious actuation.

Separation between redundant channels of equipment, control cables, and power cables provides defense of redundant AFIS functions. Power and control cables for redundant elements of AFIS equipment are routed in separate cable trays.

7.9.4 Periodic Testing and Reliability

The redundancy of the logic and the division of protective devices between channels form a system having two parallel protective channels either of which is capable of performing the required functions. These characteristics are basic to an inherently reliable system.

The built-in test facilities permit an electrical actuation test of each analog instrument string by the substitution of signals at the STAR module inputs. The AFIS STAR module provides both manual and automated test capability, and self-diagnostic tests performed during start-up and operation. The front panel of each of the STAR module has LED indicators, which indicate module status.

When testing, chance of an inadvertent initiation of an AFIS low pressure trip is minimized by the trip confirm function which requires actuation by both the primary and trip confirm modules.

When an analog instrument string is placed in test or bypass, the logic assigned to the digital control module changes the actuation logic to a 2-in-3 coincidence. This assures that placing an analog channel in test cannot defeat the protective action.

On-line checks of the system will confirm the normal state of the system, principally by comparative readings of similar analog indications between redundant measurements and by the status lamps on the logic modules.

7.9.5 Manual Initiation

A manual initiation switch is provided in each Automatic Feedwater Isolation System digital channel. The manual initiation switches are capable of actuating trip outputs without relying on the STAR outputs. There are two control switches on the control room board for the disabling of each digital channel and two control switches for manually initiating the respective header circuitry.

7.9.6 Bypassing

Bypassing must be initiated manually within a fixed pressure band above the protective system actuation point. The removal setpoints are above the actuation setpoints in order to obtain a pressure band in which the system actuation may be bypassed during a normal cooldown and startup. The bypasses do not prevent automatic actuation of the emergency feedwater pumps. Bypassing is under administrative control. Once a bypass has been initiated, the plant annunciator indicates the condition on Unit 1 only and by the OAC for all units.

After actuation of AFIS, the turbine driven and motor driven emergency feedwater pumps can be manually actuated or restarted from their respective control switches.

7.9.7 Deleted Per 2002 Update

7.9.8 Deleted Per 2002 Update

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.9.

THIS PAGE LEFT BLANK INTENTIONALLY.

7.10 Diverse Low Pressure Injection Actuation System (DLPIAS)

7.10.1 Design Basis

For units with a digital ESPS installed, a Defense-in Depth and Diversity (D^3) Analysis was performed per the guidelines of BTP HICB - 19. This analysis resulted in the inclusion of a Diverse Low Pressure Injection Actuation System (DLPIAS). The system is designed as diverse backup for ESPS during the unlikely event of a Large Break Loss of Coolant Accident (LBLOCA) concurrent with a Software Common Mode Failure (SWCMF) of the ESPS digital equipment.

7.10.2 System Design

The DLPIAS is a combination of both safety-related and non-safety-related components. The DLPIAS design does not require the use of any software. All DLPIAS process monitoring inputs are provided by existing Oconee instrumentation and control systems. The DLPIAS utilizes analog pressure input signals from the Reactor Coolant System (RCS), which are displayed on the Main Control Boards. RCS input pressure signals are isolated from the safety-related signals by the ESPS signal isolators. The signal is split on the front end of the ESPS and is not affected by the software of the ESPS computers. The analog RCS pressure signals provide input to the DLPIAS bistable trip units which output to a 2-out-of-3 relay logic circuit to actuate the ESPS Channel 3 and 4 devices. Power for the bistables and relay logic is non-safety-related.

The DLPIAS is actuated on low RCS Pressure. The system is designed as a diverse backup for ESPS during the unlikely event of a LBLOCA concurrent with a SWCMF of the ESPS digital equipment. A low RCS pressure condition is the most appropriate indication that a LBLOCA has occurred. Because the DLPIAS is a backup system for LBLOCA, the setpoint for actuation of the DLPIAS is chosen such that the ESPS actuation of the LPI components will occur prior to DLPIAS actuation.

Physical separation is maintained between safety-related and non-safety-related components per IEEE Std 384-1992 separation criteria. The bistables and relays are rail mounted components. Electrical separation between safety-related and non-safety-related components is maintained by the use of signal isolators for the analog signals and relays. All equipment associated with the DLPIAS, with the exception of the RCS pressure transmitters and associated cabling, is located in the Control Room and is qualified for a mild environment.

The DLPIAS 2-out-of-3 relay logic minimizes an inadvertent actuation of the LPI components. The circuit relays are energized to actuate, therefore loss of power will not result in actuation of the trip circuit. The design includes a DLPIAS Bypass Switch located on the Unit Control Board. The switch is used to bypass the DLPIAS system for both maintenance and operations.

Procedures require that the DLPIAS be bypassed on controlled shutdowns at the same time the LPI Bypass is initiated for the ESPS. The interface with the LPI actuation circuit is safety- related. The design includes indications in the Control Room for a DLPIAS trip, DLPIAS Bypass, and DLPIAS Bistable Tripped. The indication circuits are non-safety-related.

A DLPIAS Override switch is located on the unit board which allows operators to override the DLPIAS in case of an inadvertent actuation. Once the override is initiated, operators are able to manually position ESPS components.

Manual initiation of LPI is accomplished with the existing ESPS Trip/Reset buttons located on the main control board. The logic for this manual trip bypasses the ESPS logic and allows the Operator to initiate actuation on a per channel basis.

7.10.3 Testing

Periodic testing of DLPIAS will use the Bypass Switch located on the Control Board for testing each output channel of DLPIAS. Whenever this switch is in the Bypass position, an indicator in the Control Room will be illuminated continuously.

These systems are designed so that a 2-out-of-3 relay logic actuates the system, and provisions are incorporated which allow disabling of the system output when the protective channels are placed in test. This prevents accidental initiation of the system during protective channel testing.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.10.

7.11 Diverse High Pressure Injection Actuation System (DHPIAS)

7.11.1 Design Basis

For units with a digital ESPS installed, Duke committed to install a Diverse High Pressure Injection Actuation System (DHPIAS). This system is designed as a diverse backup for ESPS during the unlikely event of a Small Break Loss of Coolant Accident (SBLOCA) concurrent with a Software Common Mode Failure (SWCMF).

7.11.2 System Design

The DHPIAS is a combination of both safety-related and non-safety-related components. The DHPIAS design does not require the use of any software. All DHPIAS process monitoring inputs are provided by existing Oconee instrumentation and control systems. The DHPIAS utilizes analog pressure input signals from the Reactor Coolant System (RCS), which are displayed on the Main Control Boards. RCS input pressure signals are isolated from the safety- related signals by the ESPS signal isolators. The signal is split on the front end of the ESPS and is not affected by the software of the ESPS computers. The analog RCS pressure signals provide input to the DHPIAS bistable trip units which output to a 2-out-of-3 relay logic circuit to actuate ESPS Channel 1 and 2 devices. Power for the bistables and relay logic is non-safety-related.

The DHPIAS is actuated on low RCS Pressure. This system is designed as a diverse backup for ESPS during the unlikely event of a SBLOCA concurrent with a SWCMF of ESPS digital equipment. A low RCS pressure condition is the most appropriate indication that a SBLOCA has occurred. Because the DHPIAS is a backup system, the setpoint for actuation of the DHPIAS is chosen such that the ESPS actuation of the HPI components will occur prior to DHPIAS actuation.

Physical separation is maintained between safety-related and non-safety-related components per IEEE Std 384-1992 separation criteria. The bistables and relays are rail mounted components. Electrical separation between safety-related and non-safety-related components is maintained by the use of signal isolators for the analog signals and relays. All equipment associated with DHPIAS, with the exception of the RCS pressure transmitters and associated cabling, is located in the Control Room and is qualified for a mild environment.

The DHPIAS 2-out-of-3 relay logic minimizes an inadvertent actuation of the HPI components. The circuit relays are energized to actuate, therefore loss of power will not result in actuation of the trip circuit. The design includes a DHPIAS Bypass Switch located on the Unit Control Board. The switch is used to bypass the DHPIAS system for both maintenance and operations.

Procedures require that the DHPIAS be bypassed on controlled shutdowns at the same time the HPI Bypass is initiated for the ESPS. The interface with the HPI actuation circuit is safety- related. The design includes indications in the Control Room for a DHPIAS trip, DHPIAS Bypass, and DHPIAS Bistable Tripped. The indication circuits are non-safety-related.

A DHPIAS Override switch is located on the unit board which allows operators to override the DHPIAS in case of an inadvertent actuation. Once the override is initiated, operators are able to manually position ESPS components.

Manual initiation of HPI is accomplished with the existing ESPS Trip/Reset buttons located on the main control board. The logic for this manual trip bypasses the ESPS logic and allows the Operator to initiate actuation on a per channel basis.

7.11.3 Testing

Periodic testing of DHPIAS will use the Bypass Switch located on the Control Board for testing each protective channel of DHPIAS. Whenever this switch is in the Bypass position, an indicator in the Control Room will be illuminated continuously.

These systems are designed so that a 2-out-of-3 relay logic actuates the system, and provisions are incorporated which allow disabling of the system output when the protective channels are placed in test. This prevents accidental initiation of the system during protective channel testing.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.11.

Table of Contents

List of Tables

List of Figures

7.0 Instrumentation and Control

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.0.

THIS PAGE LEFT BLANK INTENTIONALLY.

7.1 Introduction

Instrumentation and control systems include the Reactor Protective System, the Engineered Safeguards Protective Systems, the Rod Drive Control System, the Integrated Control System, the Nuclear Instrumentation System, the Non-Nuclear Instrumentation System, the Incore Monitoring System and the Automatic Feedwater Isolation System.

7.1.1 Identification of Safety-Related Systems

The protective systems, which consist of the Reactor Protective Systems, the Engineered Safeguards System and the Automatic Feedwater Isolation System perform important control and safety functions. The protective systems extend from the sensing instruments to the final actuating devices, such as circuit breakers and pump or valve motor contactors.

7.1.2 Identification of Safety Criteria

7.1.2.1 Design Bases

The protective systems are designed to sense plant parameters and actuate emergency actions in the event of abnormal plant parameter values. They meet the intent of the Proposed IEEE "Criteria for Nuclear Power Plant Protection Systems" dated August, 1968. (IEEE No. 279). The RPS/ESPS also meets the intent of IEEE Std 603-1998. Protective system equipment located in the Control Room, Cable Room, and Aux Building is designed for a mild environment, not LOCA conditions (i.e. 59 psig, 273°F).

7.1.2.2 Single Failure

The protective options meet the single failure criterion of IEEE No. 279 and IEEE Std 603-1998 to the extent that:

1. No single component failure will prevent a protective system from fulfilling its protective functions when action is required.
2. No single component failure will initiate unnecessary protective system action where implementation does not conflict with the criterion above.

7.1.2.3 Redundancy

All protective system functions are implemented by redundant sensors, measuring channels, logic, and actuation devices. These elements combine to form the protective channels.

7.1.2.4 Independence

Redundant protective channels are electrically independent and are packaged to provide physical separation.

7.1.2.5 Separation

Protective channels are physically separate and are electrically isolated from regulating instrumentation. Only one string of instrumentation may be selected at a given time for use in a system control function, and electrical isolation is assured through the use of appropriate isolation devices. A fifth channel of regulating instrumentation not associated with protection is employed for additional control purposes.

Protective channels of the RPS and ESPS are interconnected with fiber optic cabling for inter-channel communication. These cables are used for diagnostic data that is shared between protective channels over

fiber optic communications links, do not serve a mutually redundant safety related function, and are not required for the RPS and ESPS to perform their safety related functions. Therefore, these fiber optic cables do not require physical separation. The fiber optic cables that run between safety-related cabinets or enclosures are colored red. Fiber optic media without metallic shields or armor inherently provides sufficient Class 1E electrical isolation for data exchange pathways between devices. Fiber optic cable that is used for mutually redundant safety related functions are required to be physically separated.

7.1.2.6 Manual Trip

Manual trip switches, independent of the automatic trip instrumentation, are provided.

7.1.2.7 Testing

Manual testing facilities are built into the protective systems to provide for:

1. Preoperational testing to give assurance that a protective system can fulfill its required protective functions.
2. On-line testing to prove operability and to demonstrate reliability.
3. In the Automatic Feedwater Isolation System (AFIS), BWNT STAR module provides both manual and automated test capability, and self diagnostic tests performed during start-up and operation. The front panel of the STAR module has LED indicators which indicate module status.
4. The RPS/ESPS provides a test mode and a manual bypass are provided. The system provides the capability to perform start-up and operational testing through the Graphical Service Monitor when the test mode is enabled. The system performs continuous testing through self checking routines.

7.1.3 Identification of Protective Equipment

All safety related sensors, transmitters, transducers, cabinets, etc. located outside the control room are physically identified by placement of a permanent, conspicuous tag on or adjacent to the device. A typical tag bears the wording "Safety Related." The following are examples of equipment that should be tagged:

Swgr 1TC

LD Ctr lX8

MCC lXSl

ESG channel 1, 3, 5, & 7

DC Pnlbd 1DIA

Vital Pwr Pnlbd 1KVIA

RPS Ch A

AFIS Analog Channel 1

Swgr 1TD

LD Ctr 1X9

MCC 1XS2

ESG channel 2, 4, 6, & 8

DC Pnlbd 1DIB

Vital Pwr Pnlbd 1KVIB

RPS Ch B

AFIS Analog Channel 2

Swgr 1TE

MCC lXS3

DC Pnlbd 1DIC

Vital Pwr Pnlbd 1KVIC

RPS Ch C

AFIS Analog Channel 3

AFIS Digital Channel 1

ESG Channel Even-Odd

DC Pnlbd 1DID

Vital Pwr Pnlbd 1KVID

RPS Ch D

AFIS Analog Channel 4

AFIS Digital Channel 2

7.1.4 NRC IE BULLETIN 90-1 AND SUPPLEMENT 1

The NRC issued IE Bulletin 90-1, "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 Power Company's Bulletin response actions included identification of transmitters from the suspect lots for Oconee 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 form 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 Oconee Nuclear Station.

The NRC issued Supplement 1 to IE Bulletin 90-01, "Loss of Fill-Oil in Transmitters Manufacturecd by Rosemount," on December 22, 1992, providing further details on monitoring programs for the transmitters described in the original bulletin. Duke Power Company responded on May 24, 1993 by the letter from H. B. Tucker to the NRC. Subsequently, the NRC issued its Safety Evaluation Report (SER) on May 19, 1995 which provided approval and closeout of IE Bulletin 90-01 and Supplemental 1 for the Oconee Nuclear Station.

7.1.5 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 Bulleting No. 90-01, Supplement 1, "Loss of Fill Oil in Transmitters Manufactured by Rosemount."

4. Nuclear Regulatory Commission, Letter from L. A. Wiens to J. W. Hampton (DPC), May 19, 1995, "NRC Bulletin 90-01 Supplement 1, Loss of Fill Oil in Transmitters Manufactured by Rosemount."

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.1.

7.2 Reactor Protective System

Deleted Paragraph (s) per 2009 Update

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

7.2.1 Design Bases

The RPS includes all design basis features of Section 7.1.2 with the following additions:

7.2.1.1 Loss of Power

A loss of power to a reactor protective channel will cause that protective channel to trip.

7.2.1.2 Equipment Removal

Deleted per 2013 Update.

Removal of a computer card from the RPS will initiate a protective channel trip. Removal of an input card will fault the input signals on that card and alarm, but will not initiate a protective channel trip. Removal of an output card will generate a channel trouble alarm and will initiate a half-channel trip (both of the outputs from the affected card assume a tripped state which creates a half-channel trip).

7.2.1.3 Diverse Means of Reactor Trip

In the unlikely event of a systematic or complete failure of the Reactor Coolant System low pressure signals to trip the reactor following the initiation of emergency core cooling, there is a separate, diverse means of assuring reactor trip. A high pressure in the Reactor Building is independently sensed by four sensors, and independent signals are fed from these sensors to the four Reactor Protective System channels to provide the desired diverse reactor trip signal.

7.2.2 System Design

7.2.2.1 System Logic

Deleted per 2013 Update.

Deleted Paragraph(s) per 2009 Update.

Deleted per 2013 Update.

The RPS consists of four independent protective channels, as shown in Figure 7-1. Each RPS protective channel contains the sensor input modules, output modules, a channel computer, four hardwired reactor trip relays (RTRs) and associated contacts. When the protective channel inputs are in the normal, or untripped, state the RTR is energized and no trip signal is sent to the CRD trip devices. Channel A provides input signals to its associated Channel A RTR within its cabinet and also sends this signal to each of its remaining Channel RTRs in the Channel B, C, and D cabinets. Each channel cabinet has the four RTR contact sets configured to provide 2-out-of-4 coincidence trip logic. When a protective channel trips, it sends the protective channel trip signal to its corresponding relays in each protective channel. When any two RPS protective channels receive channel trip signals, the RTR logic in each protective channel actuates to remove power from its associated CRD trip device. All RTRs trip whenever any two

of the four protective channels trip.

The coincidence logic contained in the RPS protective channel A RTR controls breaker A in the Control Rod Drive (CRD) System as shown in Figure 7-1. Protective Channels B, C, and D will control breakers B, C, and D respectively in the Control Rod Drive System. Breakers A and C are placed in series in one parallel path and breakers B and D are in series in the other parallel path. All 600VAC 3-phase power to the rod drives is via these parallel paths. Combinations that could initiate a trip, in Boolean logic terms, are AB + AD + BC + CD (+ meaning logic "or"). This is 1-out-of-2 logic taken twice and is referred to as (1-out-of-2) x 2 logic. It should be noted that when any two out of four RPS protective channels trip, all RTRs trip, commanding all CRD trip breakers to open.

Independence is maintained in the four protective channels which are interconnected via fiber-optic data links. These links provide the means to exchange data, which is used for signal validation, fault and deviation detection, and trip actuation. This provides additional fault detection. If interchannel communications are lost, the associated signals are faulted as well. Faulted signals are eliminated from use in the signal selection logic. With only the hardwired signal as valid, the signal is passed directly to the subsequent logic, thus ensuring protective channel independence. The second maximum (2.MAX) and second minimum (2.MIN) signal selection functions are used for analog inputs, and 2-out-of-4 selection logic is used for contact inputs. The 2.MAX and 2.MIN functions remain until less than two valid signals are present. The 2-out-of-4 logic function reduces to a 2-out-of-3 logic for any condition that causes an input signal fault, including loss of power.

Three of the four RPS channel computers (A, B, and C) also perform a redundant ESPS logic function (Section 7.3.2). Therefore, three of the four RPS protective channel computers calculate both RPS and ESPS functions. RPS protective channel D calculates only RPS functions.

The undervoltage coils of the control rod drive breakers receive their power from the protective channel associated with each breaker. The manual reactor trip switch is interposed in series between each breaker's RTR logic and the assigned breakers undervoltage coil.

In response to NRC Generic Letter 83-28 automatic actuation of the AC breaker shunt trip attachments for the Reactor Trip System and Manual Trip Actuation have been installed. This upgrade improves the reactor trip breaker reliability.

For the reactor trip breakers in each channel a relay is installed with its operating coil in parallel with the existing undervoltage device. The output contacts of these relays control the power to the shunt trip devices. Thus, when power is removed from the breaker undervoltage trip attachment on either a manual or automatic trip signal, the shunt trip attachment is energized to provide an additional means to trip the breaker. Test switches are installed to permit independent testing of the shunt and undervoltage trip devices. Loss of shunt trip control power is annunciated in the control room indicating that the shunt trip device is not operable.

7.2.2.2 Summary of Protective Functions

The four Reactor Protective System protective channels are identical in their functions, which combine in the system logic to trip the reactor automatically and protect the reactor core for the following conditions:

1. When the reactor power, as measured by neutron flux, exceeds a fixed maximum limit.
2. When the reactor power, as measured by neutron flux, exceeds the limit set by the reactor coolant flow and power imbalance.
3. When the reactor power exceeds the limit set by the number and combination of reactor coolant pumps in operation.

4. When the reactor outlet temperature exceeds a fixed maximum limit.
5. When a specified reactor pressure-outlet temperature relationship is exceeded.
6. When the reactor pressure falls below a fixed minimum limit.
7. When Reactor Building pressure exceeds a fixed maximum limit.
8. The RPS automatically trips the reactor to protect the Reactor Coolant System whenever the reactor pressure exceeds a fixed maximum limit.
9. The RPS automatically trips the reactor upon main turbine trip or trip of both main feedwater pumps.

The abnormal conditions that initiate a reactor trip are keyed to the above listing and tabulated in Table 7-1.

7.2.2.3 Description of Protective Channel Functions

The functions of the RPS described below apply to each protective channel. Reference Figure 7-1 for Control Logic.

7.2.2.3.1 Over Power Trip

Deleted per 2013 Update.

The nuclear instrumentation provides a linear neutron flux signal in the power range to the four protective channels. The protective channel signals are then compared and when the 2.MAX neutron flux signal exceeds the trip setpoint in two or more protective channels, a reactor trip is generated. Reference Trip #1 of Figure 7-1 for control logic.

7.2.2.3.2 Nuclear Over Power Trip Based on Flow and Imbalance

Deleted per 2013 Update.

Neutron flux and the reactor coolant flow are continuously monitored. Upper and Lower flux signals are received from the nuclear instrumentation and a total flux and a delta flux reading is calculated by each RPS protective channel. Total reactor coolant flow is calculated by each RPS protective channel from the differential pressure reading for each loop. A power level trip setpoint is established for each RPS protective channel based on the percentage reactor coolant flow rate multiplied by the flux to flow ratio and limited by the maximum allowed thermal power (Pmax). The value of Pmax is established to prevent exceeding the limits established by the COLR in the event that indicated reactor coolant flow increases due to instrument failure. The delta flux or imbalance (power in the top half of the core minus the power in the bottom half of the core) reduces the power level trip setpoint such that the four pump power-imbalance boundaries illustrated in Figure 7-3 are not exceeded. Less than four pump power-imbalance protection is provided by the power level trip setpoint decrease due to flow decrease. When the 2.MAX neutron flux signal exceeds the power level trip setpoints established by the total reactor coolant flow and the reactor power imbalance in two or more protective channels, a reactor trip is generated. Reference Trip #3 of Figure 7-1 for control logic.

All flow ΔP cells for a single loop are connected to common 1-inch "low" and "high" lines from the flow tube in that loop. Severance of the "low" line will result in maximum indicated flow for the loop in all four protective channels. All console indicators for the loop will go to 110 percent full flow. Severance of the "high" line will result in zero indicated flow for the loop and possibly a power/flow reactor trip. See Section 7.4.2.3.1 for more details.

7.2.2.3.3 Power/Reactor Coolant Pumps Trip

The reactor coolant (RC) pumps are monitored to determine that they are running. Loss of a single pump initiates four independent signals, one to each protective channel. This information is received by a pump monitor logic which counts the number of RC pumps in operation and identifies the coolant loop in which the pumps are operating. The inputs from the RC Pump monitors are processed by each RPS protective channel and a trip is generated for the conditions in Table 7-1. Reference Trip #11 of Figure 7-1 for control logic.

7.2.2.3.4 Reactor Outlet Temperature Trip

The reactor outlet temperature is measured by resistance elements.

One of the four reactor outlet temperatures is designated for each protective channel. When the 2.MAX RTD input exceeds the predetermined setpoint, the associated protective function is automatically placed in its tripped state. When the 2.MAX reactor outlet temperature exceeds the trip setpoint in two or more protective channels, a reactor trip is generated. Reference Trip #7 of Figure 7-1 for control logic.

Deleted per 2013 Update.

7.2.2.3.5 Pressure-Temperature Trip

Figure 7-2 shows typical operating reactor coolant pressure-temperature boundaries formed by the combined reactor high temperature, high pressure, low pressure, and the pressure-temperature comparator trip settings.

When reactor coolant 2.MAX or 2.MIN pressure or temperature exceeds these boundaries, a trip signal is generated within the protective channel. If two or more protective channels reach the trip condition, a reactor trip signal is generated. Reference Trip #6 of Figure 7-1 for control logic.

7.2.2.3.6 Reactor Coolant Pressure Trip

The reactor coolant system pressure is measured by four independent pressure transmitters, one pressure input to each RPS protective channel. When the 2.MAX or 2.MIN pressure input exceeds its setpoint (high or low), the associated protective function is automatically placed in its tripped state. When the 2.MAX or 2.MIN reactor coolant pressure exceeds the trip setpoints in two or more protective channels, a reactor trip is generated. Reference Trips #4 and #5 of Figure 7-1 for control logic.

Deleted per 2013 Update.

7.2.2.3.7 Main Turbine Trip

Pressure switches monitoring the hydraulic fluid pressure in the Turbine Emergency Trip System header will input an open indication to the RPS on turbine trip.

Each RPS protective channel A, B, C & D monitors one of four hydraulic fluid pressure switch contact inputs. The status of these four contact inputs is shared between protective channels over fiber optic communications links. If the reactor trip function is enabled and 2-out-of-4 Main Turbine hydraulic fluid pressure switch contacts are open, then that RPS protective channel produces a trip signal. If two or more RPS protective channels are in the tripped state, a reactor trip is generated via the 2-out-of-4 reactor trip relay logic. Reference Trip #10 of Figure 7-1 for control logic. This trip is bypassed below a predetermined flux level for unit startup.

7.2.2.3.8 Loss of Main Feedwater Trip

Hydraulic oil pressure switches for each feedwater pump turbine will input an open indication to the RPS on feedwater pump turbine trip.

Each RPS protective channel A, B, C & D monitors both feedwater pump turbines hydraulic oil pressure switch contact inputs. The status of these eight contact inputs is shared between protective channels over fiber optic communication links. If the reactor trip function is enabled and both feedwater pump turbines are tripped, then that RPS protective channel produces a trip signal. If two or more RPS protective channels are in the tripped state, a reactor trip is generated via the 2-out-of-4 reactor trip relay logic. Reference Trip #9 of Figure 7-1 for control logic. This trip is bypassed below a predetermined flux level for unit startup.

7.2.2.3.9 Reactor Building Pressure Trip

Each of the four protective channels receives Reactor Building pressure information from an independent pressure switch.

A 2-out-of-4 logic scheme is used within each RPS Protective Channel. The 2-out-of-4 logic within each RPS protective channel looks for a second open contact from the pressure switches to initiate a protective channel trip. This logic eliminates a single failure from tripping an RPS protective channel and will only provide a reactor trip when there is valid Reactor Building High Pressure (2-out-of-4). A single open contact will be annunciated via the respective protective channel's Trouble Statalarm and via the OAC computer. Reference Trip #8 of Figure 7-1 for control logic.

7.2.2.4 Setpoint Adjustments for Single Loop Operation

Following amendments 165/165/162 to the facility operating license, single loop power operation is prohibited.

7.2.2.5 Availability of Information

The reactor trip components associated with a single protective channel are wholly contained within two RPS cabinets.

Deleted per 2013 Update.

All system analog and binary input signals are monitored by the plant computer. Separate from the computer, equipment failures and trip actions are sequence-annunciated in the plant status annunciator. Such sequencing permits the operator to readily identify the protective channel trip actions. Process information including power, imbalance, flow, temperature, and pressure is also available on the main control console.

Plant annunciator windows provide the operator with immediate indications of changes in the status of the RPS. The following conditions are annunciated for each RPS protective channel:

1. channel trip
2. channel trouble
3. channel on test
4. NI power supply failure
5. shutdown bypass initiated
6. manual bypass initiated

Any time a test switch is in other than the operate position, a test annunciator will be lit and the associated protective channel must be administratively declared out of service.

The RPS system communicates with the plant OAC and annunciators through the Monitoring and Service Interface (MSI). The MSI has three communication functions which are to: provide unidirectional data to the OAC, provide bidirectional data to the Service Unit, and provide isolated communication between the safety related RPS and the non-safety plant systems such as annunciators and the ICS. The Graphical Service Monitor (GSM) resides on the Service Unit and provides an interface into the RPS for testing and maintenance. The OAC is sent unidirectional data through a gateway which provides real time information to the OAC. Reference Figure 7-1, pg 16 for a diagram of the MSI interface.

Deleted per 2013 Update.

7.2.3 System Evaluation

7.2.3.1 System Logic

The RPS is a four-channel, redundant system in which the four protective channels are brought together in four identical 2-out-of-4 logic networks of the reactor trip components. The Reactor Trip Component (RTC) is made up of two digital output modules and four Reactor Trip Relays (RTR) all contained within the respective RPS channel's cabinet. The RTC receives a channel trip signal in its own channel and channel trip signals from the digital output modules in the other three RPS channels. A trip in any 2 of the 4 protective channels initiates a trip of all four logic networks. The system to this point has the reliability and advantages of a pure 2-out-of-4 system.

Each of the reactor trip components (2-out-of-4 logic networks) controls a control rod drive breaker. A trip in any 2 of the 4 protective channels initiates a trip of all the breakers. The breakers are arranged in what is effectively a 1-out-of-2 logic taken twice (Figure 7-4). This system combines the advantages of the 2-out-of-4 and the 1-out-of-2 x 2 systems. The combination results in a system that is considered superior to either of the basic systems alone.

In evaluating system performance, it is arbitrarily assumed that "failure" can either prevent a trip from occurring or can initiate trip action.

The redundant Reactor Protective System inputs operate in a true 2-out-of-4 logic mode so that the failure of an input leaves the system in either a 2-out-of-3 or a 1-out-of-3 logic mode, with either state providing sufficient redundancy for reliable performance.

The system can tolerate several input function failures without a reduction in performance capability provided the failures occur in unlike variables in different protective channels, or are of a different mode in different protective channels, or all occur within one protective channel. When a single protective channel fails, the system is left in either a 2-out-of-3 or 1-out-of-3 logic mode as explained below.

The protective channel trip relay of each channel is located in the reactor trip component associated with the channel. Within each reactor trip component, there is a logic relay for each protective channel. These combine in each reactor trip component to form the 2-out-of-4 logic. A Failure Mode and Effects analysis of the reactor trip component has demonstrated that single failures within the reactor trip component or interconnections can produce only the following effects:

1. Trip the breaker associated with the reactor trip component.
2. Place the system in a 2-out-of-3 mode, as if the associated protective channel had a "cannot" trip failure.
3. Place the system in a 1-out-of-3 mode, as if the associated protective channel had tripped.

The combination of reactor trip components and control rod drive breakers form a 1-out-of-2 x 2 logic. At this level the system will tolerate a "cannot trip" type of failure of one reactor trip component, or of the breaker associated with one reactor trip component without degrading the system's ability to trip all

control rods. The failure analysis demonstrates that no single failure involving a reactor trip component will prevent its associated breakers from opening.

7.2.3.2 Redundancy

The design redundancy of the Reactor Protective System allows the loss of a single protective channel. If that protective channel is in the Trip state, the remaining components and protective channels are operational in a 1-out-of-3 system logic. If that protective channel is in Manual Bypass, the remaining components and protective channels are operational in a 2-out-of-3 system logic.

7.2.3.3 Electrical Isolation

Deleted per 2013 Update.

Electrical isolation is inherent in the use of fiber-optic data links. In order to maintain electrical independence when input signals are shared between channels, a TXS communication link module is used to convert the signal from hard wire to fiber optic. The fiber optic communication equipment is qualified as Class 1E isolation and provides the required electrical separation between each protective channel. Fiber optic communication equipment is also used between protective channels and the Monitoring and Service Interface (MSI). Fiber optic isolation prevents internal electrical faults from propagating from one protective channel to other redundant channels.

All signals leaving the RPS to non-qualified systems (such as ICS) utilize qualified signal isolators to protect against faults occurring external to RPS.

Each input/output interface type was tested in both differential (across input/output) and common (input/output to ground) modes. Fault signals of 600 VAC and 250 VDC were applied for 30 seconds. This testing verified the RPS operation was not affected by the simulated faults.

7.2.3.4 Periodic Testing and Reliability

Deleted per 2013 Update.

The use of 2-out-of-4 logic between protective channels permits a channel to be tested online without initiating a reactor trip. Test circuits are supplied which utilize the redundant, independent, and coincidence features of the Protective Systems. This makes it possible to manually initiate online trip signals in any single protective channel in order to test trip capability in that channel without affecting the other protective channels. Surveillance requirements have been established for performance of protective channel calibrations and protective channel functional testing.

The RPS provides continual online automatic monitoring of each of the input signals in each channel, performs a signal online validation, and provides functional validation of hardware performance. The RPS has a Graphical Service Monitor (GSM) which supplies individual screens for monitoring and recording the analog and binary inputs during Protective Channel Calibration tests. To prevent adverse system actions, the analog or binary signals may be placed in Bypass using the GSM Trip/Bypass screens. There are also screens to exercise the reactor trip logic, statalarms, and events recorder. Each protective channel is provided with a key-operated Parameter Change Enable keyswitch. The system software controls access to the computer from each protective channel by controlling the operating modes of the computer. Under normal operating conditions, the computer is in the OPERATION mode. The PARAMETERIZATION Mode allows changes to specific parameters or performance of tests from the GSM screens. Permission to change from the OPERATION mode into the PARAMETERIZATION mode is provided by the Parameter Change Enable Keyswitch. After the permissive is provided from a system processor via its Keyswitch, communication from the Service Unit to that processor is allowed to change its operating mode. Placing the PROCESSOR into the FUNCTION TEST and DIAGNOSTIC

modes requires first enabling the PARAMETERIZATION Mode with the keyswitch and then setting a separate parameter to enable these modes with the GSM. The FUNCTION TEST Mode allows disabling the application function and forcing the output signals (normally not used). The DIAGNOSTIC Mode allows download of new application software. The FUNCTION TEST and DIAGNOSTIC modes result in the processor ceasing its cyclic processing of the application functions. The Parameter Change Enable Keyswitches are administratively controlled (no hardware or software interlocks are provided). When a keyswitch is placed in the Parameter Change Enable Mode Position for any activity, the affected processor shall first be declared out of service. In addition to declaring the processor out of service (1) the affected RPS channel shall be bypassed and (2) either the affected ESPS input channel (A1, B1, or C1) shall be tripped OR the ESPS Set 1 voters shall be placed in Bypass for the following activities:

- Loading or revising the software in a processor.
- Changing parameters via the RPS High Flux Trip (Variable Setpoint) screen at the Service Unit.
- Changing parameters via the RPS Flux/Flow/Imbalance Parameters screen at the Service Unit.

Only one RPS channel at a time is allowed to be placed into Parameter Change Enable Mode Position for these activities. Parameter Change Enable Keyswitch status information is sent to a statalarm and is also sent to the OAC via the gateway.

The test scheme for the Reactor Protective System is based upon the use of comparative measurements between like variables in the four protective channels. Trip action is taken when the 2.MAX or 2.MIN value for analog signals or two out of four for binary inputs, based on the trip being tested, exceeds the actual protective function trip points. The alarms for the trip function for the channel under test will actuate when the trip condition for that channel's input is met.

The reliability of the system has been made very high so as to eliminate the need for frequent tests of the logic. The system software is not susceptible to transient, random, aging, or environmental related faults since it does not fail in the conventional sense. It can be reasonably expected to exhibit no degradation from these factors. The cyclic self-monitoring routine verifies that the code is not corrupted. The Mean Time Between Failure (MTBF) data for the Teleperm XS equipment calculates MTBF rates from 29 years to 267 years at 40°C (Reference 6).

All RPS protective channels, logic, and control rod drive power breakers are tested to demonstrate operability. Protective Channel Functional Testing, which is part of the Channel Calibration, is performed every refueling outage. The RPS software performs a continuous online automated cross Channel Check, separately for each protective channel, and continuous online signal error detection and validation. The combination of the self-testing features and the reliability of the TXS equipment support a protective channel functional test frequency of refueling outage. The setpoints in the software are manually verified every 92 days. The protective channel interposing relays are manually actuated every 92 days. RPS logic is re-verified every refueling outage by rebooting the channel computer and checksums are verified at that time.

The control rod drive breaker associated with a reactor trip component is tested prior to startup from a refueling outage and monthly during the fuel cycle.

In addition, power range protective channel readings are compared with a thermal calculation of reactor power. This check, the Channel Checks, and the continuous online self-monitoring of the system are designed to detect the majority of failures that might occur in the analog portions of the system as well as the self-annunciating type of failure in the digital portions of the system.

The periodic electrical tests are designed to detect more subtle failures that are not self-evident or self-annunciating and are detectable only by testing.

7.2.3.5 Physical Isolation

The need for physical isolation has been met in the physical arrangement of the protective channels within separate cabinets and wiring within the cabinets separating power and signal wiring so as to reduce the possibility of some physical event impairing system functions. The systems sensors are separated from each other. There are four pressure taps for the reactor coolant pressure measurements to reduce the likelihood of a single event affecting more than one sensor. Outside the Reactor Protective System cabinets, vital signals and wiring are separated and physically protected to preserve protective channel independence and maintain system redundancy against physical hazards.

Redundant detectors and transmitter applied in the Reactor Protective System are located to provide physical separation. Redundant out of core nuclear detectors are located in separate quadrants around the reactor vessels. Two resistance thermometers assigned to the RPS are located on each reactor coolant outlet header. Cables approach redundant temperature detectors from opposite directions. Redundant pressure transmitters are located outside the secondary shield in four separate quadrants of the Reactor Buildings. Two reactor coolant pressure transmitters for RPS are connected to each of the two loops. Separate flow transmitters for each RPS channel are applied to sense the flow in each loop. This arrangement results in detectors and transmitters associated with one RPS channel being located in essentially (the reactor vessels are not in the center of the Reactor Buildings) the same quadrant of a Reactor Building, and with redundant detectors and transmitters located in another quadrant of the Reactor Building. Since each RPS channel receives a flow signal from both loops, one of the flow transmitters for each channel is not located with the other RPS transmitters for that channel. Location and cable routing for these transmitters is such that separation of at least seven feet is provided between redundant channels inside the Reactor Buildings. Cables for redundant RPS and ES detectors and transmitters are routed in separate directions to four separate Reactor Building penetrations in trays carrying only nuclear instrumentation, RPS, ES, and accident monitoring instrumentation. These penetration assemblies are assigned to nuclear instrumentation, ES instrumentation, accident monitoring instrumentation, and RPS cables exclusively. Two of these penetration assemblies are located sixty feet apart in separate quadrants of each Reactor Building. One is used for RPS and ES channel A instrumentation; the other for RPS and ES channel B instrumentation. A penetration assembly for RPS and ES channel C instrumentation and one for RPS channel D are located on the opposite side of the Reactor Buildings thirty feet apart. Located under the control rooms between the outside of the Reactor Buildings and the cable and equipment rooms, four separate trays are provided per unit which carry nuclear, RPS, ES, and accident monitoring instrumentation cables. Three separate routes are followed by these trays. RPS channel C and RPS channel D follow the same route but are separated vertically by 1-1/2 feet. A detailed review of cable tray and pipe routing in this area indicates that no more than two RPS channels could be damaged by a single pipe failure or missile. Equipment locations in the Auxiliary Building provide the basis for vertical arrangement of trays following the same route from the Reactor Buildings. Switchgear for power equipment is located at lower elevations and instrumentation cabinets are located at higher elevations. Therefore, vertical separation of classes of cables in trays is as follows from top trays down:

1. Instrumentation cable trays
2. Control cable trays
3. Power and control cable trays
4. Power cable trays

Cables from each protective channel are routed in trays separate from those carrying cables from any other protective channel with the exception of fiber optic cables used for interchannel communication. Included in these trays are instrumentation cables from the Reactor Building, control and interconnecting cables associated with that protective channel, and non-protective instrumentation and control cables.

Both protective and non-protective cables are individually armored, with the exception of fiber optic cables, and are flame retardant.

Reactor trip cables from the four RPS cabinets are routed separately to a reactor trip switch located on the main control board. From the trip switch, the cables follow four separate paths to the reactor trip breakers and the control rod drive cabinets.

Where overfill situations exist in the Unit 1, 2, and 3 Cable Rooms, and dedicated trays cannot be provided for individual channels, trays are allowed to carry protective and non-protective mutually redundant cable provided separation is maintained by distance (minimum of five inch air gap) or by barriers the continuous length where the cables are adjacent in the tray.

7.2.3.6 Primary Power

The primary source of 120V ac power for the Reactor Protective System comes from four vital buses, one for each protective channel, as described in Section 8.3.2.1.4.

7.2.3.7 Manual Trip

Manual trip may be accomplished from the control console by a trip switch. This trip is independent of the automatic trip system. Power to the control rod drive breakers' undervoltage coils comes from the reactor trip components (digital output modules and Reactor Trip Relays). The manual trip switch contacts are between the reactor trip component output and the breaker undervoltage coils. Opening of the switch contacts opens the lines to the breakers' undervoltage coils, tripping them. There is a separate set of switch contacts in series with the output of each reactor trip component. All switch contacts are actuated through a mechanical linkage from a single pushbutton.

7.2.3.8 Bypassing

Deleted per 2013 Update.

Each protective channel is provided with two key-operated bypass switches: Shutdown Bypass and Manual Bypass keyswitches. Software bypasses are available for the protective channels and individual input signals within a protective channel. These can be set via the Graphical Service Monitor (GSM) and the Change Enable keyswitch.

The RPS Shutdown Bypass feature allows the following RPS protective functions for a protective channel to be bypassed:

- Low RCS Pressure Trip

Variable Low RCS Pressure (based on RCS Temperature) Trip

- Flux/Flow/Imbalance Trip
- Reactor Coolant Pump/Power Monitor Trips

The RPS Shutdown Bypass function also initiates reductions to setpoints for the following RPS protective functions:

- Nuclear Overpower (High Neutron Flux)
- Reactor Coolant System High Pressure

This function provides the capability to perform control rod drive system testing after the reactor has been shut down and reactor coolant system pressure has been reduced. The RPS Shutdown Bypass keyswitches are administratively controlled (no hardware or software interlocks). All RPS Protective

Channels may be placed in Shutdown Bypass as required. The RPS Shutdown Bypass keyswitch status information is sent to the Statalarm panels. Status information is also sent to the OAC via the Gateway.

The software bypass feature allows the following functions to be bypassed:

- Each of the protective channels as listed above
- Individual protective channels of Neutron Flux Power Range
- Individual protective channels of Reactor Coolant Hot leg Temperature
- Individual protective channels of Reactor Coolant Flow
- Individual protective channels of Reactor Coolant Pressure
- Individual protective channels of Reactor Building Pressure
- Individual protective channels of Main Feedwater Pump Turbine Trip
- Individual protective channels of Main Turbine Trip
- Individual protective channels of Reactor Coolant Pump/Power Monitor Trip

This function allows an individual input which has failed to be bypassed instead of bypassing an RPS channel. The system logic associated with the parameter which has one input bypassed would default to 2 out of 3 coincidence logic while the system logic associated with the remainder of the inputs would still maintain 2 out of 4 coincidence logic.

The Manual Bypass allows putting a complete RPS protective channel into bypass for maintenance activities. This includes the powerdown of the protective channel computer for each protective channel. If the Manual Bypass keyswitch is in the "ON" position, it provides 24V to the relays of the hardwired "2-out-of-4" trip logic in parallel to the output of the computer. This assures that the four output TRIP relays remain energized independent of the status of the TXS computer. It also sets the FAULT status of all input signals prior to sending input signal data to the other protective channels, via the fiber optic communication data links. Thus, during testing with an RPS channel in Manual Bypass, the system will operate in 2-out-of-3 coincidence logic. The Manual Bypass keyswitches are administratively controlled (no hardware or software interlocks are provided). Administrative control allows only one RPS Protective Channel in Manual Bypass at a time. Only one Manual Bypass key is available for each unit. Manual Bypass switch status information is sent to the Control Room Annunciators. Manual Bypass switch status information is also sent to the OAC via the Gateway.

Deleted per 2013 Update.

7.2.3.9 Post Trip Review

Post trip review data and information capabilities are provided by use of time history and sequence of events recording equipment. Time history data is provided by the transient monitoring application of the Process Monitoring Computer system (PMC). Sequence of events is determined by data from the sequence of events recorder (SER), the OAC, and the PMC system. This equipment, along with OAC input and operator interviews, provides sufficient information on plant parameters to assure that the course of the reactor trip can be reconstructed as well as provide root cause determination. In the event of failure of the PMC system, information necessary to conduct a post-trip review or transient investigation can be retrieved from other independent sources, such as the OAC and control room chart recorders. See Reference 1 and Section 7.7.2.

7.2.4 References

1. H. B. Tucker letter to H. R. Denton (NRC), November 4, 1983. Response to Generic Letter 83-28.

2. SER on GL 83-28, Item 1.1, Post Trip Review (Program Description and Procedure), May 15, 1985.
3. H. B. Tucker letter to J. F. Stolz (NRC), February 27, 1986. Response to GL 83-28, Item 1.2, Data and Information Capabilities.
4. SER on GL 83-28, Item 1.2, Post Trip Review (Data and Information Capability), September 11, 1986.
5. 10CFR50.59 USQ Evaluation, dated November 21, 2000, "Duke/ONS Commitment to GL 83-28…".
6. AREVA Document 32-5061241, Oconee Nuclear Station, Unit 1, 2, and 3 RPS/ESFAS TXS Upgrade Availability Analysis (OM 201.N-0028-007)
7. Safety Evaluation Report for RPS/ESPS Digital Upgrade dated January 28, 2010, by the Office of NRR related to Amendment Numbers 366, 368, and 367 to renew Facility Operating Licenses DPR-38, DPR-47, and DPR-55, Oconee Nuclear Station Units 1, 2, and 3 Docket Numbers 50-269, -270,-287

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.2.

7.3 Engineered Safeguards Protective System

Deleted Paragraph(s) per 2009 Update

The Engineered Safeguards Protective System (ESPS) monitors parameters to detect the failure of the Reactor Coolant System and initiates operation of the High and Low Pressure Injection Systems, the Building Isolation, the Reactor Building Cooling and the Reactor Building Spray Systems. In addition, the signal is used to start the standby power source and initiate a transfer to the standby power source when required as described in Section 8.3.1.1.3.

7.3.1 Design Bases

The design basis of the system includes the items of Section 7.1.2 with the following additions:

7.3.1.1 Loss of Power

Deleted per 2013 Update.

1. The loss of vital bus power to an ESPS protective channel will not cause an automatic trip.
2. A loss of power to an input module of an input channel results in the associated signals being faulted.
3. The ESPS voters require power to energize the associated protective relays therefore loss of power to either the ODD or EVEN voter cabinets would result in the inability to automatically actuate the associated ESPS ODD or EVEN train.

Deleted per 2013 Update.

7.3.1.2 Equipment Removal

Deleted per 2013 Update.

1. Removal of an output card or computer card from the digital ESPS will result in an alarm but will not automatically initiate a protective channel trip.
2. Removal of a module in an ESPS protective channel while online does not inhibit the overall system functional design performance in other channels and will not initiate a system actuation.

Deleted per 2013 Update.

7.3.1.3 Control Logic of ESF Systems

All systems receiving the ES signal remain in the emergency mode required by the ES actuation after the signal is reset. A separate deliberate action is required to shut off the ES systems and power supplies.

The following systems have been modified to conform to the above requirement of I.E. Bulletin 80-06:

1. HPI Pumps
2. Penetration room exhaust fans
3. Reactor Building Cooling Unit fans
4. Keowee Start

7.3.2 System Design

7.3.2.1 System Logic

Deleted per 2013 Update.

The ESPS is a protective system which employs 2-out-of-3 coincidence logic to actuate engineered safeguards functions in the event that Reactor Coolant System pressure or reactor building pressure setpoints are exceeded. The functions include signal acquisition, data-processing, and actuation signal voting. The ESPS processes both analog and contact signals from the field for input into the ESPS instrument input channels. The input processors perform software logic and parameter checks on the analog and contact input signals and provide software logic outputs to the other ESPS instrument input channels as well as to the actuation logic channels. Each input variable is measured by three process sensors; the three redundant signals are processed within the input channel and voter processors, which provide an ESPS channel actuation through a set of output Ro relays (Ro1 and Ro2). The eight actuation logic channels are split between ODD and EVEN voters as shown in Figure 7-5, pg. 2. Either of the two voters is independently capable of initiating the required protective action through redundant equipment. The 2.MAX or 2.MIN (depending on the analog trip) is selected to compare to the trip setpoint. For binary inputs a 2 out of 3 trip logic is used to actuate the trip.

The ESPS processes both analog and contact signals from the field for input into the three ESPS instrument input channels. These three input channels are shared by 2 redundant ESPS Subsystems. Subsystem 2 operates in the ESPS cabinets and is designated as A2, B2 and C2. Subsystem 1 is designated as A1, B1 and C1 and operates in the Reactor Protective System (RPS) channel cabinets A, B, and C. Each of the ESPS and RPS processors performs software logic and parameter checks on the same analog and contact input signals and provides software logic outputs to the other instrument input channels as well as to the ESPS voter subsystems.

The ESPS subsystems are interconnected via fiber-optic data links. This provides a means to exchange data between subsystem inputs , which are used for signal validation, fault and deviation detection, and trip actuation. Alarms are initiated when signals fail validation tests or when failures or abnormal deviations are detected. Analog signals are faulted when extremely low signals (significantly below off-scale) are detected, indicating transmitter failure or power supply failure. If inter-channel communications are lost, the associated signals are faulted as well. Faulted signals are eliminated from use in the signal selection logic. An additional level of reliability is provided through the utilization of second maximum (2.MAX) and second minimum (2.MIN) signal selection functions for analog inputs and 2-out-of-3 selection logic for contact inputs. These functions reduce the probability of using an erroneous signal for determining trip conditions.

Independence is maintained in the subsystem inputs which are interconnected via fiber-optic data links. If interchannel communications are lost, the associated signals are faulted as well. Faulted signals are eliminated from use in the signal selection logic. With only the hardwired signal as valid, the signal is passed directly to the subsequent logic, thus ensuring instrument input channel independence. The 2.MAX and 2.MIN signal selection functions are used for analog inputs, and 2-out-of-3 selection logic is used for contact inputs. The 2.MAX and 2.MIN functions remain until less than two valid signals are present. The 2-out-of-3 logic function reduces to a 2-out-of-2 logic for any condition that causes an input signal fault, including loss of power.

The ODD/EVEN voter designation is associated with redundant actuation devices. The ODD1 and ODD2 voters provide output to ESPS actuation logic channels 1, 3, 5 and 7. The EVEN1 and EVEN2 voters provide output to ESPS actuation logic channels 2, 4, 6 and 8. There is an ODD/EVEN subsystem 1 and an ODD/EVEN subsystem 2, which correspond to the ESPS instrument input channels which provide signals to them. Voters ODD1 and EVEN1 receive input from ESPS instrument input channels

A1, B1 and C1. Voters ODD2 and EVEN2 receive input from ESPS instrument input channels A2, B2 and C2. Either voter subsystem is capable of performing all required protective actions.

The instrument input channel trip signals are provided to the voters via fiber-optic data links. The voters use 2-out-of-3 logic on these trip signals for actuating the Ro relays.

The logic reduces to 2-out-of-2 for any condition that causes an input signal fault, including loss of power.

In addition, each voter (ODD1, EVEN1, ODD2 and EVEN2) is made up of a master and a checker processor, or 8 processors total. Each processor utilizes the same input information and executes the same software in performing an independent 2-out-of-3 logic for actuating the Ro relays (Ro1 and Ro2). At the end of each processing cycle, prior to sending output commands to redundant digital output boards that energize separate Ro relays, the master and checker processors compare results. If a calculation mismatch occurs between the Master and Checker processors, the respective subsystem automatically disables all of its output modules by shutting down the power supply to the output modules, generates an alarm, and initiates a reboot of the voter subsystem. This reduces the possibilities for inadvertently actuating the output Ro relays and subsequently energizing the Engineered Safeguards equipment when not required. Contacts from Ro1 and Ro2 are wired in series to prevent spurious actuation due to digital output board failure. Reference Figure 7-5 for trip logic diagrams.

The output Ro relays are normally de-energized. The contacts of the Ro relays are normally open within the control circuits of the individual Engineered Safeguards equipment. An ESPS actuation energizes the Ro relays and closes the Ro contacts which in turn energizes the control relays (CR) in each of the protective device (valve, pump, etc.) control circuits.

Deleted per 2013 Update.

7.3.2.2 High and Low Pressure Injection and Reactor Building Non-Essential Isolation Systems

There are three independent reactor coolant pressure sensors and three independent reactor building pressure sensors which provide input to the ESPS. Reactor coolant pressure and the reactor building pressure inputs are monitored by two independent signal processing subsystems. The non-faulted inputs are combined within the ESPS into 2-out-of-3 coincidence logic for initiating High Pressure Injection (HPI) system, Low Pressure Injection (LPI) system and Reactor Building Non-Essential Isolation actions. System Logic for ESPS is described in Section 7.3.2.1 and is shown in Trips #1 and #2 of Figure 7-5.

The instrumentation, logic, and actuation of the High Pressure Injection (HPI) and Low Pressure Injection (LPI) Systems are identical in design. The systems differ only in their actuation setpoints.

During reactor operation, HPI and the Reactor Building Non-Essential Isolation will initiate if 2-out-of-3 of the reactor coolant pressure sensors indicate a decrease in pressure below the RCS Low pressure setpoint, or if 2-out-of-3 reactor building pressure sensors indicate an increase in pressure beyond setpoint. These ESPS functions start Keowee Hydro Units, provide permissives for emergency power, start the HPI pumps and align various valves. Two ESPS actuation output logic channels are initiated either of which is independently capable of initiating the required protective action.

During reactor operation, LPI and the Low Pressure Service Water System (LPSW) will initiate if 2-out-of-3 of the reactor coolant pressure sensors indicate a decrease in pressure below the RCS Low-Low pressure setpoint, or if 2-out-of-3 reactor building pressure sensors indicate an increase in pressure beyond setpoint. These ESPS functions initiate LPI and LPSW pumps and align various valves. Two ESPS actuation output logic channels are initiated either of which is independently capable of initiating the required protective action.

Deleted per 2013 Update.

7.3.2.3 Reactor Building Cooling and Reactor Building Essential Isolation System

There are three independent reactor building pressure sensors which provide input to the ESPS. Reference Trip #3 of Figure 7-5 for trip logic diagram.

The non-faulted inputs are combined within the ESPS into a 2-out-of-3 coincidence logic for initiating Reactor Building Cooling (RBC) and Reactor Building Essential Isolation System actions. System Logic for ESPS is described above in Section 7.3.2.1.

RBC and the Reactor Building Essential Isolation System will initiate if 2-out-of-3 of the reactor building pressure sensors indicate an increase in building pressure above the high building pressure ESPS trip point. The second maximum of the sensor inputs is selected to compare to the trip setpoint. The three reactor building pressure inputs to ESPS are also utilized for HPI and LPI System initiations as previously discussed in Section 7.3.2.2. Two ESPS actuation output logic channels are initiated either of which is independently capable of initiating the required protective action.

This ESPS function starts RBC unit fans and penetration room fans as well as aligns certain component cooling water and LPSW valves when reactor building pressure increases above the ESPS setpoint. The Channel A Reactor Building Isolation signal is sent to the ICS to denote degraded containment conditions. The ICS is configured such that this signal is not utilized to initiate any action within the ICS.

Deleted per 2013 Update.

7.3.2.4 Reactor Building Spray System

Reactor building pressure switch inputs are monitored by 6 pressure switches. Two sets of three switches feed two independent digital processing input channels. The non-faulted inputs are combined within the ESPS into 2-out-of-3 coincidence logic for initiating Reactor Building Spray (RBS) actions. System Logic for ESPS is described above in Section 7.3.2.1 and is shown in Trip #4 of Figure 7-5 for the trip logic diagram.

RBS will initiate if 2-out-of-3 of the reactor building pressure switches indicate an increase in building pressure above the High High building pressure ESPS trip setpoint. Two ESPS actuation output logic channels are initiated either of which is independently capable of initiating the required protective action.

This ESPS function starts RBS pumps and aligns the RBS valves required for system operation.

Deleted per 2013 Update.

7.3.2.5 Availability of Information

All system signals are monitored by the plant computer. ESPS device position status is indicated on the ES Status panels and also is monitored by the plant computer. Statalarm panel alarms provide the following ESPS conditions:

- HPI and LPI bypass permit,
- Input channel bypass for HPI and LPI,
- Input channel trip,
- Input channel trouble,
- Input channel in test,
- Manual bypass for each of voters ODD1, ODD2, EVEN1 and EVEN2,
- EVEN and ODD voter trouble,
- EVEN and ODD voter in test,

- EVEN and ODD voter in emergency override,
- Actuation output logic channel trip,

The ESPS provides automatic analog and binary process signal monitoring for signal failure (Fault) and for Channel Deviation, which are alarmed via the trouble alarms. If an instrument input channel fails the acceptance criteria, it is alarmed (OAC alarms & Statalarm windows) so that the Control Room Operator can take appropriate action. This feature allows automation of the channel check surveillance.

The ESPS system communicates with the plant through the Monitoring and Service Interface (MSI). The MSI has three communication functions which are to: provide unidirectional data to the OAC, provide bidirectional data to the Service Unit, and provide isolated communication between the safety related ESPS and the nonsafety plant systems such as annunciators and the ICS. The Graphical Service Monitor (GSM) resides on the Service Unit and provides an interface into the ESPS for testing and maintenance. The OAC is sent unidirectional data through a gateway which provides real time information to the OAC. Reference Figure 7-1 for a diagram of the MSI.

Any time a test switch is in other than the operate position, a test annunciator will be lit and the associated protective channel must be administratively declared out of service.

Deleted per 2013 Update.

7.3.2.6 Summary of Protective Action

Actions initiated by the Engineered Safeguards Protection System are tabulated in Table 7-2. The devices actuated by the Engineered Safeguards Protection System are listed in Table 7-3. Channels indicated may be referred to applicable systems as shown in Figure 7-5. All actuated devices remain in their emergency modes after the reset of an engineered safeguards actuation signal until the devices are reset by operator action.

7.3.3 System Evaluation

The ESPS is a basic three-channel redundant system employing 2-out-of-3 coincidence between measured variables.

The system will tolerate the failure of one of three variables among either the reactor coolant pressure measurements or Reactor Building pressure measurements without losing its ability to perform its intended functions.

The High and Low Pressure Injection and Reactor Building Non-Essential Isolation Systems are actuated by either reactor coolant pressure or Reactor Building pressure, thus providing diversity in actuation. The system will tolerate single or multiple failures within one protective channel without affecting the operation of other protective channels. This is the result of keeping each of the protective channel logics independent of every other protective channel. The independence is carried through the protective channel logic and up to the final actuating CR control relay. This is best illustrated by considering the actuation arrangement for the high pressure injection pumps (Figure 7-5).

There are three High Pressure Injection System pumps which operate in the event of an accident. HP-P1A is under the control of protective channel 1, HP-P1C is under the control of protective channel 2, while HP-P1B is under the control of both channels. There is a single CR control relay controlled by the Ro relays within the motor control logic for HP-PlA and HP-PlC. Should any two of the three reactor coolant pressure variables drop below the RCS Low Pressure set point, both protective channel 1 and 2 logics will trip, energizing the appropriate CR relays, and start the pumps.

Within the motor control logic for HP-P1B there are two independent CR relay strings, each controlled by separate Ro relays from ESPS (the Ro relays in output channel 1 and the Ro relays

in output channel 2). The arrangement is identical to the way a channel would control any device since all elements are independent and duplicated through the CR relay. The only common element is the power source for the CR relays which is common to the motor controller. Loss of this power prevents the motor control from operating as well as the pump. Relays that monitor actuator coils for each motor or valve control detect either an open coil or a loss of control power.

Independence is maintained in the three instrument input channels which are interconnected via fiber-optic data links. These links provide the means to exchange data, which is used for signal validation, fault and deviation detection, and trip actuation; thus providing additional fault detection. If interchannel communications are lost, the associated signals are faulted as well. Faulted signals are eliminated from use in the signal selection logic. The 2.MAX and 2.MIN signal selection functions are used for analog inputs, and 2-out-of-3 selection logic is used for contact inputs. The 2.MAX and 2.MIN functions remain until less than two valid signals are present. When only the hardwired signal is valid, then the 2.MAX and 2.MIN functions directly pass the signal to the subsequent logic. The 2-out-of-3 logic function reduces to a 2-out-of-2 logic for any condition that causes an input signal fault, including loss of power.

The voters maintain their independence in the ESPS. The ODD/EVEN voter designation is associated with redundant actuation devices. The ODD1 and ODD2 voters provide output to ESPS actuation output logic channels 1, 3, 5 and 7. The EVEN1 and EVEN2 voters provide output to ESPS actuation output logic channels 2, 4, 6 and 8. There is an ODD/EVEN subsystem 1 and an ODD/EVEN subsystem 2, which correspond to the ESPS input channels which provide signals to them. Voters ODD1 and EVEN1 receive input from ESPS input channels A1, B1 and C1. Voters ODD2 and EVEN2 receive input from ESPS input channels A2, B2 and C2. Either voter subsystem is capable of performing all required protective actions. The instrument input channel trip signals are provided to the voters via fiber-optic data links. The voters use 2-out-of-3 logic on these input channel trip signals for actuating the output Ro relays. The redundant Ro relays mitigate failure modes of the voter outputs.

An Override switch has been installed on the unit board for the ESPS ODD and EVEN voters which allows operators to override the ESPS system in case of an ESPS actuation caused by a Software Common Mode Failure. Once the override is initiated, operators are able to manually position ESPS components.

The example just presented shows the independence and redundancy of the system. There is redundancy of sensors, logic, and equipment. The redundancy is preserved and kept effective by independence of sensors, instrument strings, logic, and control elements in the final actuator. These characteristics enable the system to tolerate single failures at all levels.

The system protective devices (pumps, valves, etc.) require electrical power in order to operate and perform their functions. The power for operating the CR relays is taken from the power source of the associated device. Loss of power to a CR relay or device does not impair the system functions since there is a second redundant device for each required function. The power for the R_o relays, logic, and instruments is taken from the plant's system of battery backed vital buses since loss of power at this level could affect the performance capability of the system. The system will tolerate the loss of one vital bus without loss of protective capability.

7.3.3.1 Redundancy and Diversity

The system as evaluated above is shown to have sufficient diversity and redundancy to withstand single failures at every level.

7.3.3.2 Electrical Isolation

The use of isolation amplifiers will effectively prevent any faults (shorts, grounds, or cross connection of signals) on any analog signal leaving the system from being reflected into or propagating through the

system. The direct connection of any analog signal to a source of electrical power can, at worst, negate information from the measured variable involved. The use of individual R_o relays for each controlled device effectively preserves the isolation of each device and of elements of one protective channel from another. Faults in the control wiring between an R_o relay and its CR relay in the controller of a protective device will not affect any other device or protective channel action.

Electrical isolation is inherent in the use of fiber-optic data links. In order to maintain electrical independence when input signals are shared between channels, a TXS communication link module is used to convert the signal from hard wire to fiber optic. The fiber optic communication equipment is qualified as Class 1E isolation and provides the required electrical separation between each protective channel. Fiber optic communication equipment is also used between protective channels and the Monitoring and Service Interface (MSI) and between the ESPS input channels and the Voters. Fiber optic isolation prevents internal electrical faults from propagating from one protective channel to other redundant protective channels.

Separation of redundant Engineered Safeguards (ES) functions is accomplished by assigning the eight actuation channels (Table 7-2) to three groups. Isolation for power, control, equipment location, and cable routing is maintained throughout. Channels l, 3, 5 and 7 are assigned to one group (odd actuation channels). Channels 2, 4, 6 and 8 are assigned to a second group (even actuation channels). Equipment which is actuated by both the even and odd actuation channels is assigned to a third group. All equipment required to perform a specific ES function is assigned to the same group. For example, a pump motor and all valves required for that pump to perform its function are assigned to the same group.

For Oconee 1, AC power for equipment controlled by the odd numbered actuation channels is supplied from Switchgear Group 1TC (4KV), motor control center 1XSl, 1XSF, and 1XS4 (600 and 208 volts), actuation power from Vital Power Panelboard 1KVIA and DC control power from DC Panelboard 1DIA. ES functions which are redundant to those controlled by the odd numbered actuation channels are controlled by the even numbered actuation channels. AC power for this equipment in Oconee 1 is supplied from Switchgear Group 1TD (4KV), Motor Control Center 1XS2 and 1XS5 (600 and 208 volts), from Vital Power Panelboard lKVIB, and DC control power from DC Panelboard 1DIB. Where a third unit of ES equipment is used to provide additional redundancy, it is actuated by both the even and odd actuation channels. AC power for this equipment in Oconee l is supplied from Switchgear Groups 1TE or 2TC (4KV), Motor Control Center 1XS3 (600 and 208 volts), actuation power from either Vital Power Panelboard 1KVIA for odd channel actuation or Vital Power Panelboard 1KVIB for even channel actuation, and DC power from DC Panelboard 1DIC. Similar arrangements are employed for ES equipment in Oconee 2 and 3 with different power and control sources for each unit. Motor Control Centers XS4, XS5 and XS6 are complements to Motor Control Centers XS1, XS2 and XS3 respectively. These are described in Section 8.3.

7.3.3.3 Physical Isolation

The arrangement of ESPS components within the system cabinets is designed to reduce the chance of physical events impairing system operation. Control wiring between the ESPS output components and the final actuating devices is physically separated and protected against damage which could impair system operation.

Separation between redundant channels of equipment, control cables, and power cables provides independence of redundant ES functions. The one exception to this separation are the fiber optic cables used for interchannel communication. Power and control cables for each group of ES equipment are routed in cable trays that contain no cable for redundant equipment or meet current separation criteria. Cables for Reactor Building cooling units enter each Reactor Building through three separate penetrations located at least 25 feet apart and are routed in three different directions to the cooling units. The only

other ES equipment located inside the Reactor Buildings are electric motor operated isolation valves which are all common to the odd numbered actuation group discussed above.

7.3.3.4 Periodic Testing and Reliability

The ESPS input processors perform software logic and parameter checks on the analog and contact input signals and provide software logic outputs to the other input channels as well as to the voter output channels. Each input variable is measured by three process sensors. The 2.MAX and 2.MIN signal selection functions are used for analog inputs and 2-out-of-3 selection logic is used for contact inputs. Trip signals from the three input channels are processed within the voter processors which provide an ESPS output channel actuation through a set of Output Ro relays. The use of 2-out-of-3 logic between protective input channels and GO/NOGO (described below) testing of system outputs permits a protective channel to be tested online without initiating an output channel trip. The test circuits take advantage of the system redundancy, independence, and coincidence logic software to make it possible to manually initiate test signals in one protective channel without affecting the other channels. Surveillance requirements have been established for performance of protective channel calibrations and protective channel functional testing.

The ESPS provides continual online automatic monitoring of each of the input signals in each input channel, performs signal online validation, and provides functional validation of hardware performance.

The ESPS has a Graphical Service Monitor (GSM) which supplies individual screens for monitoring and recording the analog and binary inputs during Protective Channel Calibration tests. To prevent adverse system actions while performing these tests, the analog or binary signals under test may be placed in Bypass using the GSM Trip/Bypass screens. There are also screens to exercise the output channel trip logic, statalarms, and events recorder. Each protective channel can be tripped in a GO or NOGO test. A NOGO test will trip half of the output string and provide indication of a successful test on the GSM screen without moving the component. A GO test will trip both halves of the output string and provide indication of a successful test in the GSM and reposition the component to the ESPS position. Each protective channel is provided with a key-operated Parameter Change Enable keyswitch. The system software controls access to the computer from each protective channel by controlling the operating modes of the computer. Under normal operating conditions, the computer is in the OPERATION mode. The PARAMETERIZATION Mode allows changes to specific parameters or performance of tests from the GSM screens. Permission to change from the OPERATION mode into the PARAMETERIZATION mode is provided by the Parameter Change Enable Keyswitch. After the permissive is provided from a system processor via its Keyswitch, communication from the Service Unit to that processor is allowed to change its operating mode. Placing the PROCESSOR into the FUNCTION TEST and DIAGNOSTIC modes requires first enabling the PARAMETERIZATION Mode with the keyswitch and then setting a separate parameter to enable these modes with the GSM. The FUNCTION TEST Mode allows disabling the application function and forcing the output signals (normally not used). The DIAGNOSTIC Mode allows download of new application software. The FUNCTION TEST and DIAGNOSTIC modes result in the processor ceasing its cyclic processing of the application functions. The Parameter Change Enable Keyswitches are administratively controlled (no hardware or software interlocks are provided). When a keyswitch is placed in the Parameter Change Enable Mode Position for any activity, the affected processor shall first be declared out of service. In addition to declaring the processor out of service, when loading or revising software in an input channel processor, the affected ESPS inputs shall be tripped OR the associated ESPS voters shall be placed in Bypass. If this activity is being performed on an ES Input Channel in subsystem 1, the associated RPS channel shall also be placed in manual bypass. Only one ESPS channel at a time is allowed to be placed into Parameter Change Enable Mode Position for software loading/revision. In addition to declaring the processor out of service, when loading or revising software in a voter processor, the affected ESPS voter (Set 1 or Set 2) shall be placed in Bypass. Only one ESPS voter at a time is allowed to be placed into Parameter Change Enable Mode Position for software

loading/revision. Parameter Change Enable Keyswitch status information is sent to a statalarm and is also sent to the OAC via the gateway.

The reliability of the system has been made very high so as to eliminate the need for frequent tests of the logic. The system software is not susceptible to transient, random, aging, or environmental related faults since it does not fail in the conventional sense. It can be reasonably expected to exhibit no degradation from these factors. The cyclic self-monitoring routine verifies that the code is not corrupted. The Mean Time Between Failure (MTBF) data for the Teleperm XS equipment calculates MTBF rates from 29 years to 267 years at 40°C. See Reference 1.

Protective Channel Functional Testing, which is part of the Protective Channel Calibration, is performed every refueling outage. The ESPS software performs a continuous online automated cross channel input check, separately for each input channel, and continuous online signal error detection and validation. The combination of the self-testing features and the reliability of the TXS equipment support a protective channel functional test frequency of every refueling outage. The setpoints in the software are manually verified every 92 days. The output channel output relays are manually actuated every 92 days. ESPS logic is re-verified every refueling outage by rebooting the channel computer and checksums are verified at that time.

Deleted per 2013 Update.

7.3.3.5 Manual Trip

Deleted per 2013 Update.

Each actuation channel (1 through 8) may be manually tripped from the Manual Trip pushbuttons on the Unit Board. This trip is independent of the software and may be initiated during any mode of operation. Each actuation channel (1 through 8) may be manually reset from the Reset pushbuttons on the Unit Board following either automatic or manual actuation of the channel. The ESPS manual actuation paths do not pass through the software, and therefore are not dependent on the correct functioning of the software.

7.3.3.6 Bypassing

The trip functions of the High and Low Pressure Injection and Reactor Building Non-Essential Isolation Systems are bypassed whenever the reactor is to be depressurized below the trip point of the systems. Bypassing must be initiated manually within a fixed pressure band above the protective system trip point. The High Pressure Injection and Reactor Building Non-Essential Isolation System may be bypassed only when the reactor pressure is 1,750 psi or less, and the Low Pressure Injection System may be bypassed only when the reactor pressure is 900 psi or less. The bypass is automatically removed when the reactor pressure exceeds the removal set point associated with the bypass values. This is in accordance with IEEE 279, Section 4.12 and IEEE Std 603-1998 Section 6.6 and 7.4. The removal set points are above the trip points in order to obtain a pressure band in which the trips may be bypassed during a normal cooldown. The bypasses do not prevent actuation of the HP and LP Injection and Reactor Building Non-Essential Isolation Systems on high Reactor Building pressure. Bypassing is under administrative control. Since the ESPS incorporates triple redundancy in its input subsystems, there are three HP injection bypass switches and three LP injection bypass switches. Two of the three switches must be operated to initiate a bypass. Once a bypass has been initiated, the condition is indicated by the plant annunciator and by lamps associated with the bypass switches.

7.3.3.7 References

1. AREVA Document 32-5061241, Oconee Nuclear Station, Unit 1, 2, and 3 RPS/ESFAS TXS Upgrade Availability Analysis (OM 201.N-0028-007).

2. Safety Evaluation Report for RPS/ESPS Digital Upgrade dated January 28, 2010, by the Office of NRR related to Amendment Numbers 366, 368, and 367 to renew Facility Operating Licenses DPR-38, DPR-47, and DPR-55, Oconee Nuclear Station Units 1, 2, and 3 Docket Numbers 50-269, -270,-287.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.3.

7.4 Systems Required for Safe Shutdown

7.4.1 Nuclear Instrumentation

The nuclear instrumentation system is shown in Figure 7-6. The system meets the intent of the Proposed IEEE "Criteria for Nuclear Power Plant Protection Systems," dated August, 1968, (IEEE No. 279), for those elements associated with the Reactor Protective Systems.

7.4.1.1 Design Bases

The nuclear instrumentation (NI) system is designed to supply the reactor operator with neutron information over the full operating range of the reactor and to supply reactor power information to the RPS and to the Integrated Control System (ICS).

The system sensors and instrument strings are redundant in each range of measurement. Measurement ranges are designed to overlap to provide complete and continuous information over the full operating range of the reactor.

7.4.1.2 System Design

The nuclear instrumentation has eight channels of neutron information divided into three ranges of sensitivity: source range, wide range, and power range. The three ranges combine to give a continuous measurement of reactor power from source level to approximately 200 percent of rated power or ten $^{+}$ decades of information. A minimum of one decade of overlapping information is provided between successive higher ranges of instrumentation. The relationship between instrument ranges is shown in Figure 7-7.

The source range instrumentation has four redundant count rate channels originating in four high sensitivity fission chambers. These channels are used over a counting range of 0.1 to 10^5 counts/sec as displayed on the operator's control console in terms of log counting rate. The channels also measure the rate of change of the neutron level as displayed for the operator in terms of startup rate from -1 to +7 decades/min.

The wide range instrumentation has four log N channels originating in four electrically identical fission chambers. Each channel provides ten+ decades of flux level information in terms of the log of chamber count rate and startup rate. The fission chamber/wide range monitor output range is from 10^{-8} to 200% power. The startup rate range is from -1 to +7 decades/min. A high startup rate of +2 decades/min. in any channel will initiate a control rod withdraw inhibit.

The power range channels have four linear level channels originating in four composite uncompensated ion chambers. The channels output is directly proportional to reactor power and covers the range from 0 to 125 percent of rated power. The gain of each channel is adjustable providing a means for calibrating the output against a reactor heat balance.

Power range channels NI-5, -6, -7, and -8 supply reactor power level information continuously to the RPS. Dual indicators on the control console provide the operator with both total reactor power information (ϕ), and reactor power imbalance information ($\Delta\phi$), from each of the four channels. The method of obtaining ϕ and $\Delta\phi$ is described in Section 7.4.1.2.1.

Reactor power information is provided to the ICS from NI-5, NI-6, NI-7 and NI-8. Isolation amplifiers are used to provide isolation of the power range signals leaving the RPS cabinets. Isolation amplifiers are used to buffer the signals leaving the RPS cabinets, preventing the reflection of faults on external signal lines back into the RPS. The ICS uses 2nd highest median select logic for selection of NI-5, NI-6, NI-7,

or NI-8 power range signal to be used for control and display on a recorder located on the control console above the power range indicators.

7.4.1.2.1 Neutron Detectors

The detectors used in the source range and wide range channels are fission chambers. The same detector/electronics string provides both source range and wide range outputs.

Uncompensated ion chambers are used in the power range channels. Power range detectors consist of two nominally 70-inch sections with a single high voltage connection and two separate signal connections. The outputs of the two sections are summed and amplified by the linear amplifiers in the associated power range channel to obtain a signal proportional to total reactor power (ϕ). A signal proportional to the difference in percent full power between the top and bottom halves of the core, the reactor power imbalance or $\Delta\phi$, is derived from the difference in currents from the top and bottom sections of the detector. The difference signal is displayed on the control console to permit the operator to maintain proper axial power distribution. The manual test and calibration facilities provide a means for reading the output of the individual sections of the detector. Each detector has a combined sensitive volume extending approximately from the bottom to the top of the reactor core.

The physical locations of the neutron detectors are shown in Figure 7-8, Figure 7-9, and Figure 7-10. The power range detectors for channels NI-5, -6, -7, and -8 are positioned adjacent to each of the four quadrants of the core. The source/wide range detectors are located adjacent to each of the four quadrants of the core.

Table 7-4 provides pertinent characteristics of the out-of-core neutron detectors. The flux ranges illustrated in Figure 7-7 are seen to be compatible with these characteristics. Nearly identical Westinghouse out-of-core detectors are presently in use at power reactors as follows:

Tube Type	Reactors	Utility
FC	Haddam Neck	Connecticut Yankee Power
	San Onofre	Southern California Edison
	Three Mile Island	GPU Nuclear
	Crystal River 3	Florida Power Corp.
UCIC	Haddam Neck	Connecticut Yankee Power

7.4.1.2.2 Test and Calibration

Test and calibration facilities are built into the system to permit an accurate calibration of the system and the detection of system failures in accordance with the requirements of Reactor Protective System design and IEEE No. 279. The digital RPS systems are also subject to IEEE Std 603-1998 "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations".

7.4.1.3 System Evaluation

The nuclear instrumentation will monitor the reactor over a minimum 10+decade range from source range to 200 percent of rated power. The full power neutron flux level at the power range detectors will be approximately 3.2×10^{9} nv. The detectors employed will provide a linear response up to approximately 1.5×10^{10} nv before they are saturated.

The wide range channels fully overlap the source range and the power range channels as shown in Figure 7-7, providing the continuity of information needed during startup.

The steady-state radial flux distribution within the reactor core will be measured by the incore neutron detectors (Section 7.6.1). Both the out-of-core (NI-5, -6, -7, and -8) and incore detectors will be used to obtain the axial power distribution. The sum of the outputs from the two sections of each (out-of-core) power range detector will be calibrated to a heat balance. The sum will be recalibrated whenever it is determined that the sum disagrees with the heat balance by 2 percent or more. The signals from the two sections of the detector may be individually read and compared independent of the sum of the outputs. The operator, therefore, may correlate the difference signal against the core power distribution obtained from the incore system.

7.4.1.3.1 Primary Power

The nuclear instrumentation draws its primary power from vital buses and uninterruptable buses described in Section 8.3.2.1.4 and Section 8.3.2.1.5.

7.4.1.3.2 Reliability and Component Failure

The requirements established for the Reactor Protective System apply to the nuclear instrumentation. All channel functions are independent of every other channel, and where signals are used for safety and/or control, electrical isolation is employed to meet the criteria of Section 7.1.2.

7.4.1.3.3 Relationship to Reactor Protective System

The relation of the nuclear instrumentation to the RPS is described in Section 7.2. Power range channels NI-5, -6, -7, and -8 are associated with the Reactor Protective System. NI-5, NI-6, NI-7 and NI-8 also provide information for the Integrated Control System through Isolation Amplifiers.

The periodic test requirements of the Reactor Protective System are not dictated by the accuracy of the power range channels. The accuracy of the linear amplifiers is better than ±0.2 percent including drift.

7.4.2 Non-Nuclear Process Instrumentation

7.4.2.1 Design Bases

The non-nuclear process instrumentation provides the required input signals of process variables for the reactor protective, regulating, and auxiliary systems. It performs the required process control functions in response to those systems and provides instrumentation for startup, operation, and shutdown of the reactor system under normal and emergency conditions.

7.4.2.2 System Design

The non-nuclear instrumentation provides measurements used to indicate, record, alarm, interlock, and control process variables such as pressure, temperature, level, and flow in the reactor coolant, steam supply, and auxiliary reactor systems as shown in system drawings in Chapter 5, Chapter 9, Chapter 10 and Chapter 11. Process variables required on a continuous basis for the startup, operation, and shutdown of the unit are indicated, recorded, and controlled at the control rooms. Alternate essential indicators and controls are provided at other locations to maintain the reactor in a hot shutdown condition if the control rooms have to be evacuated. Other instrumentation is provided at auxiliary panels with alarm at the control rooms.

Response time and accuracy of measurements are adequate for reactor protective and regulating systems and other control functions to be performed.

7.4.2.2.1 Non-Nuclear Process Instrumentation in Protective Systems

Four independent measurement channels are provided for each process parameter for input to the Reactor Protective System.

Three independent measurement channels are provided for each process parameter and input to the Engineered Safeguards Protective System.

a. Reactor Outlet Temperature

   Reactor outlet temperature inputs to the Reactor Protective System are provided by two fast-response resistance elements and associated transmitters in each loop.

b. Reactor Coolant Flow

   Reactor coolant flow inputs to the Reactor Protective System are provided by eight high-accuracy differential pressure transmitters which measure flow through calibrated flow tubes welded into the reactor outlet pipe. The power/flow monitor of the reactor protective system utilizes this flow measurement to prevent reactor power from exceeding a permissible level for the measured flow. Operation of each reactor coolant pump breaker is also monitored as an indication of flow.

   RPS Channel E, provides reactor coolant loop A and loop B flow information to the ICS. Channel E is in no way associated with Reactor Protective functions. Reactor coolant loop A and B flow information is also provided to the ICS from RPS Channel A and RPS Channel B. Optical Isolators are used to provide isolation from the RPS. Optical Isolators are used to buffer the signals leaving the RPS cabinets, preventing the reflection of faults on external signal lines back into the RPS. The ICS uses median select logic for selection of the reactor coolant loop A and B flow signal to be used for control.

c. Reactor Coolant Pressure

   Reactor Protective System inputs of reactor coolant pressure are provided by two pressure transmitters in each loop.

   RPS Channel E, provides reactor coolant pressure information to the ICS. Channel E is in no way associated with Reactor Protective functions. Reactor coolant pressure information is also provided to the ICS from RPS Channel A and RPS Channel B. Optical Isolators are used to provide isolation from the RPS. The Optical Isolators are used to buffer the signals leaving the RPS cabinets, preventing the reflection of faults on external signal lines back into the RPS. The ICS uses median select logic for selection of the reactor coolant pressure signal to be used for control and display on a recorder located on the control console.

   Engineered Safeguards Protective System inputs of reactor coolant pressure in each loop are provided by redundant pressure transmitters. One pressure signal is utilized for recording, low pressure alarm, and interlock to decay heat removal return flow valve LP-1. This pressure signal can be supplied from either ES Channel A or B.

d. Reactor Building Pressure

   Reactor Building pressure inputs to the Engineered Safeguards Protective System are provided by:

   1) Three pressure transmitters which are located outside the Reactor Building. These provide inputs for initiation of Reactor Building isolation, high pressure injection, low pressure injection, and Reactor Building cooling.

   2) Three groups of two pressure switches each are located outside the Reactor Building. These provide input signals of high Reactor Building pressure for initiation of Reactor Building spray by safeguards actuation.

Table 7-5 provides pertinent information concerning the NNI sensors supplying inputs to the RPS and ESPS, respectively.

7.4.2.2.2 Non-Nuclear Process Instrumentation in Regulating Systems

Selective reduntant measurements and input signals are provided for the process variables required for critical control functions. Selection between the redundant measurements and input signals is performed within the ICS utilizing two types of equipment. The "Control STAR" [TM] modules perform valid signal selection between certain redundant signals utilizing the median selection technique. Valid signal selection for the remaining critical control process variables is provided by a Smart Automatic Signal Selector (SASS). The SASS detects a rapid change in signal and automatically switches the SASS output signal to the remaining valid input signal.

The SASS instrumentation is located in ICS Cabinet 8 and provides automatic signal selection. The SASS instrumentation monitors the following process signals and selects the valid signal independent of the control board mounted key switch.

1. OTSG Operate Level Loop A
2. OTSG Operate Level Loop B
3. Pressurizer Level

The SASS can also detect a mismatch between the two input signals and provides indication of the mismatch on the SASS panel. The plant computer also receives the same signals as SASS and provides mismatch alarms to the operator via the plant computer.

The "Control STAR" modules are located in the ICS cabinets and provide automatic selection of the median signal for the following process parameters.

1. Reactor Coolant System Pressure
2. Reactor Coolant Flow Loop A
3. Reactor Coolant Flow Loop B
4. Power Range Neutron Flux
5. Feedwater Flow Loop A
6. Feedwater Flow Loop B
7. T-Hot Loop A
8. T-Hot Loop B
9. T-Cold Loop A
10. T-Cold Loop B
11. Turbine Header Pressure
12. OTSG Start-up Level Loop A
13. OTSG Start-up Level Loop B

TM - Control STAR is a trademark of Framatome Technologies.

The following inputs to the Integrated Control System are provided:

a. Reactor Outlet Temperature

Selected loop or unit average outlet temperature input is provided in each loop by two fast response resistance elements and associated transmitters.

b. Reactor Controlling Average Temperature

Loop or unit average temperature signals are selected for indication and input as controlling average temperature. Automatic selection determined by loop flows is provided for input of the appropriate signals.

Reactor inlet temperature signals required for loop, and unit average or differential temperatures are provided in each loop by two fast response resistance elements and associated transmitters.

c. Reactor Inlet Differential Temperature

Reactor inlet differential temperature is calculated, indicated and provided for input to the Integrated Control System.

d. Reactor Coolant Flow

Reactor coolant flow signals are provided for each loop and summed for total flow. Total flow is recorded and "low" total flow is alarmed.

Loop "low" flow signals provide the logic for automatic selection of reactor controlling average temperature.

Contacts from reactor coolant pump motor breakers provide fast indication to the ICS that a pump has tripped.

e. Feedwater Temperature

Feedwater temperature input is provided by three resistance elements and associated transmitters. The selected input also provides indication and feedwater flow temperature compensation.

f. Feedwater Flow

The main feedwater flow measurement in each loop is provided by three redundant differential pressure transmitters that measure flow through a flow nozzle. The automatically selected median feedwater flow signal for each loop is compensated by feedwater temperature. The compensated main feedwater flow signal for each loop is indicated, recorded and input to the ICS.

The start-up feedwater flow measurement in each loop is provided by a differential pressure transmitter that measures flow through a flow nozzle. The start-up feedwater flow signal for each loop is compensated by feedwater temperature. The start-up feedwater flow signal for each loop is indicated to the operator.

g. Feedwater Control Valves Differential Pressure

Pressure drop measurement across the valves is provided for input by redundant differential pressure transmitters. The selected input signal is also indicated.

h. Steam Generator Level

Selected "startup" level and "operate" level inputs are provided from each steam generator. Redundant measurements of each level are provided by differential pressure transmitters. Temperature compensation to augment the predetermined compensation for normal operating temperature is provided by two resistance elements and associated transmitters which measure steam generator lower downcomer temperature.

The selected "operate". level input is recorded and "high" level alarmed. The selected "startup" level input is indicated and "low" level alarmed.

A full range level measurement is provided for indication of each steam generator level but does not provide protective or regulating systems input.

i. Steam Generator Outlet Pressure

Selected outlet pressure input is provided from each steam generator. Measurement is made by pressure transmitters in both outlet lines of each steam generator. The selected input is also indicated.

j. Turbine Header Pressure

Turbine header pressure measurement is provided for input by a pressure transmitter in each header line from the steam generators. The selected pressure signal is also recorded, and high and low pressures alarmed. Additional redundant transmitters in each header line provide indication only.

7.4.2.2.3 Other Non-Nuclear Process Instrumentation

The following instrumentation is provided for measurement and control of process variables necessary for proper operation:

1. Pressurizer Temperature

   Pressurizer temperature is measured by three resistance elements and their associated transmitters. Two resistance elements provide temperature compensation of the Inadequate Core Cooling pressurizer level instrumentation. The third resistance element is used by the pressurizer heater controls to calculate reactor coolant system saturation pressure.

2. Pressurizer Level Control

   Pressurizer level is measured by three differential pressure transmitters. One temperature compensated signal is selected for indication, recording, interlock and level control. The selected level control signal provides alarms and interlock to de-energize the pressurizer electric heaters on low level. The level controller output positions the makeup control valve in the High Pressure Injection System to maintain a preset level. Pressurizer level is lowered by reactor coolant letdown or by manual control at the control room.

3. Reactor Coolant Pressure Control

   The reactor coolant pressure signal for control is provided by isolated signals from RPS Channel A, RPS Channel B and RPS Channel E (the fifth channel). The isolated RPS A, RPS B and the RPS E reactor coolant pressure signals are median selected within the ICS by the "Control Star" module to provide the selected RC Pressure control signal. The selected signal is used as an input to pressure switches which provide signals for automatic control of:

   a. Pressurizer electric heaters.

   b. Pressurizer spray control valve.

   c. Pressurizer electromatic relief valve.

   The heaters are grouped in banks which are energized below preset pressures.

   The selected signal also provides input to a pressure controller which automatically modulates the output of one bank of heaters to maintain a preset pressure.

   The spray and relief valve are opened at preset pressures above the desired reactor coolant system operating pressure.

   The selected signal is recorded and high and low pressures alarmed.

Reactor coolant pressure is recorded on a multi-channel recorder. One Channel has a range of 1700-2500 PSIG, and its input is the median selected reactor coolant pressure signal selected for control. The other channel has a range of 0-2500 PSIG, and its input is from a transmitter in the "A" loop.

Reactor coolant temperature is also recorded on a multi-channel recorder. One channel has a range of 50°F to 650°F and its input is selectable from either of four cold leg RTDs, two located in "A" loop cold legs and two located in "B" loop cold legs. A second channel indicating average temperature receives its imput from the reactor coolant average temperature selected for control and has a range of 520°F to 620°F. A third channel has a range of 520°F to 620°F and receives its input from the selected "A" loop THOT signal. A fourth channel has a range of 520°F to 620°F and receives its input form the selected "B" loop THOT signal. A fifth channel has a range of 520°F to 620°F and receives its input from the selected Average THOT signal.

4. Coolant Pump Control

   Interlock signals of reactor coolant inlet temperature are provided to each pump switching logic to prevent operation of more than three pumps during startup until a preset temperature is reached.

5. Feed and Bleed Control

   The feed and bleed control instrumentation in the High Pressure Injection System provides control and interlocks to permit adjustment of the reactor coolant boron concentration.

7.4.2.3 System Evaluation

The quantity and types of process instrumentation have been selected to provide assurance of safe and orderly operation of all systems and processes over the full operating range of the plant. Some of the criteria for design are:

1. Separate instrumentation and Engineered Safeguards Protective System, Reactor Protective System and Steam Generator Level Control System isolated output signals are used for vital control circuits.
2. Time of response and accuracy of measurements are adequate for protective and control functions to be performed.
3. Where wide process variable ranges are required and precise control is involved, both wide range and narrow range instrumentation are provided.
4. All electrical and electronic instrumentation required for operation is supplied form redundant vital and uninterruptable instrumentation buses.

7.4.2.3.1 Failure in RC Flow Tube Instrument Piping

7.4.2.3.1.1 Reactor Coolant Flow Indication

In each primary loop, reactor coolant flow is detected by measuring the ΔP developed across a flow tube that is an integral part of the outlet piping of the loop. Each flow tube has a high pressure (HP) tap and a low pressure (LP) tap. Connections to the taps are made with 1-inch lines. The 1-inch lines are terminated at root valves located inside the secondary shield wall to HP and LP headers. Five ΔP transmitters are connected between the two headers. Four are used to provide information to the Reactor Protective System. The fifth is used to provide input to the ICS. Isolated output signals from RPS Channel A, RPS Channel B and the fifth transmitter are input to the ICS "Control STAR" modules. The median selected signal provides alarms and indication as described in Section 7.4.2.2.2.

Each of the four Reactor Protective System channels receives a ΔP signal from a different one of the four ΔP transmitters. In other words, one transmitter is exclusively assigned to one protective channel. The

identical arrangement and assignment of transmitters is used for each of the two primary reactor coolant loops.

Within each Reactor Protective System channel, the square roots of the ΔP signals from each loop are extracted to obtain loop flow signals. The loop flow signals are summed to obtain a total reactor coolant flow signal. The three flow signals are displayed by connecting the STAR CTC to the channel's STAR module. The three signals are monitored by the plant computer.

The reactor operator can read the individual loop flows and total flow at the control console. The flow information is available to the operator on the plant computer for each unit.

7.4.2.3.1.2 Failures Considered

The following failures are considered:

1. Break in one of the 1-inch instrument lines.
2. Break in one of the 1/2-inch instrument lines.
3. A leak in one of the instrument lines.
4. Deleted per 2005 update.

7.4.2.3.1.2.1 Break in 1 Inch Instrument Lines

A break of a 1-inch instrument line will result in a reactor trip due to low RC pressure. If the break occurs in a HP line, the reactor will trip due to a high power/flow ratio if the power/flow limit is exceeded.

The operator will receive at least the following alarms and indications:

Alarms:

1. Break in 1-inch HP Instrument Line
   a. Low RC flow.
   b. Plant computer alarm and alarm log for low flow.
   c. Letdown storage low level.
   d. Pressurizer low level.
   e. Low reactor coolant pressure.
   f. Plant computer alarm and alarm log for low RC pressure.
2. Break in a 1-inch LP Instrument Line

   Identical alarms as listed for HP line break except RC flow is alarmed on high value.

Indication:

1. Break in a 1-inch HP Instrument Line
   a. Control room indication of the Reactor Building atmosphere particulate and gas radioactivities increases.
   b. Loop flow indication on console falls to zero.
   c. Loop flow indication in each RPS channel falls to zero. Flow is not displayed in the RPS channel cabinets unless STAR CTC is connected to channel.
   d. Total flow indication on console falls approximately 50 percent.

e. Total flow indication in each RPS channel falls approximately 50 percent. Flow is not displayed in the RPS channel cabinets unless STAR CTC is connected to channel.

f. Makeup flow goes to maximum value.

g. RC pressure falls on console indicators and with each RPS channel.

h. Reactor Building pressure and temperature indication rises.

2. Break in a 1-inch LP Instrument Line

   Identical indication as listed for HP line break except all loop flow indication goes full scale, total flow indication increases above normal.

7.4.2.3.1.2.2 Break in a ½-inch Instrument Line

A break of a ½-inch instrument line will result in a reactor trip due to low RC pressure. If the break occurs in a HP line, the reactor will trip due to a high power/flow ratio if the power/flow limit is exceeded.

The operator will receive the same alarms and indication as described for the 1-inch instrument line break.

7.4.2.3.1.2.3 Leak in One of the Instrument Lines

If the leak occurs in a HP line the operator will receive a low flow alarm for a 5 percent change in indication flow and a high flow alarm for a similar leak in the LP line. At this alarm Point, the leakage is in excess of 1 gallon per minute, hence Reactor Building radiation monitors will readily detect such a condition and result in leak evaluation, and subsequent action as required by Technical Specifications.

Depending on the size of the leak, alarms and indication described in Section 7.4.2.3.1.2.1, may occur. If the leak occurs on either of the ΔP transmitters associated with the RPS-A, RPS-B or the fifth channel input, the ICS "Control STAR" modules will select the median signal for control and indication as described in Section 7.4.2.2.2.

7.4.2.3.1.2.4 Deleted per 2005 Update

7.4.2.3.1.3 Conclusion

The conclusion of this analysis is that the operator has adequate indication and alarm facilities to quickly recognize a common mode failure in the flow instrumentation for the reactor protection system. Corrective action would therefore be positive and prompt.

7.4.2.3.2 Coincident LOCA and Systematic Failure of Low RCS Pressure Trip Signal.

Several break sizes and locations for the loss-of-coolant accident have been investigated with an assumed systematic failure of the low Reactor Coolant System pressure trip signal. Although this failure is not considered credible, the analysis has shown that either the void shutdown mechanism or the power/flow comparator should provide backup to shut down the reactor and render the Emergency Core Cooling System (ECCS) effective.

7.4.3 Emergency Feedwater Controls

7.4.3.1 Emergency Feedwater and Pump Controls

7.4.3.1.1 Design Basis

The Emergency Feedwater (EFW) System is designed to start the EFW pumps automatically in the event of loss of both main feedwater pumps or low water level in either steam generator.

The EFW control valves are designed to control steam generator level when the EFW System is supplying feedwater to the steam generators.

All automatic initiation logic and control functions are independent from the Integrated Control System (ICS).

7.4.3.1.2 System Design

Three EFW pumps powered from diverse power sources are provided. These include two independent motor driven pumps, each supplying feedwater to one steam generator; and one turbine driven pump, supplying feedwater to both steam generators.

Each of the EFW pumps is supplied with its own independent starting circuit which will start automatically as outlined below. Automatic initiation of the EFW pumps by ATWS Mitigation System Actuation Circuitry is described in Section 7.8. These independent control circuits are powered by the 125 VDC station batteries. Each pump is also provided with a control switch with which the operator may start the pump manually.

Discharge flow from the EFW pumps is normally aligned and controlled by discharge control valves located in the supply line to each steam generator's emergency feedwater connection. The control valves limit or increase emergency feedwater as necessary to maintain steam generator inventory and cooldown rate. These valves may be automatically controlled, or manually controlled by the operator.

Indication is provided in the control room to allow the operator to monitor EFW System parameters during a cooldown.

Alarms are provided to alert the operator of conditions exceeding normal limits. Essential plant parameters are annunciated or alarmed by the process computer in addition to specific EFW System alarms.

Motor Driven EFW Pumps (MDEFWP's):

Power for the motor driven pumps is normally provided by the normal station auxiliary power system. During loss of offsite power operation, these pumps are aligned to the Emergency Power System

Automatic starting of the MDEFWP's is determined by the position of the control room selector switch for each pump. The MDEFWP's are provided with a four position selector switch which allows the operator to select between OFF, AUTO 1, AUTO 2 and RUN. When the selector switch is in the AUTO 1 position, LOW STEAM GENERATOR WATER LEVEL in either steam generator (OTSG) will start the pump after a time delay to prevent spurious actuations. When the selector switch is in the AUTO 2 position, LOW STEAM GENERATOR WATER LEVEL or LOSS OF BOTH MAIN FEEDWATER PUMPS will start the pump. Loss of both main feedwater pumps is sensed by pressure switches which monitor feedwater pump turbine hydraulic oil pressure.

Automatic starts of the MDEFWPs are disabled if a main steam line break is sensed by the Automatic Feedwater Isolation System (AFIS). Upon an AFIS actuation, the MDEFWP aligned to the affected steam generator will automatically stop and be inhibited from any further automatic starts. Once automatically started, the MDEFWPs will continue to operate until manually secured by the operator or

disabled by an AFIS signal. The operator can manually start the MDEFWP by placing its selector switch to RUN.

Cooling water is initiated automatically, upon manual or automatic start of the MDEFWPs.

Turbine Driven EFW Pump (TDEFWP):

The steam supply for the TDEFWP turbine is provided from the main steam lines upstream of the main turbine stop valves and/or from the Auxiliary Steam System. Upon loss of station air, the supply is maintained by nitrogen bottle back-ups which are used on the pressure control valves. Should the nitrogen bottle back-ups fail, these control valves would fail to the open position.

The steam admission valve to the turbine, MS-93 is controlled by a normally energized solenoid valve. Upon receipt of a manual or automatic start signal, the solenoid valve will de-energize and immediately start the turbine by opening the steam admission valve. The steam admission valve will fail open upon loss of power to the normally energized solenoid valve or loss of supply air. The supply air is equipped with instrument air, auxiliary instrument air, and bottled Nitrogen backups. The EFW pump turbine speed is controlled by MS-95. The position of MS-95 is regulated by a hydraulic oil speed governing mechanism, with oil supplied from either the auxiliary oil pump or the shaft driven oil pump. MS-95 is designed to fail closed on loss of hydraulic oil pressure. An AFIS actuation will energize and close solenoid valve (TO-145) to isolate the hydraulic oil supply to close MS-95.

THE TDEFWP auxiliary oil pump is started automatically when the steam admission valve is opened, and provides hydraulic oil pressure for the operation of the TDEFWP governor control valve until the TDEFWP shaft driven oil pump is available. The TDEFWP auxiliary oil pump and its associated circuitry is required for automatic start of the TDEWFP. This equipment is powered from station batteries.

Automatic starting of the TDEFWP is determined by the position of the control room selector switch for the pump. The TDEFWP is provided with a three position-pull to lock selector switch. The operator can select between OFF, AUTO and RUN. When the selector switch is in the AUTO position, LOSS OF BOTH MAIN FEEDWATER PUMPS, with exception to loss due to the AFIS logic, will start the pump. Loss of both main feedwater pumps is sensed by pressure switches which monitor feedwater pump turbine hydraulic oil pressure. Automatic starts of the TDEFWP are disabled if a main steam line break is sensed by the AFIS circuitry. Upon an AFIS actuation, the TDEFWP will automatically stop and be inhibited from any further automatic starts. Once automatically started, the TDEFWP will continue to operate until manually secured by the operator or disabled by an AFIS (Unit 1) or MSLB (Units 2 and 3) signal. The operator can manually start the TDEFWP by placing the selector switch to RUN.

Once automatically started, the TDEFWP will continue to operate until manually secured by the operator or shutdown by the MSLB circuitry.

Control Valves:

Deleted paragraph(s) per 2002 Update.

Each emergency feedwater discharge line to each steam generator is provided with a control valve and a check valve. The air operated control valves receive an electric current signal that is converted to an air signal through an I/P converter. The converted signal is used for modulation of the valve in response to steam generator level, independent from the ICS. Each control valve has a Hand/Auto station mounted on the main control board. A pushbutton is provided on each Hand/Auto station to allow the individual EFW control valve to be placed in either an automatic level control mode or in a manual level control mode of operation. The Hand/Auto stations may be utilized to position the respective control valve when in the manual mode. Open/Closed valve position indication is provided for each control valve in the main control room. Power to the controller is battery backed DC converted to AC via the vital inverters.

The control valves are normally closed in the automatic mode due to steam generator level > setpoint. In automatic, an Auto/Manual relay for each control valve is de-energized, allowing the valve to be positioned automatically.

The control valves are arranged to fail to the automatic control mode upon loss of control power to the Hand/Auto station. If the selected train of automatic control experiences a loss of power, then the valve would fail open. Also, upon loss of station air, the valves will continue to control using the nitrogen supply. If the nitrogen supply fails the valve would fail open. These modes of operation show that Emergency Feedwater isolation will not result from valve control circuitry failure or motive force failure.

7.4.3.1.3 System Evaluation

Redundancy is provided with separate, full capacity, motor and turbine driven pump subsystems. Failure of either the motor driven pumps or the turbine driven pump will not reduce the EFW System below minimum required capacity. Pump controls, and instrumentation are separate and independent in design.

7.4.3.2 Steam Generator Level Control

7.4.3.2.1 Design Basis

The Steam Generator Level Control System (SGLCS) provides automatic Once Through Steam Generator (OTSG) water level control while the EFW System is supplying feedwater to the steam generators. SGLCS is designed to automatically control and modulate emergency feedwater supply to the steam generators during all initiating conditions for the EFW System (Section 7.4.3). Each OTSG has two independent level control systems each of which is capable of supplying a signal to the associated OTSG emergency feedwater level control valve.

The Steam Generator Level Control System (SGLCS) provides the automatic start signal for both MDEFWPs based on low level in either steam generator.

All automatic initiation logic and control functions are independent from the Integrated Control System (ICS).

7.4.3.2.2 System Design

Each OTSG is provided with two independent level control systems, each of which supplies a signal to that OTSG's emergency feedwater level control valve. The two systems provided for each OTSG monitor the 0-388 inch range (range at cold shutdown) of water in the OTSG. A signal deviation check between the two output signals is performed.

The SGLCS controls level higher than the normal ICS level setpoint to prevent control system conflict. Upon loss of all four reactor coolant pumps, such as during blackout conditions, the level control setpoint is automatically raised to promote natural circulation in the Reactor Coolant System.

Deleted paragraph(s) per 2002 Update.

The operator has a selector switch on the main control board, which is used to select either control channel on each OTSG. Also provided on the main control board is a Hand/Auto station, which may be utilized to override the automatic level control signal. A control switch is provided on the control board for each EFW control valve that can be selected to bypass the Hand/Auto station. When this switch is selected to the bypass or off position only the automatic level control signal is sent to the respective valve. The Hand/Auto stations have redundant QA-1 power sources to minimize the possibility of losing the manual control capability of these valves.

7.4.3.2.3 System Evaluation

Each level channel is separate and independently powered from its counterpart on each OTSG. Redundancy is provided with two trains/channels monitoring each steam generator. Each level channel per steam generator is capable of performing the necessary control and modulation of the feedwater control valves. In addition, sufficient alarms and indications are provided to alert the operator to a system failure and ensure correct manual operation of a level control valve.

7.4.4 Reactor Building LPSW Low Pressure Instrumentation Circuitry

7.4.4.1 Design Basis

Generic Letter 96-06 required consideration of effect inside containment due to the change in environment during a Loss of Coolant Accident (LOCA). This consideration identified the potential for waterhammers in cooling water systems serving containment following a Loss of Offsite Power (LOOP) concurrent with a LOCA or Main Steam Line Break (MSLB). Analysis and system testing in response to GL 96-06 concluded that waterhammers could occur in the Low Pressure Service Water (LPSW) system during all LOOP events (e.g. LOCA/LOOP, MSLB/LOOP). The LPSW piping supplies the Reactor Building Cooling Units (RBCU), the Reactor Building Auxiliary Coolers (RBAC), and the Reactor Coolant Pump Motor Coolers (RCPMC). During Loss of Offsite Power (LOOP) events or Loss of Coolant Accident (LOCA) events coupled with a LOOP it was possible to create a Column Closure Waterhammer (CCWH) or Condensation Induced Waterhammer (CIWH) in the LPSW piping and components inside containment. CCWH could have occured when the LPSW pumps restart following a LOOP and rapidly close vapor voids with the system. CIWH could have occurred when heated steam voids interact with sub-cooled water in long horizontal piping sections.

7.4.4.2 System Design

The Reactor Building LPSW Low Pressure Instrumentation Circuitry consists of four (4) analog channels each powered from a separate safety related battery backed power panel board and two (2) digital actuation channels each powered from a separate safety related battery backed power panel board. Portions of the analog and digital channels are shared with the RBAC LPSW Low Pressure Instrumentation Circuitry which isolates the LPSW supply and return flow to the Reactor Building Auxiliary Coolers (RBAC).

The design function of the instrumentation circuitry is to close the pneumatic discharge isolation valves (LPSW-1121, 1122, 1123, and 1124) and open controllable vacuum breakers (LPSW-1150 and LPSW-1151) any time a low pressure condition occurs in the LPSW supply header. Closure of LPSW-1121, 1122, 1123, and 1124 and the opening of controllable vacuum breakers LPSW-1150 and LPSW-1151 on low LPSW pressure will maintain the LPSW piping inside the Reactor Building water solid thereby avoiding water hammers in the RBCU LPSW piping.

7.4.4.2.1 Analog Channels

A pressure transmitter for each of the four (4) analog channels monitors LPSW supply header pressure. When pressure decreases to the design set point as sensed by a particular channel, a trip relay and alarm relay are actuated for each of the respective channels that sensed the low pressure condition.

The low pressure output from each of the four (4) analog channels provide input to the two redundant 2 out of 4 trip logic paths in each of the two (2) digital logic trip channels.

7.4.4.2.2 Digital Channels

The inputs from the four analog channels are arranged in such a way as to provide different paths within each of the two redundant 2 out of 4 logic circuits. This assures the Reactor Building LPSW flow does not terminate to the Reactor Building due to a single failure of one of the other analog channels during an analog channel test.

The two redundant digital logic trip channels provide a close command signal to the solenoid valves for pneumatic discharge isolation valves LPSW-1121, 1122, 1123, and 1124. The two redundant digital logic trip channels also provide a trip open command signal to the solenoid valves for controllable vacuum breakers LPSW-1150 and LPSW-1151 when a low LPSW pressure condition occurs.

7.4.4.2.3 System Actuation and Reset

Upon actuation of the system, power is removed from solenoid valves LPSW-1121, 1122, 1123 and 1124 to cause each of the normally open pneumatic discharge isolation valves LPSW-1121, 1122, 1123, and 1124 to "Trip" (go to the closed position).

Simultaneously, power is applied to solenoid Valves LPSSV-1150 and LPSSV-1151 which in turn cause the normally closed controllable vacuum breakers LPSW-1150 and LPSW-1151 to "Trip" (i.e., go to the open position). Controllable vacuum breakers LPSW-1150 and LPSW-1151 will "Reset" (i.e., go to the closed position) if both low pressure trips have returned to their normal state. If this should fail to reset the controllable vacuum breaker for a particular train, then, the controllable vacuum breakers for that train will still reset when the normal pressure reset logic for that train has been satisfied as described below.

The low pressure LPSW trips reset to provide a permissive for the resetting of the Waterhammer Protection System (WPS) and the controllable vacuum breakers following the return to normal LPSW system pressure.

However, as stated above, pneumatic discharge isolation valves for a particular train will not actually re-open (Reset) until the low pressure trip for that particular train has also reset, which should have already occured by the time that the normal pressure reset logic circuit has been actuated. Therefore, when the LPSW supply pressure is restored to a value greater than its normal set point value as sensed on two of the four analog input channels, then, power will be reapplied to the solenoid valves that control the pneumatic discharge isolation vlaves LPSW-1121, 1122, 1123, and 1124 results in the re-opening of these valves. Simultaneously, the power path will be interrupted to the solenoid valves that control the controllable vacuum breakers LPSW-1150 and 1151 resulting in the re-closing of these valves, if they have not already done so by the removal of the two trip signals from the digital trip logic.

7.4.4.2.4 RBAC

As stated above, portions fo the pneumatic discharge isolation valves instrumentation circuitry are shared with the RBAC LPSW Low Pressure Instrumentation Circuitry. After the LPSW supply pressure is restored, LPSW Valves LPSW-1054, 1055, 1061, and 1062 will remain closed until the control room operator resets the circuitry by depressing the respective channel reset pushbutton on the control room vertical board and initiates a slow ramp open circuit to restore flow back to the RBAC units.

7.4.4.2.5 Loss of Electrical Power

The pneumatic discharge isolation valves LPSW-1121, 1122, 1123, and 1124 are spring loaded to open and require air to close. The controllable vacuum breakers, LPSW-1150 and LPSW-1151, are spring loaded to close and require air to open. The pneumatic discharge isolation valves and the controllable vacuum breakers all fail closed on loss of electrical power to their respective control solenoid valves.

7.4.4.2.6 System Evaluation

Each analog channel is powered from a separate safety related battery backed power panel board. Likewise, each digital channel is also powered from a separate safety related battery backed power panel board. Redundancy is provided by two pressure transmitters/analog channels monitoring each LPSW supply header. The two-out-of-four logic prevents actuation from the failure of a single transmitter. The LPSW Waterhammer Prevention System is QA1. The system is capable of performing the necessary control and modulation of the LPSW system.

7.4.5 References

1. *Evaluation of Transient Nuclear Instrumentation Power Range Flux Error* - Duke Power Company - March 1981.
2. Qualification Testing of Protective System Instrumentation Babcock and Wilcox - *BAW - 10003 Rev. 3 - April, 1974 and BAW - 10003A Rev. 4 - January, 1976.*
3. *Evaluation of Reactor Protective System Grounding Concern* Babcock and Wilcox - March, 1978.
4. *177 FA Plants NI/RPS Ground Problem Discussion and Recommended Test Scheme* Babcock and Wilcox - March, 1978.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.4.

7.5 Display Instrumentation

7.5.1 Criteria And Requirements

7.5.1.1 Type A Variables

Type A variables are defined as those variables which are monitored to provide the primary information required to permit the Control Room operator to take specific manually controlled actions for which no automatic control is provided and that are required for safety systems to accomplish their safety functions for design basis accidents. Primary information is defined as that which is essential for the direct accomplishment of the specified safety functions; it does not include those variables associated with contingency actions which may also be identified in written procedures.

Emergency Procedures provide the lead guidance for selection of Type A variables. The following variables are those determined to be Type A for Oconee Nuclear Station, as defined above:

1. Reactor Coolant System Pressure
2. Core Exit (Thermocouples) Temperature
3. Pressurizer Level
4. Degrees of Subcooling
5. Steam Generator Level
6. Steam Generator Pressure
7. Borated Water Storage Tank Level
8. High Pressure Injection Flow
9. Low Pressure Injection Flow
10. Deleted per 2006 update
11. Deleted per 2005 update
12. Upper Surge Tank Level
13. Low Pressure Service Water (LPSW) Flow to Low Pressure Injection (LPI) Coolers.

7.5.1.2 Type B and C Variables

Type B and C variable selection is based on the Safety Parameter Display System (SPDS) Critical Safety Functions. The SPDS, which meets the requirements of NUREG 0737, Supplement 1,is provided as an aid to the Control Room operating crew in monitoring the status of the Critical Safety Functions. The Critical Safety Functions monitored are those defined in the SPDS Critical Safety Function Fault Trees. The SPDS provides continuous status updated at regular intervals of the Critical Safety Functions.

Since these Critical Safety Functions constitute the basis of the Oconee SPDS, it is Duke Power's position that they should also be identified as the plant safety functions for accident monitoring (i.e., the basis for Type B & C variable selection).

Using the SPDS Critical Safety Functions as the basis for defining the accident monitoring instrumentation incorporates the concept of monitoring the multiple barriers to the release of radioactive material. The Critical Safety Functions monitored are those which assure the integrity of these barriers. The Fault Tree provides an explicit, systematic mechanism for organizing the plant data required to

evaluate a Critical Safety Function. The prioritization of the Critical Safety Functions is consistent with the concept of multiple barriers to radiation release.

The Critical Safety Functions are:

1. Subcriticality

The subcriticality fault tree monitors the reactor core to assure that it is maintained in a subcritical condition following a successful reactor trip.

2. Inadequate Core Cooling

The inadequate core cooling fault tree monitors those variables necessary to evaluate the status of fuel clad heat removal.

3. Heat Sink

The heat sink fault tree monitors the ability to transfer energy from the reactor coolant to an ultimate heat sink.

4. Reactor Coolant System Integrity

The Reactor Coolant System integrity fault tree monitors those variables indicating a challenge to or a breach of the Reactor Coolant System pressure boundary.

5. Containment Integrity

The containment integrity fault tree monitors those variables which would indicate a threat to containment integrity or other undesirable conditions within containment.

6. Reactor Coolant System (RCS)

The RCS inventory fault tree monitors for indications of off-normal quantities of reactor coolant in the primary system.

7.5.1.3 System Operation Monitoring (Type D) and Effluent Release Monitoring (Type E) Instrumentation

7.5.1.3.1 Definitions

Type D: Those variables that provide information to indicate the operation of individual safety systems.

Type E: Those variables to be monitored as required for use in determining the magnitude of the release of radioactive materials and in continually assessing such releases.

The Type D and E variables are selected on the basis of individual plant specific system design requirements.

7.5.1.3.2 Operator Usage

The plant design has included variables and information display channels required to enable the Control Room operating personnel to:

1. Ascertain the operating status of each individual safety system to the extent necessary to determine if each system is operating or can be placed in operation to help mitigate the consequences of an accident. (Note: Type D and E are not always safety systems)
2. Monitor the effluent discharge paths to ascertain if there have been significant releases (planned or unplanned) of radioactive materials and to continually assess such releases.

3. Obtain required information through backup or diagnosis channel where a single channel may be likely to give ambiguous indication.

7.5.1.4 Design and Qualification Criteria

Design and qualification criteria used by Duke Power Company for plant instrumentation are provided below. The category designations are provided for reference to the Regulatory Guide 1.97 (Revision 2) document.

7.5.1.4.1 Design and Qualification Criteria - Category 1

Accident monitoring instrumentation which comprise this design and qualification category are considered by Duke Power to be Nuclear Safety Related and thus are classified as Quality Assurance Condition 1 (QA1).

1. QA1 instrumentation is environmentally qualified as described in the Oconee Nuclear Station IEB-79-01B Duke Power Company submittal and the Resolution of Safety Evaluation Reports for Environmental Qualification of Safety Related Electrical Equipment. Seismic qualification is in accordance with the Oconee Nuclear Station licensing basis as specified in Oconee FSAR Chapter 3 and the Duke Power Seismic Design Criteria (OSDC-0193.01-00-0001).

2. No single failure within either the accident monitoring instrumentation, its auxiliary supporting features, or its power sources, concurrent with the failures that are a condition or result of a specific accident, will prevent the operators from being presented the information necessary to determine the safety status of the plant and to bring the plant to and maintain it in a safe condition following that accident. Where failure of one accident-monitoring channel results in information ambiguity (i.e., the redundant displays disagree) that could lead operators to defeat or fail to accomplish a required safety function, additional information is provided to allow the operators to deduce the actual conditions in the plant. This is accomplished by providing additional independent channels of information of the, same variable (an identical channel) or by providing an independent channel to monitor a different variable that bear a known relationship to the multiple channels (a diverse channel). The information provided to the operator to eliminate ambiguity between redundant channels is needed only during a failure of one of the instrument loops. Therefore, it is considered acceptable to use installed instrumentation of equal design and qualification category, installed instrumentation of a lessor design and qualification category, temporary or portable instrumentation, or sampling to allow the operators to deduce the actual conditions in the plant. Redundant QA1 channels are electrically independent and physically separated from each other per the separation criteria described in Chapter 7 of the Oconee FSAR.

   At least one channel of QA1 instrumentation is displayed on a direct indicating or recording device. (Note: Within each redundant division of a safety system, redundant monitoring channels are not needed.)

3. The instrumentation is energized from the safety grade Emergency Power sources (as described in Chapter 8 of the Oconee FSAR) and is backed by batteries where momentary interruption is not tolerable.

4. The instrumentation channel will be available prior to an accident except as provided in Paragraph 4.11, "Exception" as defined in IEEE Standard 279-1971 or as specified in Technical Specifications. For the digital RPS/ESPS system, which includes the TXS cabinets and their associated hardware, the instrumentation channel will be available as defined in IEEE Std 603-1998 Sections 5.7, 6.7, 7.5 and 8.3.

5. The following documents pertaining to quality assurance are referenced:

a. Duke 1A, Duke Power Company Topical Report, "Quality Assurance Program"

b. Oconee FSAR Chapter 17

6. Continuous indication display is provided. Where two or more instruments are needed to cover a particular range, overlapping of instrument span is provided.

7. Recording of instrumentation readout information is provided for at least one of the redundant channels. Recorders which are utilized as the primary display device will be seismically qualified. Where direct and immediate trend or transient information is essential for operator information or action, the recording is continuously available on dedicated recorders. Otherwise, it may be displayed on non-seismically qualified recorders or continuously updated, stored in computer memory, and displayed on demand. Intermittent displays such as data loggers and scanning recorders may be used if no significant transient response information is likely to be lost by such devices. All analog variables which are wired to the plant computer may be trended upon demand and a hard-copy can be generated as needed.

7.5.1.4.2 Design and Qualification Criteria - Category 2

7.5.1.4.2.1 Nuclear Safety Related (QA1) Category 2 Instrumentation

For instrumentation loops that are installed as nuclear safety related (QA1), environmental qualification is provided per the methodology described in the Oconee Nuclear Station IEB 79-01B submittal and the Resolution of Safety Evaluation Reports for Environmental Qualification of Safety Related Electrical Equipment. Seismic qualification is in accordance with the Oconee Nuclear Station Licensing basis as specified in the Oconee FSAR and Duke Power Seismic Design Criteria (OSDC-0193.01-00-0001). Quality Assurance of these QA Condition 1 instrumentation systems is described in the Duke Power Company Topical Report "Duke 1A" and Oconee FSAR Chapter 17. These instruments are powered from the safety grade Emergency Power sources (as described in Chapter 8 of the Oconee FSAR) and are backed by batteries where a momentary power interruption is not tolerable.

7.5.1.4.2.2 Non Nuclear Safety Related (Non-QA1) Category 2 Instrumentation

For instrumentation loops of lesser importance which are not nuclear safety related, appropriate qualification is provided. Environmental qualification is provided per the methodology described in the Oconee Nuclear Station IEB 79-01B submittal and the Resolution of Safety Evaluation Reports for Environmental Qualification of Safety Related Electrical Equipment.

Category 2 instrumentation which is of primary use during one phase of an accident need not be qualified for all phases of the event. For example, an instrument of primary importance prior to attained the recirculation mode need not be demonstrated to withstand post-recirculation radiation.

For non-QA1 Category 2 instrumentation, seismic qualification is not required unless seismic induced failure of the instrumentation would unacceptably degrade a safety system.

These instrumentation systems are designed, procured, and installed per Duke Power Company standard practices. Duke Power considers that this is adequate to assure the quality of the subject instrumentation.

Isolation devices are provided to interface between Nuclear Safety Related (QA1) and Non Nuclear Safety Related (non QA1) portions of any of the subject instrumentation loops.

The instrumentation is energized from a highly reliable power source, not necessarily safety grade Emergency Power, and is backed by batteries where momentary interruption is not tolerable.

7.5.1.4.2.3 All Category 2 Instrumentation

For both Nuclear Safety Related and Non Nuclear Safety Related Category 2 instrumentation:

The out-of-service interval should be based on normal Technical Specification requirements for the system it serves where applicable or where specified by -other requirements.

The instrumentation signal may be displayed on an individual instrument or it may be processed for display on demand by CRT or by other appropriate means.

The method of display may be by dial, digital, CRT, or stripchart recorder indication. Effluent radioactivity monitors and meteorology monitors will be recorded. Where direct and immediate trend or transient information is essential for operation information or action, the recording is continuously available on dedicated recorders. Otherwise, it may be continuously updated, stored in computer memory, and displayed on demand.

7.5.1.4.3 Design and Qualification Criteria - Category 3

These instruments do not play a key role in the management of an accident but they do add depth to the Category 1 and 2 instrumentation to the extent that they remain operable. The instrumentation is of high quality commercial grade and is selected to withstand the normal power plant service environment.

The method of display may be by dial, digital, CRT, or stripchart recorder indication. Effluent radioactivity monitors and meteorology monitors will be recorded. Where direct and immediate trend or transient information is essential for operator information or action, the recording is continuously available on dedicated recorders. Otherwise, it may be continuously updated, stored in computer memory, and displayed on demand.

7.5.1.4.4 Additional Criteria for Categories 1 and 2

In addition to the criteria of Duke Position 7.5.1.4, the following criteria apply to Categories 1 and 2:

1. For Nuclear Safety Related (QA1) signals which are transmitted to non-safety related (non QA1) equipment, isolation devices are utilized.
2. Dedicated control board displays for the instruments designated as Types A, B, and C, Category 1 or 2 and qualified for use throughout all phases of an accident will be specifically identified on the control panels so that the operator can discern that they are available for use under accident conditions.

7.5.1.4.5 Additional Criteria for All Categories

In addition to the above criteria, the following criteria apply to all instruments identified in this document:

1. Servicing, testing, and calibration programs are specified to maintain the capability of the monitoring instrumentation. For those instruments where the required interval between tests will be less than the normal time interval between generating station shutdowns, the capability for testing during power operation is provided.
2. Whenever means for removing channels from service are included in the design, the design facilitates administrative control of the access to such removal means.
3. The monitoring instrumentation design minimizes the development of conditions that would cause meters, annunciators, recorders, alarms, etc., to give anomalous indications which are potentially confusing to the operator. Human factors guidelines are used in determining type and location of displays. The Duke Control Room Review Team made recommendations as to the type and location of displays, for added instrumentation.

4. To the extent practicable, the instrumentation is designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.
5. To the extent practicable, monitoring instrumentation inputs are from sensors that directly measure the desired variables.
6. To the extent practicable, the same instruments which are used for accident monitoring are used for the normal operations of the plant to enable the operators to use, during accident situations, instruments with which they are most familiar. However, where the required range of monitoring instrumentation results in a loss of necessary sensitivity in the normal operating range, separate instruments are used.
7. Periodic checking, testing, calibration, and calibration verification are in accordance with the applicable portions of the Oconee FSAR Chapter 7.

7.5.2 Description

Display instrumentation provided for Oconee operators is described below.

7.5.2.1 Reactor Coolant System Pressure

Three channels of Reactor Coolant System (RCS) Pressure indication are available through the plant operator computer (OAC), which receives the RCS Pressure signals through the Engineered Safety Features Actuation System (ESFAS) cabinets. This instrumentation is powered from a highly reliable battery backed source. These instrumentation channels monitor RCS pressure over the range 0 to 2500 psig. Two channels are recorded.

Two upgraded QA Condition 1 channels of Wide Range RCS Pressure indication are provided for post accident monitoring in response to Regulatory Guide 1.97. These instrumentation loops are seismically and environmentally qualified and are powered from safety grade emergency power sources. Signals to the Control Board readouts are processed through the Inadequate Core Cooling Monitoring (ICCM) system cabinets. The range for the readouts, 0-3000 psig, is in compliance with Regulatory Guide 1.97 specifications.

RCS pressure is a Type A Category 1 variable at Oconee, since the operator relies on this indication to determine when to switch from high pressure injection to low pressure injection.

Two upgraded QA Condition 1 channels of Low Range RCS Pressure indication are available via the Low Temperature Overpressure Protection (LTOP) System. These instrumentation loops are seismically and environmentally qualified and powered from safety grade emergency power sources. Although not required, the loops meet the RG 1.97 Category 1 instrumentation requirements of Section 7.5.1.4. The range for the readouts is 0-600 psig. The LTOP instrumentation loops are not credited in any design basis event. The instrumentation is classified as RG 1.97 Type D.

7.5.2.2 Inadequate Core Cooling Instruments

The Inadequate Core Cooling Monitor (ICCM) is of Westinghouse design. The ICCM system monitors hotleg level, reactor vessel head level, loop subcooling margin, core subcooling margin and core exit temperature and provides advanced warning of the approach to inadequate core cooling. The ICCM is a redundant two train Nuclear Safety-Related system powered by the vital instrumentation and control power system.

The microprocessor-based monitoring trains provide essential information to the control room operator so that conditions inherent to or leading to Inadequate Core Cooling (ICC) can be recognized and addressed.

The functions performed by the ICCM are as follows:

1. Assists in detecting a void or loss of level in the hotleg during natural circulation.
2. Indicates loss of subcooling margin.
3. Assists in detecting presence of a gas bubble or void in the reactor vessel head.
4. Assists in the detection of the approach to inadequate core cooling.

The ICCM system consists, on a per train basis of centrally located electronics/microprocessor cabinet, display electronics package, display selector key pad, and the plasma display unit on the main control board.

A description of each of the process sub-systems are described as follows.

7.5.2.2.1 Core Exit Temperature

There may be up to 52 Core Exit Thermocouples (CETs) per Oconee Unit. Twenty-four (12 per train) have been upgraded for accident monitoring and to meet seismic and environmental qualification requirements.

The plant computer is the primary display for up to 47 CETs of the 52. 5 CETs are displayed on the corresponding SSF unit console. The ICCM plasma displays (1 per train) located in the Control Room serve as safety related backup displays for the twenty-four nuclear safety qualified CETs. The range of the readouts is 50°F to 2300°F.

The ICCM CET function uses inputs from twelve incore thermocouples per train to calculate and display temperatures of the reactor coolant as it exits the core and to provide indication of thermal conditions across the core at the core exit.

Each of the twelve qualified thermocouples per train is displayed on a spatially oriented core map on the plasma display. The distribution of the monitored CETs in both trains assure minimum monitoring of at least four per core quadrant. Trending of CET temperature is available continuously on the plasma display. The average of the five hottest CETs is trendable for the past forty minutes.

Inputs to the plant computer for thermocouples used in the ICCM backup display is through qualified isolation devices. Power for the backup display is from safety grade emergency power sources, and power for the non-safety Operator Aid Computer (OAC) portion is from a highly reliable battery backed control bus. The plant computer and ICCM backup display are installed in a mild environment.

Core exit temperature is classified as a Type A Category 1 variable at Oconee because the operator relies on this information following a design basis event (LOCA) to secure HPI and throttle LPI, (SBLOCA) to throttle HPI and begin forced HPI cooling if needed, (MSLB, OTSG Tube Rupture) throttle HPI and isolate affected OTSG.

(RE: NSMs ON-1/2/32401)

7.5.2.2.2 Degrees of Subcooling Monitoring

The margin to saturation for the hotlegs and the reactor core are calculated from Reactor Coolant System (RCS) pressure and temperature measurements. The hotleg subcooling margin is calculated from wide range RCS pressure measurements and individual hotleg RTD temperature measurements. The hotleg subcooling margins are displayed in the Control Room on the ICCM plasma display unit. Train A displays the RCS Loop A hotleg subcooling margin while the Train B display provides RCS Loop B hotleg subcooling margin. Computer inputs are also provided for both hotlegs.

The reactor core subcooling margin is displayed in the Control Room in an identical manner. The core subcooling margin is calculated from the average of the five highest qualified Core Exit Thermocouples

(CET's) out of twelve inputs to each train of ICCM. This average value is then used with the RCS pressure measurement to calculate core subcooling margin.

The degrees of subcooling is also input to the plant computer through isolation buffers and is recorded on a recorder in the Control Room. The range of the degrees of subcooling readouts is 200°F subcooled to 50° superheat which envelopes the Regulatory Guide 1.97 range of 200°F subcooling to 35°F superheat.

Degrees of Subcooling Monitoring is classified as a Regulatory Guide 1.97, Rev. 2 Type A Category 1 variable at Oconee.

(RE: NSMs ON-1/2/32401)

7.5.2.2.3 Reactor Vessel Head and Hotleg Levels

The Reactor Vessel Head Level indicating system (RVHLIS) and Hotleg (HL) system are an adaptation of the Westinghouse RVLIS to the Babcock and Wilcox nuclear steam supply system. The HL and RVHLIS monitor the RCS for voids and loss of level conditions only under natural circulation.

The HL and RVHLIS uses two sets of two d/p (differential pressure) cells to measure both vessel and hot leg levels under natural circulation conditions. These cells are used to measure the pressure drop from the hot leg decay heat drop line connection to the top of the vessel, and from the hot leg decay heat drop line connection to the top of the candy cane on each hot leg. This differential pressure measuring system uses cells of differing ranges to cover natural circulation conditions.

This is a two train system containing Trains A and B which are physically separate and electrically isolated from each other. The trains perform the same function using identical but redundant inputs from differential pressure transmitters, impulse line temperature sensors, reactor coolant temperature sensors and wide range reactor coolant system pressure.

Software algorithms automatically perform compensation calculations required for variations in impulse line temperatures. Software also calculates and provides the necessary compensation for reactor coolant density.

Whenever the Reactor Coolant Pumps (RCPs) are running, the subcooling margin monitors and RCP monitor current meters are used to detect possible void conditions. Computer inputs are provided for both trains of level measurement. The Train A level measurements are recorded on a continuous recorder on the Main Control Board. The plasma displays for each train provide indication of both HL and RVHLIS in the Control Room.

Reactor Vessel Head and Hotleg Levels are classified as Regulatory Guide 1.97, Rev. 2 Type B Category 1 variables at Oconee.

7.5.2.3 Pressurizer Level

Two channels (2 level indications for Train “A” channel and 1 level indication for Train “B” channel)) of QA 1 instrumentation are provided for post accident monitoring the Pressurizer Level in response to Regulatory Guide 1.97, Revision 2. The indicated range is 0 to 400 inches which represents 11% to 84% level as a percentage of volume. Duke considers this range adequate for the intended monitoring function.

In order to determine the range or level that should be monitored for the pressurizer, it is important to understand how the pressurizer is sized and how the level taps are located. The pressurizer water volume is chosen such that the reactor coolant system can experience a reactor trip from full power without uncovering the level sensors in the lower shell and to maintain system pressure above the High Pressure Injection (HPI) system actuation setpoint. The steam volume is chosen such that the reactor coolant

system can experience a turbine trip without uncovering level sensors in the upper shell. Oconee has a 0 to 400 in range for pressurizer level based on these criteria. Although the installed range of instrumentation is not in complete compliance with the recommendation of Regulatory Guide 1.97, Revision 2, that pressurizer level be monitored from bottom to top, it is consistent with B&W NSSS requirements and is adequate for the intended monitoring function, including monitoring to ensure continued safe operation of pressurizer heaters.

The qualified instrument channels are powered by safety grade emergency power sources. Continuous recording is provided for one channel. The range for the instrumentation channels is 0 to 400 inches which Duke considers adequate for the intended monitoring function as referenced in the above paragraph.

Pressurizer level is classifed a Type A Category 1 variable at Oconee because the operator relies on this information following a design basis event (SBLOCA, OTSG Tube Rupture, MSLB) to throttle HPI.

(RE: NSMs ON-1/2/32448)

7.5.2.4 Steam Generator Level

Oconee has several different methods of Steam Generator level measurement and indication, as follows:

1. Start-up Range - Four transmitters (two per S/G) feed the ICS with signal ranges of 0" to 250". The four channels are used in the ICS for steam generator water level and feedwater control. The ICS employes median select between these signals and isolated signals from Item 4 below to control level and feedwater. The ICS displays the controlling level signal on a dual scale gage on the main control board.
2. Operate Range - Four transmitters (two per S/G) are combined with temperature compensation to feed two recorders with ranges of 0-100% (96"-388"). The four channels are switch selectable for feeding the recorders.
3. Full Range - Two transmitters (one per S/G) feed one dual gauge with ranges of 0 to 100% (0-650").
4. Extended Startup Range - Four transmitters (two per S/G) feed four gauges with ranges of 0" to 388".

Items 1 through 3 are used during normal plant operating conditions and are not required to meet Regulatory Guide 1.97, Type A, Category 1 Variable Requirements. These instruments may be used as backup verification for post accident monitoring to the extent they are available.

The instrumentation in Item 4 above is safety related and is used for post-accident monitoring. This instrumentation is powered by safety grade emergency power sources and the transmitters are seismically and environmentally qualified. Signal conditioning is provided by seismically and environmentally qualified equipment. Two transmitters, one per steam generator, provide electrically isolated level signals to the ICS for use in steam generator water level and feedwater control. The ICS will display these level signals if they have been selected for control on the control room indicator described in Item 1 above.

During accident conditions, the required range for a B&W once through steam generator is based on that level in the steam generator needed to recover from loss of subcooling margin conditions. The installed range of 0" to 388" ensures that the level required to restore subcooling margin as given in the emergency procedures can be measured.

Steam Generator Level is classified a Type A Category 1 variable at Oconee because the operator relies on this information following a design basis event (MSLB, OTSG Tube Rupture) to isolate affected OTSG.

(RE: NSMs ON-1/2/32447)

7.5.2.5 Steam Generator Pressure

Four QA Condition 1 channels, two channels per steam generator, are provided for post-accident monitoring steam generator outlet steam pressure in response to Regulatory Guide 1.97. Each instrument channel is seismically and environmentally qualified and powered from a safety grade source.

Each instrument channel inputs to the Inadequate Core Cooling Monitoring (ICCM) cabinets. The ICCM cabinets, Channel A and B respectively, provide safety inputs to two qualified indicators located on the Main Control Board in the Control Room. One channel per steam generator also provides an input to a recorder located in the Control Room. The ICCM system cabinets, channels A and B respectively, also provide non-safety inputs to the Operator Aid Computer (OAC). Safety train integrity is maintained by isolation buffers provided by the ICCM system cabinets. Additionally, each steam line has one QA Condition 1 channel of steam generator pressure instrumentation. These instrument channels along with corresponding ICCM steam generator instrumentation provide input signals into the Automatic Feedwater Isolation System (RE: NSM-ON-1/2/33053).

Each steam generator has two non-safety related channels of steam generator outlet pressure instrumentation (total of four) used for control by the ICS. In addition, two channels of QA-1 steam generator outlet pressure instrumentation used in the Automatic Feedwater Isolation System (AFIS) logic are electrically isolated and provided to the ICS for control. This makes a total of six pressure signals, three per steam generator, for use in the ICS for control. Each group of three pressure signals (3 - OTSG "A", 3 - OTSG "B") are used in median select strategy by the ICS for control. The control signal used in the ICS for each steam generator is provided for indication on the main control board. The indicated range is 0 - 1200 psig which corresponds to 14% above the lowest main steam safety relief valve setting and 8% above the highest safety valve setting. An additional channel of QA-steam generator outlet pressure instrumentation on each header is used in AFIS. All eight signals, four per steam generator, are also input to the plant computer (OAC) and trend recording is available to the control room operator if demanded. The non-safety related instrumentation is powered from highly reliable battery backed buses. The safety-related (QA-1) instrumentation is powered from the QA-1 vital instrumentation and control battery backed buses.

The main steam lines are provided with safety relief valves, atmospheric dump valves and condenser dump valves to prevent over pressurization of the lines as well as pressure control. Operability of the main steam safety valves ensures that the secondary system pressure will be limited to within its design pressure (1050 psig) during the most severe anticipated system operating transient. With an assumed 3% accumulation when these safety valves are operating, the maximum pressure while they are relieving will be less than 10% above design pressure. Also the Facility Operating License limit the plant power and thus steam flow in order to maintain that excess relief capacity. Therefore, based on the facts that the, highest safety valve setting is 1104 psig, the steam relief capacity is 17% above the expected steam flow rate and that excess relief capacity is maintained when safety valves are inoperable, the existing range of 0 to 1200 psig is sufficient for this variable.

Steam Generator Pressure is classified a Type A Category 1 variable at Oconee because the operator relies on this information following a design basis event (MSLB, OTSG Tube Rupture) to isolate affected OTSG.

(RE: NSMs ON-1/2/32447)

7.5.2.6 Borated Water Storage Tank Level

Three QA Condition 1 channels of level instrumentation are provided for normal and post accident monitoring the Borated Water Storage Tank (BWST) level. Each channel is seismically qualified. Two channels are powered from a safety grade source and the third channel has a safety and a non-safety grade power distribution. Signals to the Control Board are processed through the Inadequate Core Cooling

Monitoring (ICCM) system cabinets. The range for the readouts, 0 to 50 ft (13%-100% of volume), is in compliance with Regulatory Guide 1.97, Rev. 2.

Two of the three QA Condition 1 instrumentation channels provide inputs to the ICCM system cabinets, Train A and B respectively. The ICCM cabinets provides safety inputs to qualified indicators on the Control Board and non-safety inputs to the Operator Aid Computer (OAC). Safety train integrity is maintained through the use of isolation buffers provided by the ICCM system.

The third channel of qualified instrumentation provides a safety input from train B to a recorder (through a qualified isolator). This channel also provides input to the computer and various annunciators via an optical isolator which maintains safety train B integrity.

BWST level is classified a Type A Category 1 variable at Oconee because the operator relies on this information following a design basis event (LOCA, SB LOCA) to realign LPI to take suction from RB sump.

(RE: NSMs ON-1/2/32450)

7.5.2.7 High Pressure Injection System and Crossover Flows

Two channels of QA condition 1 instrumentation are provided for post accident monitoring of High Pressure Injection (HPI) flow in response to Regulatory Guide 1.97. Each channel is seismically and environmentally qualified and powered from a safety grade source. Each channel signal, A and B respectively, inputs to a recorder and qualified indicator via the Inadequate Core Cooling Monitoring (ICCM) system cabinets. Two channels of QA condition 1 instrumentation are also provided for monitoring HPI crossover flow. These instrument channel signals directly input to qualified indicators on the Control Board. HPI System and Crossover Flow instrumentation channels monitor flow over the range 0 - 750 gpm which envelopes the 0 to 110% design flow criteria of Regulatory Guide 1.97, Rev. 2.

The ICCM cabinets also provide non-safety inputs to the Operator Aid Computer (OAC) and annunciator points. Safety channel integrity is maintained through the use of isolation buffers provided in the ICCM.

HPI System flow is a Type A Category 1 variable at Oconee because the operator relies on this information following a design basis event (LOCA, SB LOCA, MSLP, OTSG Tube Rupture) to throttle HPI and initiate HPI bypass (if necessary).

(RE: NSMs ON-1/2/32589)

7.5.2.8 Low Pressure Injection System Flow

Two QA Condition 1 instrumentation channels are provided for normal and post accident monitoring Low Pressure Injection (LPI) flow in response to Regulatory Guide 1.97. Each channel is seismically and environmentally qualified and powered from a safety grade source. Each channel signal, train A and B respectively, inputs to a qualified indicator and a recorder via the Inadequate Core Cooling Monitoring (ICCM) system cabinets. These channels monitor LPI flow over the range 0-4000 gpm which envelopes the 0-110% of design flow criteria for Regulatory Guide 1.97.

The ICCM cabinets also provide non-safety inputs to the Operator Aid Computer (OAC) and annunciator points. Alarms generated in the ICCM cabinets provide high and low LPI flow and low Decay Heat removal flow for each train. Safety train integrity is maintained through the use of isolation buffers provided by the ICCM. Two non-qualified transmitters, one per train, also provide non-safety inputs to the OAC.

LPI System is a Type A Category 1 variable at Oconee because the operator relies on this information following a design basis event (LOCA, SB LOCA) to terminate HPI flow.

(RE: NSMs ON-1/2/32587)

(RE: NSMs ON-1/2/33093)

7.5.2.9 Reactor Building Spray Flow

Two QA Condition 1 instrumentation channels are provided for post accident monitoring Reactor Building Spray flow in response to Regulatory Guide 1.97. Each instrumentation channel is seismically and environmentally qualified and powered from a safety grade source. Each instrument channel signal, train A and B respectively, inputs to a qualified indicator and a recorder via the inadequate core cooling monitoring (ICCM) cabinets. These channels monitor Reactor Building Spray flow over the range 0-1500 gpm which envelopes the Regulatory Guide 1.97 range requirement of 0-110% of design flow.

The ICCM cabinets also provide non-safety inputs to the Operator Aid Computer (OAC), annunciator, and a non-safety indicator located in the Control Room. Safety train integrity is maintained through the use of isolation buffers provided by the ICCM system. Also provided is two non-safety instrument channels which provide non-safety inputs to the OAC.

For all units at Oconee, throttling is not required, and the RBS flow variable is classified as Type D Category 1 for indication of continued operation of the RBS system to support long term cooling requirements and iodine removal. However, this instrument is only required to meet Category 2 requirements.

(RE: NSMs ON-1/2/32588 and ON-1/2/33105)

7.5.2.10 Reactor Building Hydrogen Concentration

Two redundant channels of nuclear safety related instrumentation monitor reactor building hydrogen concentration. The reactor building hydrogen monitoring system meets the requirements of NUREG 0737, Item II.F.1.6, and is described in more detail in Section 9.3.7 of the UFSAR. The indicated range is from 0 to 10% concentration which envelopes the Regulatory Guide 1.97 range requirements.

Both channels are powered by safety grade emergency buses. Control of the sample line switching valves and sample selector solenoid valves is accomplished at the analyzer remote control panel. These instruments are seismically and environmentally qualified.

Reactor Building Hydrogen Concentration is classified as a Regulatory Guide 1.97, Rev. 2 Type E Category 3 variable at Oconee.

7.5.2.11 Upper Surge Tank and Hotwell Level

Oconee's Emergency Feedwater System (EFDW) draws condensate grade suction primarily from the Upper Surge Tanks and supplementarily from the Condenser Hotwell. Condensate may also be provided from the Condensate Storage Tank (CST) and the Makeup Demineralizers. Additional backup of the two normal condensate sources is provided by these same locations associated with the other two units. The level transmitters which monitor Upper Surge Tank and Hotwell level are located in the Turbine building which is a mild environment.

Instrumentation is available to monitor Hotwell level in the Control Room. The plant computer system is provided to display both current and past values of this variable. Hotwell level is not calssified as a Regulatory Guide 1.97 variable at Oconee.

Two QA Condition 1 instrumentation channels are provided for monitoring Upper Surge Tank (UST) level in response to Regulatory Guide 1.97. These instrument channels are seismically qualified and powered from a safety grade source. Each instrument channel, train A and B respectively, input to the Inadequate Core Cooling Monitoring (ICCM) system cabinets. The ICCM Train A cabinet provides safety inputs to a qualified indicator and to a recorder (through a qualified isolator), both located in the

Control Room to provide UST level indication. The ICCM Train B cabinet also provides a safety input to a qualified indicator located in the Control Room. The range of UST level indication is 0 - 12 feet.

The ICCM cabinets, Train A and B respectively, also provide non-safety inputs to two computer alarm points and one annunciator window. Safety train integrity is maintained through the use of isolation buffers provided by the ICCM system.

Upper Surge Tank level is a Type A Category 1 variable at Oconee because the operator relies on this information following a design basis event.

(RE: NSMs ON-1/2/32449)

7.5.2.12 Neutron Flux

Oconee has four channels of neutron flux for the source range, and four wide range QA Condition 1 channels of full range neutron flux instrumentation which are environmentally qualified for post-accident monitoring. Four neutron flux channels exist for the power range. The indicated ranges are: Source Range 10^{-1} to 10^{5} cps, -1.0 to +7.0 decade/min. rate of change; Wide range (Post-Accident Monitoring channels) 10^{-8} to 200% power, -1 to +7 decade/min. rate of change; and Power Range, 0 to 125%.

NI-1,-2,-3, and -4 channels are environmentally qualified and powered from safety grade busses and encompass the 10^{-6} to 100% Full Power range in response to Regulatory Guide 1.97, Rev. 2. NI-1, -2, -3, and -4 channels are Type B Category 1 variables at Oconee. All other NI channels are designed for the normal Reactor Building Environment for the safety function of overpower reactor trip but they are not environmentally qualified for post-accident operation.

Operator information is provided as follows:

1. Twelve Control Room indicators (Four source, four wide, four power)
2. Twenty computer points (Eight source, eight wide range, and four power)
3. Trend recording on demand
4. One QA Condition 1 Wide Range channel recorded on a recorder. One source range, wide range, and power range channel recorded, four (two power range) channels accessible on a Non-QA Condition recorder.

(RE: NSMs ON-1/2/32596 and 1/2/32909)

7.5.2.13 Control Rod Position

Each control rod's position is indicated on an analog display which has two switchable input modes for the full 0 to 139 inch range. In addition, separate Full In and Full Out indicating lights are provided for each control rod. Analog computer points are provided for each control rod's position. Analog computer points are also provided for control rod groups 5, 6, 7 and 8, for zero to 100% rod position corresponding to the full 0 to 139 inch range. This instrumentation is powered from a highly reliable battery backed source. Control Rod Position is classified as a Regulatory Guide 1.97, Rev. 2 Type B Category 3 variable at Oconee. (Re: FSAR 4.5.3).

Operator information is provided as follows:

1. Indicating lights for Full In or Not Full In for all control rods.
2. Analog display full range for all control rods.
3. Computer inputs for all control rods and all control rod groups 5, 6, 7, and 8. Trend recording on demand.

7.5.2.14 RCS Soluble Boron Concentration

This variable is monitored by sampling and laboratory analysis. Primary system boron concentration is controlled manually with the sampling frequency determined by plant conditions and operating procedures.

7.5.2.15 Reactor Coolant System Cold Leg Water Temperature

Oconee has indication of Reactor Coolant System (RCS) Cold Leg Temperature for each of the four cold legs. The instrumentation is powered from a highly reliable battery backed source. The indicated range is 50° to 650°F. Additional diversity is provided by the Hot Leg Water Temperature and Core Exit Temperature Instruments.

The RCS Cold Leg Water Temperature is used as a backup for the key variable of Hot Leg Temperature and Core Exit Temperature. Because the Hot Leg and Cold Leg RTD's are located in the RCS loops and not in the reactor vessel, either forced or natural circulation is required through the steam generators for their indication to be representative of actual core conditions. When circulation is present, the 650°F high end of the range provides 18% excess measurement capability based on a steam generator design pressure of 1050 psig and a saturation temperature of approximately 553°F for the Oconee design. Because the RCS Cold Leg Temperature is not used in the ATOG guidelines and functions as backup to the other two variables, it is appropriate to classify this variable as a Type B Category 3. The existing design is adequate for the intended monitoring function.

7.5.2.16 Reactor Coolant System (RCS) Hot Leg Water Temperature

Two qualified, QA condition 1 channels, are provided for post-accident monitoring Wide Range RCS Hotleg Water Temperature in response to Regulatory Guide 1.97 Rev. 2. These instrument channels are powered from safety grade emergency power sources. The indication readouts are located in the Control Room in a mild environment. This variable inputs to the plant computer through isolation buffers and is recorded on a recorder in the Control Room. (RE: NSMs ON-1/2/32401). The range of the readouts is 50 to 700°F which Duke considers adequate for the intended monitoring function. Also note, this range is in compliance with the recommendations of Revision 3 to RG 1.97. Control room display is through the inadequate Core Cooling Monitoring system. RCS Hot Leg Water Temperature is classified as a Regulatory Guide 1.97, Rev 2 Type A Category 1 variable at Oconee.

7.5.2.17 Reactor Building Sump Water Level Narrow Range

Two channels of instrumentation monitor both the Normal Sump Level (0 to 2 feet, approximately 350 gallons excluding embedded piping) and the Emergency Sump Level (0 to 3 feet, approximately 4000 gallons). This instrumentation is environmentally qualified and powered from safety grade emergency power buses. Qualified backup indication is provided by the Wide Range Sump Level instrumentation. Reactor Building Sump Water Level Narrow Range is classified as a Regulatory Guide 1.97, Rev. 2 Type B Category 2 variable at Oconee and, with the Reactor Building Sump Water Level instrument in Section 7.5.2.18 below, meets the requirements of NUREG 0737, Item II.F.1.5 as described in Section 5.2.3.10.5 of the UFSAR.

(Re: FSAR 3.4.1.1.2).

(RE: NSM ON-2248)

7.5.2.18 Reactor Building Sump Water Level

Two redundant QA Condition 1 channels of level instrumentation are provided for measuring reactor building sump water level from the bottom of the Reactor Building to approximately five feet above the

maximum flood elevation which exceeds the 600,000 gallon level. The indicated range is 0 to 15 feet. Redundancy/diversity is provided by the Borated Water Storage Tank Level and the Narrow Range Sump Level indicators. The instrumentation channels are environmentally and seismically qualified and powered by safety grade emergency power buses. Reactor Building Sump Water level is classified as a Regulatory Guide 1.97, Rev. 2 Type B Category 1 variable at Oconee and, with the Reactor Building Sump Water Level Narrow Range instrument described in Section 7.5.2.17 above, meets the requirements of NUREG 0737, Item II.F.1.5 as described in Section 5.2.3.10.5 of the UFSAR.

(Re: FSAR 3.4.1.1.2).

7.5.2.19 Reactor Building Pressure

Two redundant QA Condition 1 channels of instrumentation are provided for monitoring Reactor Building Pressure in accordance with the requirements of NUREG 0737, Item II.F.1.4. The instrumentation channels are environmentally and seismically qualified and powered by safety grade emergency power buses. The indicated range is -5 to 175 psig with the reactor building design pressure being 59 psig. This instrumentation range covers nearly 99% of the recommended Regulatory Guide 1.97, Revision 2, range of 10 psig to 3 times the design pressure (177 psig). Duke considers the indicated range adequate for the intended accident monitoring function. Reactor Building Pressure is classified as a Regulatory Guide 1.97, Rev. 2 Type B Category 1 variable at Oconee.

7.5.2.20 Reactor Building Isolation Valve Position

All electrically controlled reactor building isolation valves that are active to close for containment isolation have control switches on the main control boards. Actual valve position is provided by QA Condition 1 limit switches on the valves which operate both Closed-Not Closed, and Open-Not Open control switch indicating lights. These valves are powered by safety grade emergency power buses. Additional indication is provided by the computer. Redundancy is not necessary on a per valve basis since redundant barriers are provided for all fluid penetrations as discussed in the Oconee FSAR Section 6.2.3.2. Environmental qualification of the limit switches is described in the Oconee FSAR section 3.10 and the Oconee Nuclear Station Seismic Design Criteria (OSDC-0193.01-00-00001). Reactor Building Isolation Valve Position is classified as a Regulatory Guide 1.97, Rev. 2 Type B Category 1 variable at Oconee.

7.5.2.21 Radiation Level in Primary Coolant

Oconee has one channel of primary coolant radiation level instrumentation which monitors the Reactor Coolant and Letdown Line and is isolated upon ESF actuation signal. The channel is powered from a highly reliable battery backed bus. The indicated range is 10^{1} to 10^{6} counts per minute which covers reactor coolant concentration of approximately 10^{-3} uCi/ml to 10^{3} uCi/ml (see the Oconee FSAR, Section 11.5).

Deleted paragraph(s) per 2005 update

7.5.2.22 Accident Sampling Capability, Primary Coolant, Primary Coolant Sump, Containment Air

The existing design of the sampling system for the primary coolant, the Reactor Building sump and Reactor Building air allows samples to be taken for laboratory analysis. Samples from other plant systems including various auxiliary building sumps can be obtained from sample points on system piping and/or storage tanks.

Deleted paragraph(s) per 2005 update

7.5.2.23 Reactor Building Area Radiation - High Range

Oconee has two redundant QA Condition 1 channels of Reactor Building high range radiation monitoring instrumentation. Each channel is powered by safety grade emergency power. The indicated range is 1 to 10^8 R/hr. Diversity is provided by portable instrumentation or by sampling and analysis. The instrumentation is seismically and environmentally qualified. Reactor Building high range radiation monitoring instrumentation is classified as a Regulatory Guide 1.97, Rev. 2 Type C Category 1 variable at Oconee.

7.5.2.24 Airborne Process Radiation Monitors

Airborne process radiation monitors exist for monitoring ventilation exhausts and the condenser air ejector exhaust (see Oconee FSAR, Section 11.5 and Table 11-7). However, in accordance with RG 1.97, Rev. 2 these individual airborne process radiation monitors are not required for accident monitoring due to the fact that ventilation systems and the condenser air ejector exhaust to the common unit vent (See Oconee FSAR, Section 7.5.2.52).

7.5.2.25 Area Radiation

Oconee has an extensive Area Radiation Monitoring System installed for personnel protection. Channel detector locations were selected based on areas normally having free access and low radiation dose rates with the potential of having abnormal radiation levels. These channels have an indicated range of 10^{-1} to 10^7 mr/hr. Redundant indication can be provided by portable instrumentation. The channels are powered by a highly reliable non load shed power bus capable of receiving power from the on-site emergency power sources. See the Oconee FSAR, Section 12.3.3.

The environmental qualification of some of the instrumentation is not in compliance with the recommendations of Regulatory Guide 1.97, Revision 2. However, the qualification is within the guidance provided for Type C Category 3 instrumentation which Duke considers adequate for the intended monitoring function. Also note, this is in compliance with the recommendations of RG 1.97, Rev. 3. Continuous recording is not required for the intended monitoring function.

7.5.2.26 Decay Heat Cooler Discharge Temperature

Each train of the Oconee LPI system contains instrumentation to monitor decay heat cooler discharge temperature which is referred to in Regulatory Guide 1.97, Revision 2, as RHR Heat Exchanger Outlet Temperature. The range for this instrumentation is 0 to 400°F, and the power supply is a highly reliable battery backed control bus. Each train is environmentally qualified per the IEB-79-01B submittal methodology and envelopes the Regulatory Guide 1.97, Rev. 2 range of 32° to 350°F. Decay Heat Cooler Discharge Temperature is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 2 variable at Oconee.

7.5.2.27 Core Flood Tank Level

Oconee has two channels of tank level instrumentation on each of the two core flood tanks. Power for these channels is provided by highly reliable battery backed buses. The indicated range for Units 1, 2 and 3 is 1.5 to 14 feet which corresponds to approximately 22% to 83% of the core flood tank volume. The equipment is located in a harsh environment.

The range and environmental qualification of this instrumentation is not in total compliance with the recommendations of RG 1.97, Rev. 2, which recommends a range of 10% to 90% volume and Category 2 classification.

The primary function of this instrumentation is to monitor the pre-accident status of the core flood tanks to assure that this passive safety system is prepared to serve its safety function. The indicated range envelopes the Technical Specification level requirements and Duke Power considers the range adequate to meet the intended monitoring function. This instrumentation plays no significant role in the subsequent management of an accident. Therefore, Core Flood Tank Level is not a key variable for accident monitoring and is considered to be Type D Category 3 instrumentation. The level of environmental qualification provided for the instrumentation in this system is consistent with the performance expectations of the system and meets the recommendations of Type D Category 3 in Duke's interpretation of RG 1.97, Rev. 2.

7.5.2.28 Core Flood Tank Pressure

Oconee has two channels of core flood tank pressure instrumentation on each of the two core flood tanks. Power for these channels is provided by highly reliable battery backed buses. The indicated range is 0 to 700 psig. The tanks are pressurized to 600 psig under normal operating conditions.

The primary function of this instrumentation is to monitor the pre-accident status of core flood tanks to assure that this passive safety system is prepared to serve its safety function. This instrumentation plays no significant role in the subsequent management of an accident. Therefore, Core Flood Tank Pressure is not a key variable for accident monitoring and is considered to be Category 3 instrumentation. The installed system meets the Duke interpretation of Type D Category 3 recommendations. Regulatory Guide 1.97, Revision 2, classifies this variable as Category 2.

The range of this instrumentation is not in total compliance with the recommended 0 to 750 psig range of Regulatory Guide 1.97, Revision 2. However, the indicated range covers approximately 0 to 117% of the operating pressure of the tanks. Because the purpose of this variable is to monitor and maintain Core Flood Tank pressure during normal operation to Technical Specification (TS) limits, the range of this variable should provide some margin above that TS limit. Since the Oconee TS limit is 600 ± 25 psig, a high range value of about 700 psig will provide greater than 10% excess range measurement capability and will therefore be sufficient. Duke Power considers the instrumentation adequate for the intended monitoring function.

7.5.2.29 Core Flood Tank Isolation Valve Position

The core flood tank isolation valves are provided with control switches on the main control board. During normal plant operation, power is removed from the valve operators to prevent a spurious signal from inadvertently closing the valves. The indicating lights are powered from a separate highly reliable battery backed bus and give actual valve position of both Closed-Not Closed and Open-Not Open. Environmentally qualified limit switches are provided for the core flood tank isolation valves.

Core Flood Tank Isolation Valve Position is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 2 variable at Oconee.

7.5.2.30 Boric Acid Charging Flow

Oconee NSSS does not include a charging system as part of the Emergency Core Cooling System (ECCS). Flow paths from the ECCS to the RCS include high pressure injection (HPI) and low pressure injection (LPI) with the BWST or the RB Sump as the suction source, and the Core Flood Tank injection. HPI and LPI flow rates are monitored, and BWST, Reactor Building Sump, and Core Flood Tank levels are monitored by RG 1.97 variables. Therefore, Boric Acid Charging Flow monitoring is not applicable to the operation of the ECCS and is not a Type D variable for Oconee.

7.5.2.31 Reactor Coolant Pump Status

The indicated range for RCP motor current is from 0 to 1200 amps. The instrumentation derives power from the monitored source and is adequate for the intended monitoring function. The RCP motor current instrumentation is classified as a Regulatory Guide 1.97, Rev. 2 Type D Categroy 3 variable at Oconee.

7.5.2.32 Power Operated Relief Valves Status

An acoustical leak detection monitoring system is the primary instrumentation for determining PORV position. It is a single channel system powered from a highly reliable battery backed bus. It provides the operator with positive indication of valve position by indicating fractional flow through the valve in ten steps from 0.01 to 1.0. Backup indication of PORV position is provided by limit switch operated indicating lights and PORV outlet temperature indication. The system was specified and is rated to operate in all environmental conditions for its location. Power Operated Relief Valves status is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 2 variable at Oconee.

(RE: NSMs ON-1/2/32594)

7.5.2.33 Primary System Safety Relief Valve Positions (Code Valves)

Acoustical leak detection monitoring systems are the primary instrumentation for determining code valves position. Each code valve has a single channel system powered from highly reliable battery backed bus. It provides the operator with positive indication of valve position by indicating fractional flow through the valve in ten steps from 0.01 to 1.0. Backup indication of code valve position is provided by valve outlet temperature indication. The system was specified, and is rated to operate in all environmental conditions for its location. Primary System Safety Relief Valve Position is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 2 variable at Oconee.

(RE: NSMs ON-1/2/32594)

7.5.2.34 Pressurizer Heater Status

Control indicating lights are used for indication of the ON/OFF status of the pressurizer heater groups. Indicating lights are powered by highly reliable battery backed busses. This monitoring instrumentation is located in a mild environment.

ON/OFF status of the pressurizer heaters provides the operator adequate information for Design Basis events. Additionally, RCS pressure can be monitored to determine the effectiveness of the heaters to maintain system pressure. Duke feels that this is adequate for the intended monitoring function, and that monitoring of electric current per Regulatory Guide 1.97, Revision 2, recommendations is not necessary. Pressurizer Heater status is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 2 variable at Oconee.

7.5.2.35 Quench Tank Level

The indicated range of Quench Tank Level is from 0 to 125" corresponding to tank volume of approximately 15-96%. This range is not in complete compliance with RG 1.97, Rev. 2, which recommended top to bottom tank monitoring, however, the upper range meets the intended monitoring function. No useful information would be gained by measuring tank volume from 0-15%. Normal level (pre-accident) is maintained above 15% and post-accident condition will only increase tank level. Therefore, the existing range is adequate for the intended monitoring function. Quench Tank Level is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 3 variable at Oconee.

7.5.2.36 Quench Tank Temperature

The indicated range of the Quench Tank temperature is from 50° to 350°F. The design temperature of the Quench Tank is 300°F which is approximately the maximum temperature reached in the tank during a design transient. The tank design pressure is 55 psig, and the rupture disc pressure is 55 psig. The saturation temperature for 55 psig is approximately 300°F. Thus, the indicated range of 50°F to 350°F will adequately measure the expected maximum temperature as well as saturation temperature for the Quench Tank. Quench Tank Temperature is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 3 variable at Oconee.

(RE: NSMs ON-1/2/32593)

7.5.2.37 Quench Tank Pressure

The indicated range of the Quench Tank pressure is from 0 to 60 psig. The tank rupture disc is designed to relieve at 55 psig, and the tank design pressure is 55 psig. Therefore, the installed instrumentation is adequate for the intended monitoring function. Quench Tank Pressure is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 3 variable at Oconee.

7.5.2.38 Main Steam Safety Valve Position

This variable is not monitored directly. The positions of the Main Steam Safety Valves (MSSV) are not required to mitigate the consequences of a design basis accident. Direct indication of safety valve position is not provided but indirect indication is provided via control room indication of steam generator pressure. During Duke's Control Room Design Review, a specific Task Analysis Evaluation of MSSV indication was undertaken. This evaluation dealt with steam leak transients with and without MSSV indication. As a result of this evaluation, direct MSSV indication was found not necessary. Also, sound emitted from the valves provides an audible indication to the operators when the valves lift. Duke feels that this is adequate indication for the intended monitoring function.

7.5.2.39 Main Feedwater Flow

Each feedwater line has three main feedwater flow transmitters. The indicated range for this variable is 0 to 6.0×10^6 lbs/HR which corresponds to 0 to 111% of design flow. Main Feedwater Flow is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 3 variable at Oconee.

7.5.2.40 Emergency Feedwater Flow

Oconee has four QA Condition 1 flow transmitters, two per steam generator monitoring Emergency Feedwater Flow from all EFDW pumps to each steam generator. The indicated range for this variable is 0 to 1200 GPM which corresponds to a range of 0 to 115% design flow. This instrumentation is powered from a safety grade emergency power source. The flow transmitters are located in a mild environment. Seismic qualification methodology for these transmitters is as described in the Oconee FSAR, Section 3.10. The indicators are located in the control room which is classified as a mild environment. Emergency Feedwater flow to each steam generator is recorded on separate recorders in the Control Room. Emergency Feedwater Flow is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 1 variable at Oconee.

7.5.2.41 Reactor Building Fan Heat Removal

The key variable for monitoring Reactor Building Cooler performance is Reactor Building Pressure instrumentation which is Type B Category 1. Backup instrumentation includes Nuclear Safety Related indication of each Reactor Building Cooler Fan motor starter status (high and low speed lights), each Fan motor starter status on the computer, indication of each Fan motor amperage, indication of inlet and outlet

cooling water flow to each cooler, and inlet and outlet air temperature indication for each cooler. All of the above indications are provided in the Control Room. The installed instrumentation is adequate for the intended monitoring functions. For backup indications, the level of environmental qualification provided for the instrumentation is consistent with the performance expectations of the instrumentation and meets the recommendations of Type D Category 3 in Duke's interpretation of RG 1.97, Rev. 2.

7.5.2.42 Reactor Building Air Temperature

Thirteen dual element thermocouples are provided to measure Reactor Building air temperature on Units 1 & 2. Twelve dual element thermocouples are provided on Unit 3. One element of each T/C provides an input to the plant computer and the second element of each T/C, except for Unit 2, provides an input to a multi-channel recorder. On Units 1 and 3, the T/C input into the recorders is retransmitted to the OAC via an analog output card on board the recorders. Unit 2, for the present sends both T/C elements directly to the OAC. The plant computer and the recorders display a range of 0 to 400°F. The plant computer is powered by highly reliable battery backed busses.

The displayed ranges are adequate for the intended monitoring function. The worst case DBA temperature in the Reactor Building is 286°F. For accidents in which harsh RB environments are a result, pressure and temperature are coupled such that as RB pressure is reduced the temperature is also reduced. Therefore, RB pressure is considered the priority variable with temperature as a Category 3 backup variable. The level of environmental qualification provided for this instrumentation is consistent with its performance expectations and meets the recommendations of Type D Category 3 in Duke's interpretation of RG 1.97, Rev. 2.

7.5.2.43 Makeup Flow

The existing instrumentation for this variable provides continuous monitoring of reactor coolant makeup flow. The loop range is 0 to 160 gallons per minute which encompasses the Regulatory Guide 1.97, Rev.2 criteria of 0-110% of design flow. Design flow is 35 GPM. The instrumentation is located in a mild temperature environment.

The transmitter for this variable is not rated to withstand the anticipated maximum design basis accident radiation dose for the installed location. The installed instrumentation is adequate for the intended monitoring function. For accidents in which harsh environments are a result, the portion of the system containing this instrumentation is not required for the mitigation of these accidents and is automatically bypassed upon an ESF Actuation. Therefore, Makeup Flow is not a key variable for accident monitoring and is considered to be Category 3, instrumentation. The level of environmental qualification provided for the instrumentation in this system is consistent with the performance expectations of the system and meets the recommendations of Type D Category 3 in Duke's interpretation of RG 1.97, Rev. 2.

7.5.2.44 Letdown Flow

The existing instrumentation for this variable provides continuous monitoring of reactor coolant letdown flow. The loop range is 0 to 160 gallons per minute which envelopes the Regulatory Guide 1.97, Rev. 2 criteria of 0-110% of design flow. Design flow is 70 GPM. This instrument loop is powered from a highly reliable battery backed bus. The instrumentation is located in a mild temperature environment.

The transmitter for this variable is not rated to withstand the anticipated maximum design basis accident radiation dose for the installed location.

The installed instrumentation is adequate for the intended monitoring function. For accidents in which harsh environments are a result, the portion of the system containing this instrumentation is not required for the mitigation of these accidents and is automatically isolated upon an ESF Actuation. Therefore, Letdown Flow is not a key variable for accident monitoring and is considered to be Category 3

instrumentation. The level of environmental qualification provided for the instrumentation in this system is consistent with the performance expectations of the system and meets the recommendations of Type D Category 3 in Duke's interpretation of RG 1.97, Rev. 2.

7.5.2.45 Letdown Storage Tank Level

The existing instrumentation for this variable provides continuous monitoring of the letdown storage tank level. The loop range is 0 to 100 inches which covers the linear portion of the tank (approximately 16 to 84% of tank volume). This instrument loop is powered from a highly reliable battery backed bus. This instrumentation is located in a mild environment.

Minimum and maximum letdown storage tank levels are maintained within the range of the instrument. Extending the range into the domed portions of this tank would result in nonlinear readings at each extreme of the scale. The installed range is adequate for measuring letdown storage tank level. The installed instrumentation is adequate for the intended monitoring function. This tank is not required to be utilized during an accident. As a commitment to the NRC, Duke is voluntarily upgrading this LDST level instrumentation to Type D Category 2 Nuclear Safety Related (QA-1). This change was performed on Unit 3 during the 3EOC17 refueling outage, and will be implemented on the other units in subsequent outages. This upgraded instrumentation is also adequate to perform the intended monitoring function. (Ref NSM x-2885)

7.5.2.46 Low Pressure Service Water Temperature to ESF System

The Oconee system for providing cooling water to ESF components is the Low Pressure Service Water System (LPSW). The temperature of LPSW is essentially the same as the temperature of Lake Keowee at the CCW pump suction. There is no control over the temperature of the LPSW; therefore, there is no need to indicate the LPSW temperature in the control room since no operator action is taken based on this temperature and, by design, no useful information would be provided to the operator by such instrumentation.

7.5.2.47 Low Pressure Service Water Flow to ESF Systems (Pressure)

The Oconee system for providing cooling water to ESF components is the Low Pressure Service Water System (LPSW). Primary indication of proper LPSW system and pump operation is line pressure measured in each of the two LPSW headers. The indicated range is 0 to 100 psig for a system design pressure of 100 psig. These instruments are located in a mild environment and powered by a highly reliable battery backed source which meets Type D Category 2 requirements. LPSW header pressure is a valid measurement of system and pump operation and Duke considers the existing indications to meet the intent of Regulatory Guide 1.97, Rev. 2.

Additional instrument loops provide backup indication in the Control Room of proper system operation. These include LPSW pump motor amperage, valve position indication on valves operated in the control room, inlet and/or outlet cooling water flow for certain ESF coolers, and flow and pressure alarms. For backup variables, a design qualification of Type D Category 3 is adequate for the intended monitoring functions and consistent with the performance expectations of the instrumentation.

(RE: NSMs ON-1/32590)

7.5.2.48 RC Bleed Holdup Tank Level

The indicated range for this variable is 0 to 180 inches for the RC Bleed Holdup tank. This level indication corresponds to a tank volume of approximately 1% to 99%. Although the range is not in complete compliance with the recommendation for a RG 1.97, Rev. 2 Type D Category 3 variable (top to bottom), the tap to tap range of the installed instruments is adequate to provide tank level information for

all design basis events. Duke considers the installed instrumentation adequate for the intended monitoring function.

7.5.2.49 Waste Gas Decay Tank Pressure

Oconee utilizes two tanks per unit for radioactive waste gas storage. The maximum operating pressure for these tanks is approximately 100 psig (per Oconee FSAR, Section 11.3). The indicated range is 0 to 150 psig for each tank, which is adequate for the intended monitoring function. Waste Gas Decay Tank Pressure is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 3 variable at Oconee.

7.5.2.50 Emergency Ventilation Valve Position

There are three Emergency Ventilation Systems at Oconee; Reactor Building Purge, Penetration Room Ventilation, and Reactor Building Cooling. Each system has indication that the required emergency alignment has been achieved in the control room. (Penetration Room Ventilation is no longer required due to adoption of alternate source term.)

For the Reactor Building Purge System direct indication of containment isolation valves position is provided. The in-containment isolation valves (PR-1, 6) are MOVs whose position indication is provided by internal limit switches. These valves are not in the EQ program because they are racked-out during normal operation and are not required to function during a design basis event. This instrumentation is powered from safety grade emergency power. The out-of-containment isolation valves (PR-2, 5) are AOVs and positive indication is provided by limit switches. Positive indication of these valves is required per RG 1.97 (PAM). Therefore environmental qualification is provided for these limit switches. This instrumentation is powered from safety grade emergency power. Reactor Building Purge is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 2 variable at Oconee.

For the Penetration Room Ventilation System, positive indication of system operation is provided by the Penetration Room Pressure Instrumentation. This instrumentation is pneumatic and is supplied by normal Station Air System. The Unit 1 and 2 instruments are located in mild environments; however, the Unit 3 instrumentation is located in a harsh environment. Penetration Room Ventilation System is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 2 variable at Oconee.

For a description of the instrumentation required to determine proper operation of the Reactor Building Cooling System see UFSAR Section 7.5.2.41.

7.5.2.51 Emergency Power System Status

All safety-grade emergency or battery backed control busses have undervoltage alarms in the Control Room with local diagnostic capabilities to enable an expedient assessment of abnormal situations. In addition, the 125 VDC distribution centers have analog indicators of voltage level in the Control Room. All of the Control Room alarms are on highly reliable battery backed busses. All of the sensing relays and alarm electronics are located in a mild environment. See FSAR Chapter 8. Emergency Power System Status is classified as a Regulatory Guide 1.97, Rev. 2 Type D Category 2 variable at Oconee.

7.5.2.52 Unit Vent Radioactive Discharge Monitors

Oconee has a normal range, high range and high-high range channel of unit vent radioactivity instrumentation. These channels are powered from a highly reliable non load shed power bus. The indicated range is 1 to 10^8 R/hr gross gamma for the high-high range monitor which envelopes the upper end of the recommended range. The indicated range is 10 to $1E^7$ cpm for the high range channel and 10 to $1E^7$ cpm for the normal range channel. The combined ranges of these monitors meet the requirements of Regulatory Guide 1.97, Rev. 2 Type C Category 2 variable. This instrumentation is installed in a mild environment.

7.5.2.53 Unit Vent Flow

The installed instrumentation indicates flow in the unit vent stack over the range of 0 to 110% of design flow. The design flow for the Unit 1 stack is 97,262 SCFM (98,880 for Unit 2; 114,506 for Unit 3). The indicator and recorder, Units 1, 2 and 3 respectively, actual dual ranges are the following:

Unit 1&2	-	0 to 60 x 10^3 SCFM
		0 to 120 x 10^3 SCFM
Unit 3	-	0 to 65 x 10^3 SCFM
		0 to 130 x 10^3 SCFM

The primary instrument loop which contains the transmitter, the plant computer and the retransmitter is powered by a highly reliable battery backed bus. The secondary instrument loop contains the retransmitter, indicator and recorder. The retransmitter and indicator are powered by a highly reliable auxiliary bus. The instrumentation is located in a mild environment and envelopes the Regulatory Guide 1.97, Rev. 2 Type E Category 2 variable range criteria of 0 to 110% of design flow.

7.5.2.54 Main Steam Line Radiation Monitors

Area radiation monitors are located adjacent to the main steam lines to detect radioactivity emitted from main steam. The monitors for all 3 units are located upstream of the main steam relief valves. Correlation curves allow conversion of the monitor readings in mR/hr to μCi/cc. The indicated range for the monitors is 10^{-2} to 10^7 mR/hr. The monitors are powered from a highly reliable non load shed power bus capable of receiving power from the on-site emergency power sources. This instrumentation is rated to withstand the environmental conditions that would exist during accidents in which it is intended to operate. A steam line break in the vicinity of this instrumentation may cause the environment to exceed the rated temperature, however, the instrument is not required to remain operational for this event. Main Steam Line Radiation Monitors are classified as a Regulatory Guide 1.97, Rev. 2 Type E Category 2 variable at Oconee.

7.5.2.55 Wind Direction

Oconee has two channels of wind direction instrumentation. The indicated range is 0 to 540°. Wind direction is a Regulatory Guide 1.97 Category 3 Type E Variable. The range and accuracy of the installed instrumentation is adequate for its intended purpose.

7.5.2.56 Wind Speed

Oconee has two channels of wind speed instrumentation. The indicated range is 0 - 60 mph. Wind Speed is a Regulatory Guide 1.97 Category 3 Type E Variable. The range and accuracy of the installed instrumentation is adequate for its intended purpose.

7.5.2.57 Atmospheric Stability

The indicated range for atmospheric stability is -4° to 8°C for 44.7 meter interval. Loop accuracy is at least +0.15°C. This range is adequate for Oconee site meteorological conditions. Atmospheric Stability is classified as a Regulatory Guide 1.97, Rev. 2 Type E Category 3 variable at Oconee.

7.5.2.58 Low Pressure Service Water Flow to Low Pressure Injection Coolers

Two QA Condition 1 instrumentation channels are provided (one per train) for post accident monitoring of Low Pressure Service Water (LPSW) flow to the Low Pressure Injection (LPI) coolers in response to

Regulatory Guide 1.97. Each instrument channel is seismically qualified and powered from a safety grade power source. Each instrument channel signal inputs to a qualified indicator and to the plant computer via a qualified signal isolator. These channels monitor LPSW flow to the LPI Coolers over a range of 0-8000 gpm which envelopes the 0-110% of design flow criteria for Regulatory Guide 1.97.

Two non-safety instrument channels are provided, one per train, for indication of LPSW flow to LPI Cooler and control of valves LPSW-251 and 252. Each instrument signal inputs to a controller which monitors flow and valve control. These channels monitor LPSW flow to the LPI Cooler over a range of 0-6000 gpm. These instrument channels are not required for Regulatory Guide 1.97 and are used for normal operation.

LPSW flow to LPI Coolers is a Type A Category 1 variable at Oconee because the operator relies on this information following a design basis event (LOCA) to throttle LPSW flow to LPI Coolers to maintain proper flow balance in the LPSW System.

7.5.2.59 Essential Siphon Vacuum Tank Pressure (Vacuum)

The instrumentation for this variable provides continuous display of Essential Siphon Vacuum (ESV) Tank Pressure. One instrument channel is provided for each train of ESV tank. The ESV system on a per unit basis consists of three pumps and two tanks. Each train consists of one tank and one pump. The third ESV pump serves as an in-place spare pump which can be aligned to either train. The instrumentation provides control room indication of tank vacuum from 30 In Hg to 0 In Hg. The instrumentation is seismically qualified in accordance with the Oconee licensing basis as specified in the Oconee UFSAR and Duke Power Seismic Design Criteria (OCSD-0193.01-00-0001). The instrumentation is located in the ESV building which is considered a Mild Environment. The installed equipment meets the requirements of RG 1.97, Rev 2 for Type D, Category 2 nuclear safety related (QA-1) instrumentation as described in Section 7.5.

This instrumentation monitors the Essential Siphon Vacuum Tanks for operation to provide information (two indicators, two computer alarms, and two annunciator alarms, all one per tank) to indicate the operation of the system in the event it is needed to mitigate the consequences of the design basis accident (LOCA/LOOP).

7.5.2.60 Essential Siphon Vacuum Tank Water Level

The instrumentation for this variable provides continuous local display of Essential Siphon Vacuum Tank Water level. One instrument is provided on each train of ESV tank. The level gage is physically located on the tank. The ESV system for each unit consists of three full capacity pumps and two tanks. Each train consists of one tank and one pump. The instrumentation range (0-24 inches) provides local indication of any accumulated water in the ESV Tanks. Manual action can be taken to drain the tanks as required. The instrumentation is seismically qualified in accordance with the Oconee licensing basis as specified in the Oconee UFSAR and Duke Power Seismic Design Criteria (OCSD-0193.01-00-0001). The instrumentation is located in the ESV building which is considered a Mild Environment. The installed equipment is adequate for its intended monitoring function and meets the requirements of RG 1.97, Rev. 2 for Type D, Category 2 nuclear safety related (QA-1) variables instrumentation as described in Section 7.5.

This variable monitors the Essential Siphon Vacuum Tanks for operation to provide local indication regarding the operation of the system in the event it is needed for continued post accident mitigation of the consequences of the design basis accident (LOCA/LOOP).

7.5.2.61 Siphon Seal Water Flow to Essential Siphon Vacuum Pumps

The instrumentation for this variable provides continuous local display of Siphon Seal Water (SSW) flow to the Essential Siphon Vacuum pumps as well as a signal to the plant computer for display in the control room. One instrument is provided on each SSW supply to an ESV pump. There are three ESV pumps per unit. A total of nine instruments are provided for the nine ESV pumps. A bargraph indicator is located on the local panel in the ESV Building for each Unit's three pumps. The ESV system consists of three pumps and two tanks. Each ESV train consists of one tank and one pump. The third pump is an installed spare. The instrumentation is seismically qualified in accordance with the Oconee licensing basis as specified in the Oconee UFSAR and Duke Power Seismic Design Criteria (OCSD-0193.01-00-0001). The instrumentation is located in a Mild environment. The installed equipment meets the requirements of RG 1.97, Rev. 2, Type D, Category 2 nuclear safety related (QA-1) instrumentation as described in Section 7.5.

The range (0 to 15 Gallons per Minute (GPM)) and the qualification requirements of the SSW flow to ESV pumps instrumentation is in compliance with the recommendations of RG 1.97, Rev. 2 for Type D variables. This variable monitors the Siphon Seal Water flow to the Essential Siphon Vacuum Pumps to provide information relative to the operation of the ESV system in the event it is needed for continued post accident mitigation of the consequences of the design basis accident (LOCA/LOOP).

7.5.2.62 Low Pressure Service Water Reactor Building Waterhammer Prevention System Valve Position

The Low Pressure Service Water (LPSW) Reactor Building (RB) Waterhammer Prevention System (WPS) is designed to maintain the LPSW piping inside containment water solid during events which cause a loss of LPSW such as LOOP, LOCA/LOOP, or MSLB/LOOP. The system's major components consist of check valves in the suply headers (LPSW-1111, 1116), pneumatic discharge isolation valves (LPSW-1121, 1122, 1123, 1124), pneumatic vent valves (a.k.a. controllable vacuum breakers) (LPSW-1150, 1151), and associated acutation circuitry.

The installed instrumentation provides valve position indication for the pneumatic discharge isolation valves (LPSW-1121, 1122, 1123, 1124). Position indication is provided by QA-1 indicating lamps at the control switches on the control board for the four pneumatic discharge isolation valves. These LPSW valve position indications associated with LPSW RB Waterhammer Prevention System are considered to be Regulatory Guide 1.97, Rev. 2, Type D Category 3 instrumentation.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.5.

THIS PAGE LEFT BLANK INTENTIONALLY.

7.6 Control Systems Not Required for Safety

7.6.1 Regulation Systems

Reactor output is regulated by the use of movable control rod assemblies and soluble boron dissolved in the coolant. Control of relatively fast reactivity effects, including Doppler, xenon, and moderator temperature effects, is accomplished by the control rods. The control response speed is designed to overcome these reactivity effects. Relatively slow reactivity effects, such as fuel burnup, fission product buildup, samarium buildup, and hot-to-cold moderator reactivity deficit, are controlled by soluble boron.

Control rods are normally used for control of xenon transients associated with normal reactor power changes. Chemical shim shall be used in conjunction with control rods to compensate for equilibrium xenon conditions. Reactivity control may be exchanged between rods and soluble boron consistent with limitations on power peaking.

Reactor regulation is a composite function of the Integrated Control System and Control Rod Drive System. Design data for these subsystems are given in the following sections.

7.6.1.1 Control Rod Drive System

The Control Rod Drive System (CRD) includes drive controls, power supplies, position indicators, operating panels and indicators, safety devices, and enclosures.

7.6.1.1.1 Design Basis

The Control Rod Drive System design bases are categorized into safety considerations, reactivity rate limits, startup considerations, and operational considerations.

7.6.1.1.2 Safety Considerations

The control rod assemblies (CRA) are inserted into the core upon receipt of protective system trip signals. Trip command has priority over all other commands.

No single failure shall inhibit the protective action of the Control Rod Drive System.

7.6.1.1.3 Reactivity Rate Limits

The speed of the mechanism and group rod worth provide the reactivity change rates required. For design purposes, the maximum rate of change of reactivity that can be inserted by any group of rods has been set at a conservative value used within the Chapter 15 Section 15.3 and Section 15.2. The drive controls, i.e., the drive mechanism and rods combination, have an inherent speed-limiting feature.

7.6.1.1.4 Startup Considerations

The Control Rod Drive System design bases for startup are as follows:

Reactor regulation during startup is a manual operation.

Control rod "out" motion is inhibited when a high startup rate in the wide range is detected.

7.6.1.1.5 Operational Considerations

For operation of the reactor, functional criteria related to the control rod drive system are:

CRA Positioning

The Control Rod Drive System provides for controlled withdrawal, controlled insertion, and holding of the control rod assemblies (CRA) to establish and maintain the power level required for a given reactor coolant boron concentration.

Position Indication

Continuous rod position indication, as well as full-in and full-out position indication, are provided for each control rod drive.

System Monitoring

The Control Rod Drive System design includes provisions for routinely monitoring conditions that are important to safety and reliability.

7.6.1.1.6 System Design

The Control Rod Drive System provides for withdrawal and insertion of the control rod assemblies to maintain the desired reactor output. This is achieved either through automatic control by the Integrated Control System discussed in Section 7.6.1.2 or through manual control by the operator. As noted previously, this control compensates for short term reactivity changes. It is achieved through the positioning in the core of sixty-one control rod assemblies and eight axial power-shaping rod assemblies. The sixty-one rods are grouped for control and safety purposes into seven groups. Four groups function as safety rods, and three groups serve as regulating rods. An eighth group serves to regulate axial power peaking due to xenon poisoning. Seven of the eight groups may be assigned from four to twelve control rod assemblies. Eight rod assemblies are used in Group 8.

Control rods are arranged into symmetric (by core quadrant) groups by utilizing the Engineering Work Station (EWS) to edit a data base contained in the PLC software which defines the desired rod group patterns. Typically, thirty-six rods, including the axial power shaping rods, are assigned to the regulating groups, and thirty-three rods are assigned to the safety rod groups. A typical rod grouping arrangement is shown below:

Safety Rods	Regulating Rods	Axial Power Shaping Rods
Group 1 - 8	Group 5 - 12	Group 8 - 8
Group 2 - 8	Group 6 - 8	
Group 3 - 8	Group 7 - 8	
Group 4 - 9		

During startup, the safety rod groups are withdrawn first, enabling withdrawal of the regulating control groups. The sequence allows operation of only one regulating rod group at a time except where reactivity insertion rates are low (first and last 25 percent of stroke), at which time two adjacent groups are operated simultaneously in overlapped fashion. These insertion rates are shown in Figure 7-11.

As fuel is used, dilution of soluble boron in the reactor coolant is necessary. When Group 6 is more than 95 percent withdrawn, interlocks permit dilution. The reactor controls insert Group 6 to compensate for the reduction in boron concentration by dilution. The dilution is automatically terminated by a pre-set volume measuring device. Interlocks are also provided on Group 6 rod position to terminate dilution at a pre-set insertion limit.

7.6.1.1.7 System Equipment

The Control Rod Drive System consists of three basic components: (1) control rod drive motor power supplies; (2) system logic; and (3) trip breakers. The power supplies consist of 138 Single Rod Power

Supply (SRPS) modules, with two identical wired as a redundant pair and connected to each CRDM. Each SRPS uses a six-phase half-wave (SCR) rectifier design. See Figure 7-4, Figure 7-12 and Figure 7-13.

SRPS, rectification and switching of power is accomplished through the use of Silicon Controlled Rectifiers (SCRs). This switching sequentially energizes first two, then three, then two of the six CRA motor stator windings in stepping motor fashion, to produce a rotating magnetic field for the control rod assembly motor to position the CRA. Switching is achieved by gating the six SCRs on for the period each winding must be energized. As each of the six windings utilize SCRs to supply power, six gating signals are required.

Deleted Paragraph(s) per 2009 Update

Gating signals for the SRPS are generated by a Programmable Logic Controller (PLC) using software containing logic to accept automatic commands from the ICS, or direct manual commands from the Operator Control Panel (OCP). These commands are converted to sequential digital outputs which cause the mechanism motors to step at the proper speed and direction to provide a 3-2 hold control, which ensures two-coils are energized when there are no commands. If one coil becomes de-energized the control rod position will be maintained, but cannot be exercised. A second PLC is devoted exclusively to processing absolute and relative control rod position indication signals.

Deleted Paragraph(s) per 2009 Update

The PLC is also known as a Triple Modular Redundant (TMR) Controller using a triplicated processor running in parallel, with redundant and automatic selection of the "good" signal in the event of failure or malfunction of the controlling "slice". An auctioneering network determines if any anomalies exist and selects the most credible (via a two-out-of-three voting network) of the three available signals. Each processor executes the application program simultaneously and independently. Redundant power supplies are used for all CRD mechanisms, and each is capable of carrying the full load and each is fed from separate power sources with a common SCR gating signal control source.

Deleted Paragraph(s) per 2009 Update

Major components of the system are the RPS interface Trip Breakers, Position Indication (PI) Panel, OCP, TMR Controllers, Engineering Work Station (EWS) – for software control inputs, and the SRPS.

Switches are provided at the operators control panel for selection of desired rod control mode. Control modes are: (1) Automatic mode--where rod motion is commanded by the Integrated Control System; and (2) Manual mode--where rod motion is commanded by the operator. Manual control permits operation of a single rod or a group of rods. Alarm lamps on the CRD panel alert the operator to the systems status at all times. The Group 8 control rods can only be controlled manually even when the remainder of the system is in automatic control.

The sequence section of the logic system utilizes rod position signals to generate control interlocks which regulate rod group withdrawal and insertion. Sequence logic applies in both automatic and manual modes of reactor control, and controls the regulating groups only. When operating in the "sequence mode" mode, the PLC controls sequential withdrawal and insertion of numerically adjacent regulating groups. Two adjacent groups are enabled coincidentally within 25% overlap regions, in order to minimize effects of lower rod worth at their upper and lower extremes in travel.

The automatic sequence logic can control only rod Groups 5, 6, and 7. The safety rod groups, Groups 1 through 4, are controlled manually, one group at a time. There is no way in which the automatic sequence logic can affect the operations required to move the safety rods.

In addition to the sequence logic, logic is also provided which prohibits out of sequence conditions. The selection of manual control mode and sequence bypass mode functions permit intentional out-of-sequence

conditions. This condition is indicated to the operator. If automatic control is selected, "sequence" operation cannot be bypassed.

"Sequence bypass" operation permits selection of any rod group or any single rod for control. It will not permit selection of more than one rod group at any given time. Motion of more than one group at any given time is also not possible when this operation is selected.

Inputs to the system logic from the Nuclear Instrumentation and the Integrated Control System provide interlock control over rod motion. These interlocks cause rod motion command lines and control mode selection to be inhibited.

Under certain conditions, the nuclear instrumentation generates an "out inhibit" signal. When this signal is received by the Control Rod Drive System, all out command circuits are disabled, thus preventing withdrawal of all rods in either automatic or manual control.

Automatic operation of rods can only be commanded by the ICS when the Control Rod Drive System is in the automatic mode. These commands can only affect rod Groups 5, 6, and 7.

In the Control Rod Drive System, two methods of position indication are provided: an absolute position indicator and a relative position indicator. Either position signal is available to the control board indicator through a selector switch. The absolute position transducer consists of a series of magnetically operated reed switches mounted in a tube parallel to the motor tube extension. Each switch is hermetically sealed. Switch contacts close when a permanent magnet mounted on the upper end of the lead screw extension comes in close proximity.

As the lead screw (and the control rod assembly) moves, the switches operate sequentially, producing an analog voltage proportional to position. Other reed switches included in the same tube with the position indicator matrix provide full-in and full-out limit indications.

The relative position indication is calculated by the TMR processor. Control Rod Drive System trip breakers are provided to interrupt power to the control rod drive mechanisms. When power is removed, the roller nuts disengage from the lead screw allowing a gravity trip of the CRA.

The Group 8 drive mechanisms are modified to prevent rod drop into the core when power is removed from the stators. In this type of mechanism, the roller nuts are mechanically restrained to remain engaged with the lead screw at all times. Thus, the mechanical "trip" action has been removed from these APSR's, and they remain at the position they occupied immediately before trip was initiated.

Deleted Paragraph(s) per 2009 Update

The CRD Trip Breakers are of the three-pole, stored energy type and are equipped with instantaneous undervoltage and shunt trip coils. Each of the four breakers is housed in separate metal-clad enclosures with two vertical breakers housed in the middle two compartments of each of two adjacent and integral seismically-qualified Class 1E breaker cabinets. Two other compartments in each cabinet are utilized for ancillary equipment (Reactor Trip Confirm Signals and Source Interruption Device Signals via the AC Power Interface equipment in top and 15 KVA Control Transformer in bottom). All breakers have motor-driven reset features to provide remote reset capability.

7.6.1.1.8 System Evaluation

Safety Considerations

A reactor trip occurs whenever power has been removed from the rod drive motors. The design provides stored energy breakers which do not require power to interrupt the electrical feeds to control rod drive power supplies.

Deleted Paragraph(s) per 2009 Update

The system ensures that power is removed from all of the CRDM's by utilyzing a 1 out of 2 taken twice power design. This design uses 2 qualified breakers located in the "A" power feed into the system and 2 qualified breakers located in the "B" power feed into the system. Therefore a single failure in the distribution system for the control rods does not prevent a plant shutdown.

The minimum voltage required to hold a drive in a withdrawn position is 42 volt DC per coil (2 coil "hold" mode). The probability of an external DC source being applied to the control rod drive mechanisms downstream from the reactor trip points such that the CRA are held in their withdrawn positions after a trip is not considered credible for the following reasons:

1. The trip devices in the Control Rod Drive System remove all DC power from the drives.
2. Control rod drive power cables are terminated at only three points between the Control Rod Drive System cabinets and the drive mechanisms.

   Two of these terminations are made outside and inside the Reactor Building electrical penetrations inside junction boxes containing only control rod drive power cables. The third termination is made in bulkhead connectors (one per drive) in the area of the reactor. The only other cables terminated in this area are the control rod drive instrumentation cables. The instrumentation cables are terminated in bulkhead connectors of a different size and configuration, therefore mismating of connectors could not be accomplished.
3. No cable splices are permitted between termination points described.
4. DC systems from the batteries at Oconee are not grounded and are equipped with ground detecting circuitry.

In summary, series redundant trip devices having adequate rating, testability and a 1 out of 2 taken twice power design arrangement insure safety of reactor trip circuits.

Reactivity Rate Limits

The desired rate of change of CRA reactivity insertion and uniform reactivity distribution over the core are provided for by the control rod drive and power supply design, and the selection of rods in a group. The CRA motor, lead screw, and power supply designs are fixed to provide a uniform rate of speed of 30 in./min. The speed is determined by the CRD PLC, which digitally controls speed. The reactivity change is then controlled by the rod group size. To insure flexibility in this area, rod group assignments are entered off-line at the EWS into password-protected software. This determines desired rod group worth distribution to coordinate with varying core reload design. Any rod may be assigned to any group, with the exception of group 8, so long as the same group pattern exists in each core quadrant. Rod groups may vary from a minimum of four to a maximum of 12, which translates into five possible rod groupings of 4, 5, 8, 9, and 12 – where the odd-numbered group would contain the center rod at core grid H-8. APSR rod assignments are fixed at two near the center of each quadrant.

Deleted Paragraph(s) per 2009 Update

Uniform and symmetrical reactivity addition rate is provided by synchronous withdrawal of all rods assigned to that group. All rods in any one group will have the same CRD motor stator windings simultaneously energized. Such synchronous withdrawal is achieved by phase trigger pulses from the Pulse Generator/Monitor (PG/M) modules in response to rod movement command signals generated by the TMR Controller. The TMR architecture employs a highly synchronized triplicated processor set running in parallel. Each processor "slice" executes the application program simultaneously and independently, verifying data, control, clock, and synchronization signals. These signals are partitioned and down-loaded in such a manner as to optimize execution times of the algorithms controlling synchronous motion of the entire group.

Each control rod is provided with rod position indicator logic to sense asymmetric rod patterns by comparing the individual rod position with its group average position. When the rod moves out-of-step from its group by a preset amount, this condition is alarmed to the operator, the plant computer, and the ICS. Depending on the power setting and the control mode, action is initiated by the ICS to insert rods and reduce power.

Startup Considerations

The rod drive controls receive interlock signals from the ICS and nuclear instrumentation (NI). These inputs are used to inhibit automatic mode selection when a large error exists in the ICS reactor control subsystem and to inhibit out motion for high startup rates, respectively.

In addition to the startup considerations, dilution controls, to permit removal of reactor shutdown concentrations of boron in the reactor coolant, are provided. This control bypasses the normal reactor coolant dilution controls, described in Section 7.6.1.1.6, provided all safety rods are withdrawn from the core and the operator initiates a continuous feed and bleed cycle. An additional interlock on rod Group 5 inhibits the use of this circuit when rod Group 5 is more than 80 percent withdrawn.

Operational Considerations

The control rod assembly positioning system provides the ability to move any rod to any position required consistent with reactor safety. As noted in Section 7.6.1.1.8, a uniform speed is provided by the drive system. A fixed rod position when motion is not required is obtained by the power supply ability to energize two adjacent windings of the CRA motor stator. This static energizing of the windings maintain a latched stator and fixed rod position.

Position Indication

As previously described, two separate position indication signals are provided. The absolute position sensing system produces signals proportional to CRD position from the reed switch matrix located on each CRD mechanism. The relative position indication system produces a signal proportional to the number of electrical pulses sent to the CRD motor stator windings, as determined through processing of these signals by a separate programmable logic (TMR) controller whose sole function is the processing of absolute and relative position indication signals.

Position indicating readout devices mounted on the operator's console consist of 69 single rod position meters. The operation of a selector switch permits either relative or absolute position information to be displayed on the single rod meters.

Indicator lights are provided on the position indication panel to indicate when each rod is (1) fully inserted, (2) fully withdrawn, (3) under control, and (4) whether a fault is present. Indicators on the operator control panel show full insertion, full withdrawal, under control, and fault indication for each of the eight control rod groups.

Failures which could result in unplanned control rod withdrawal are continuously monitored by fault detection logic. When failures are detected, indicator lights and alarms alert the operator. Fault indicator lights remain on until the fault condition is cleared by the operator. A list of indicated faults is shown below:

1. Asymmetric rod patterns (indicator and alarm).
2. Sequence faults (indicator and alarm).
3. Trip status (indicator and alarm).
4. Safety rods not withdrawn (indicator only).
5. Rod position sensor faults.

Faults serious enough to warrant immediate action produce automatic correction commands from the fault detection logic, and manual bypass is not possible. Status indicators on the operator's console provide monitoring of control modes.

A description of each fault detector follows:

Asymmetric Rod Monitor

Design Basis - To detect and alarm if any rod deviates from its group reference position by more than a maximum of nine inches true position.

Operation - There are 69 asymmetric rod pattern monitors, one assigned to each control rod. This logic continuously compares the individual rod absolute position signal with the absolute group reference (average) signal. The absolute value of the difference between the two signals is computed, and if this difference is less than the maximum value allowed by the software configuration, no output results. If, however, the difference is greater than the setpoint, the system alarms the asymmetric condition. Two alarm channels are provided which are identical except for the setpoints. One setpoint allows a maximum 7-inch true position separation before initiating an alarm. The other setpoint allows a maximum 9-inch true position separating before initiating the action described below.

Corrective Action - Action taken upon detection of an asymmetric rod fault depends upon the control mode and the power level in effect at the time the fault is detected. Corrective action is the same for any asymmetric condition including "stuck-in," "stuck-out," or dropped control rods.

Detection of a 7-inch position separation is defined as an "asymmetric rods alarm." Actuation of this alarm causes the fault indicator lamp for that rod to be energized and an alarm signal to be sent to the plant computer and annunciator.

If the condition is not corrected and the separation increases to a 9-inch position separation, the following actions occur:

"Asymmetric fault" lamp on the operator's console is energized. If operation is in the manual control mode, operator action is required by administrative control.

If operation is in the automatic mode, a "runback fault" signal is sent to the Integrated Control System. The ICS will impose a maximum reactor power demand of 55 percent of rated power if power is initially less than 55 percent.

When an asymmetric fault occurs, the Control Rod Drive Control System generates an "Out Inhibit" which prevents automatic rod motion that would increase reactor power. Below 60 percent reactor power the ICS generates a bypass signal for the out inhibit, which allows normal automatic rod control.

Reactor power demand remains limited to 55 percent maximum in automatic control until the fault is corrected.

Sequence Monitor

Design Basis - To detect any motion of the regulating rod groups outside of the predetermined automatic sequence patterns, and to prevent further automatic motion when such conditions occur.

Operation - The sequence logic continuously compares the group average (reference) signals for each regulating rod group with the allowable sequence patterns. In addition, the rod group "enable" logic determines if a group is enabled for motion out-of-turn. The safety rod groups' out limit signals serve as a permissive to automatic sequencing: the sequence monitor prevents automatic control until the safety rods are fully withdrawn.

Corrective Action - When an out-of-sequence condition is detected and operation is in the automatic control mode, the automatic mode disengages and an alarm lamp alerts the operator to the malfunction.

Control reverts to manual and remains in manual until the fault is corrected and the system is reset by the operator.

Trip Status

Design Basis - To sense the status of trip devices and trip channels.

Operation - The circuit contains elements, which sense the state of each trip device as well as the state of each of the four trip channels. If a trip device or a trip channel is in a trip state, its associated annunciator will alarm. The annunciators are used by operations to detect faults that may affect operation of the trip circuits, such as one trip breaker in the tripped position during normal operation.

Corrective Action - Alarms are provided.

Safety Rods Not Withdrawn

Design Basis - To prevent, on plant startup, withdrawal of the regulating rods until the safety rods are fully withdrawn.

Operation - Continuously monitors the group "out" limit for the four safety rod groups. When the four groups are all fully withdrawn, automatic control is permitted.

Corrective Action - Alarms are provided.

Rod Position Sensor Faults

All rod position sensor faults lead to false asymmetric, stuck, or dropped rod symptoms which are acted upon by the Asymmetric Rod Monitor previously described.

7.6.1.2 Integrated Control System

7.6.1.2.1 Design Basis

The Integrated Control System (ICS) provides the proper coordination of the reactor, feedwater control, and turbine under all operating conditions. Proper coordination consists of producing the best load response to the Core Thermal Power demand while recognizing the capabilities and limitations of the reactor, steam-generator feedwater system, and turbine. When any single portion of the plant is at an operating limit or control selection is on manual, the Integrated Control System design uses the limited or manual section as a load reference.

The Integrated Control System maintains constant average reactor coolant temperature between 15 and 100 percent rated power, and constant steam pressure at all loads. Optimum unit performance is maintained by limiting steam pressure variations; by limiting the unbalance between the steam generator, the turbine, and the reactor; and by limiting the Core Thermal Power demand upon loss of capability of the steam generator feed system, the reactor, or the turbine generator. The control system provides limiting actions to assure proper relationships between the generated load, turbine valves, feedwater flow, and reactor power.

The response of the Reactor Coolant System to increasing and decreasing power transients is limited by the Integrated Control System as indicated in Table 7-6. The Turbine Bypass System permits a load drop of 40 percent or a turbine trip from 40 percent load without safety valve operation.

7.6.1.2.2 Description

The Integrated Control System includes four independent subsystems as shown in Figure 7-14. The four subsystems are: the Core Thermal Power Demand; the Integrated Master; the Feedwater Control; and the Reactor Control. The system philosophy is that control of the plant is achieved through feed-forward control from the Core Thermal Power Demand. The Core Thermal Power Demand produces demands for

parallel control of the turbine, reactor, and Steam Generator Feedwater System through respective subsystems.

The Feedwater Control is capable of automatic or manual feedwater control from a startup to full power. The Integrated Master Control is capable of automatic or manual turbine valve control from minimum turbine load to full output, and of manual control below minimum turbine load. The Reactor Control is designed for automatic or manual operation above 2 percent power, and for manual operation below 2 percent power.

The basic function of the Integrated Control System is matching Turbine and Reactor Power to Core Thermal Power demand. The Integrated Control System does this by coordinating the steam flow to the turbine with the rate of steam generation. To accomplish this efficiently, the following basic reactor/steam-generator requirements are satisfied:

The ratios of feedwater flow and BTU input to the steam generator are balanced as required to obtain desired steam conditions.

BTU input and feedwater flow are controlled:

1. To compensate for changes in fluid and energy inventory requirements at each load.
2. To compensate for temporary deviations in feedwater temperature resulting from load change, feedwater heating system upsets or final steam pressure changes.

7.6.1.2.2.1 Unit Load Demand

The Core Thermal Power Demand Subsystem provides the operator with a means of establishing the desired operating power load from the plant. The demand signal produced by this subsystem is called the Core Thermal Power Demand (CTPD), and is the principle independent demand signal in the ICS. Other subsystems receive the CTPD and establish final control element positions in order to meet this demand.

The CTPD subsystem obtains a load demand signal, manually set by the operator, from the Load Control Panel. The Load Control Panel is the primary operator interface to the ICS for Integrated Mode operation. Pushbutton switches, digital meters, a digital thumb switch and status lamps are provided for manipulation of Core Thermal Power Demand Set, the Demand Rate Set, turbine Load and Unload, Maximum Runback function and status for various Load Limit and Tracking conditions. The CTPD substytem initiates load limiting and runback functions to restrict operation within prescribed limits. Figure 7-15 illustrates the functions incorporated in the subsystem.

The CTPD is restrained by a maximum load limiter, a minimum load limiter, a rate limiter and a runback limiter.

Rate limiting is designed as a function of load, so transients are limited as shown in Table 7-6.

The limiter acts to runback and/or limit the CTPD under any of the following conditions:

1. Loss of one or more reactor coolant pumps.
2. CTPD vs reactor coolant flow, variable limit.
3. Low suction pressure (FDW or Condensate)
4. Loss of one feedwater pump.
5. Asymmetric rod patterns exists in reactor.
6. The generator separates from the bus.
7. A reactor trip occurs.

The output of the limiters is a CTPD signal which is applied to the turbine control, feedwater control, and reactor control in parallel.

The controlling subsystems of the ICS (turbine control, feedwater control, and reactor control) normally operate in the automatic mode in response to a demand signal from the CTPD. The subsystems control function is kept within pre-established bounds under other than normal automatic operation by a "load tracking" feature built into the ICS. The ICS will switch to the load tracking mode if either of the following conditions exists:

One or more of the subsystems are in manual.

Errors greater than preset limits develop between the demand and the variable.

In this mode, the CTPD is made to follow the manual or limited control subsystem. Load tracking continues until the limiting condition is brought back to within the pre-established deadband or the subsystem is returned to automatic operation.

7.6.1.2.2.2 The Integrated Master

The Integrated Master has been designed to receive the Core Thermal Power Demand (CTPD) from the Core Thermal Power Demand Subsystem and utilize this signal as a demand for the feedwater, turbine and reactor control. A functional diagram of the Integrated Master Control is shown in Figure 7-16. The Integrated Master subsystem produces demand signals for the reactor control, feedwater control and turbine control (steam valves), to meet the CTPD, while providing coordination between the primary system, feedwater and turbine to maintain heat balance. The subsystem produces demands for total feedwater flow, reactor power and steam valve position to ensure that heat balance indicating parameters are kept within operating limits. The demands are modified during plant limited operation in accordance with the Control Priority. The ICS Control Priority for the four main heat balance variables is as follows:

Tave

Steam Header Pressure

Reactor Power

Cold Leg Temperature Difference (delta - Tc)

Three major control Hand/Automatic (H/A) stations are provided to give the operator a means of manually setting the integrated master demand outputs. The reactor master control station allows the operator to manually establish a demand for reactor NI-Flux and to set the controlling reactor coolant system Tave set point. The steam generator master H/A station allows the operator to manually establish the total feedwater flow demand. The turbine control H/A station allows the operator to establish the EHC load reference signal and to set the controlling turbine header pressure set point.

Turbine Control

Control of the turbine is accomplished by a pressure controller. The turbine header pressure is compared to a set point (set by the operator from the turbine H/A station) and this error drives an analog signal. The resulting analog signal is sent to the load reference logic where it is integrated into a steam valve position demand. The ICS will continue to generate a demand for turbine valve movement until the pressure error is reduced to zero.

The turbine control H/A station gives the operator the option of letting the turbine control pressure or, by transferring the turbine control station to manual, allowing the operator to establish the amount of electrical load generation.

The "LOAD" and "UNLOAD" push buttons on the "Load Control Panel" provide the operator interface with the turbine load and unload system. The turbine load and unload system enables the operator to

smoothly introduce and remove the main turbine into/from the plant control process. The system is necessary because the reactor may be operated in automatic at a power level significantly below the normal minimum load of the turbine.

Turbine Bypass

The Turbine Bypass System operates from the turbine header pressure error or individual steam generator pressures as an overpressure relief for the turbine header. The turbine bypass valves receive control inputs from their respective OTSG outlet pressure , unless the main turbine is in automatic. If the main turbine is in automatic, the bypass valves use the turbine header pressure error signal, which is the same signal controlling the main turbine controller.

The turbine bypass valves serve four functions:

1. Provide pressure control at low loads before the turbine can be placed in automatic.
2. Provide a high pressure relief if the turbine header pressure exceeds its set point (normally 885 psig) by 50 psig.
3. Provide an independent high pressure relief that operates proportionally to steam generator pressure above 1035 psig.
4. Provide pressure control after a reactor trip at 125 psi above normal set point to prevent excessive cooling of the reactor coolant fluid.

Once the main turbine is placed in automatic control, and loaded, the turbine bypass valves assume over pressure control at set point plus 50 psi.

7.6.1.2.2.3 Feedwater Control

The Feedwater Control Subsystem has been designed to receive the total feedwater demand signal from the Integrated Master Subsystem and utilize this signal to develop demand signals for control of the feedwater pumps and the feedwater valves for each steam generator. A functional diagram of the Feedwater Control Subsystem is shown in Figure 7-17.

The total feedwater demand signal developed in the Integrated Master Subsystem is corrected for feedwater temperature in the Feedwater Control Subsystem. A proportional correction is also applied to the feedwater demand when RC Pressure is greater than 2250 psig. The feedwater demand signal is limited when Neutron Error exceeds +/- 5%.

The corrected total feedwater demand signal is modified to provide a feedwater demand signal for each steam generator. Under normal conditions, each steam generator will produce one-half of the total load. The steam generator load ratio control (delta Tc control) is provided to balance reactor inlet coolant temperatures during operation with more reactor coolant pumps in one loop than in the other. The steam generator load ratio control (delta Tc control) signal is modified by an anticipatory delta Tc error circuit which is based upon a ratio of the measured RC flow.

A Feedwater Master Hand/Automatic control station for each steam generator enables manual control by the operator or operation in automatic. In the automatic mode of operation, feedwater flow is controlled by either level control or flow control. Each steam generator may independently operate on level or flow control.

Level control ("Low Level Limits", LLL) exists when loop Tave is less than the Tave set point and the steam generator level is equal to or less than the steam generator low level set point. During this mode, steam generator startup level provides a demand signal to the feedwater valves for control of feedwater flow to the steam generator.

Flow control exists when Tave is equal to or greater than the Tave set point and steam generator level is greater than the low level limit.

During the flow control mode, the loop feedwater master demand is compared to steam generator feedwater flow and to a maximum steam generator operate level set point. The resultant feedwater error signal is utilized to develop the position demand signal for the feedwater valves. The feedwater error signal drives the feedwater valves to make feedwater flow match loop feedwater flow demand, or to limit the maximum steam generator level.

Feedwater flow to each steam generator is controlled by two valves, a startup valve and a main valve. The startup feedwater control valve provides feedwater flow control from startup to approximately 15 percent reactor power. The main feedwater control valve provides feedwater flow control from approximately 15 percent to 100 percent power. Each feedwater valve has a Hand/Automatic control station which enables automatic control or the operator to manually establish a valve position demand.

Feedwater flow to both steam generators is provided from two turbine driven main feedwater pumps. The speed of both feedwater pumps is controlled by a single automatic controller to maintain a constant differential pressure across the feedwater valves. Feedwater valve differential pressure is compared to set point and the resultant error is the controller demand signal. The loop A and loop B feedwater master demand signals are input to the controller as a feed forward signal to reduce the amount of feedwater valve differential pressure change during load changes. Each main feedwater pump has a Hand/Automatic control station which enables automatic control or the operator to manually establish a pump speed demand.

Feedwater Control - Reactor Coolant Pumps tripped

Upon loss of all reactor coolant pumps, the ICS positions valves to direct main feedwater flow to the auxiliary feedwater header in each steam generator. The steam generator operate level is used as a demand signal to the startup feedwater valve to establish "natural circulation" cooling of the reactor coolant system.

Steam Generator Overfill Protection

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 10CFR 50.54(f)," on September 20, 1989. This generic letter required PWR licensees to provide a description of their steam generator overfill protection (SGOP) 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 Oconee overfill protection system is provided by the Integrated Control System (ICS) and is initiated on high water level in anyone steam generator, based on non-safety grade hardware with a 2-out-of-2 initiating logic. When the high level setpoint is reached, the ICS terminates feedwater by tripping the main feedwater pumps. The Steam Generator Overfill Protection system also added an alternate non-safety grade trip device, SV6, to assure trip of the main feedwater pump turbine in the event of a loss of control power. The NRC SER (see section 10.4.9, Reference II) concluded that this addition minimized the potential for common mode failure such that the overall design of Steam Generator Overfill Protection sufficiently satisfies the single-failure criterion of Generic Letter 89-19.

7.6.1.2.2.4 Reactor Control

The reactor control is designed to maintain a constant average reactor coolant temperature over the load range from 15 to 100 percent of rated power. The steam system operates on constant pressure at all loads. The average reactor coolant temperature decreases over the range from 15 percent to zero load. Figure 7-18 shows the reactor coolant and steam temperatures and the steam pressure over the entire load range.

The Reactor Control Subsystem controls the neutron flux production of the reactor. The subsystem varies the neutron flux such that primary temperature and pressure requirements are maintained, while the heat drawn from the primary system meets the CTPD.

The reactor control subsystem controller receives inputs from core thermal power demand, reactor coolant pressure and reactor coolant average temperature. The output of the controller is an error signal that causes the control rod drives to be positioned until the error signal is within a deadband. A block diagram of the reactor control is shown on Figure 7-19.

A reactor power demand can be established in two ways. The operator can manually establish a reactor power demand using the reactor master hand/automatic control station. The second method of establishing a reactor power demand is with the reactor master control station in automatic. In this mode of operation, the reactor demand becomes a function of CTPD with a modification from Tave, steam pressure and transient RC pressure control.

Cross limits are employed between the reactor control and feedwater control subsystems to help ensure that the basic demand relationships between the reactor and feedwater are preserved during transients. In addition to cross limits, the controller also incorporates a high limit on reactor power level demand.

The reactor power level demand is compared with the reactor power level (neutron flux). The resultant error signal is the reactor power level error (neutron error) signal.

When the reactor power level error signal exceeds the deadband settings, the control rod drive receives a command that withdraws or inserts rods depending upon the polarity of the power error signal.

The reactor controls incorporate automatic or manual rod control above 2 percent of rated power and manual control below 2 percent of rated power.

7.6.1.2.3 System Evaluation

Redundant sensors for major system parameters are available to the Integrated Control System. The list of redundant major system parameters is contained in Section 7.4.2.2.2.

Automatic signal selection between the redundant sensors is provided as described in Section 7.4.2.2.2. The operator can manually select between the redundant sensors which are monitored by SASS; however, if a failure occurs the automatic signal selector (SASS) will transfer the output signal from the failed device to the valid input. The SASS also will not allow the operator to select the failed sensor if the failure occurred on the non-selected sensor. The "Control STAR" uses the median signal selection technique to select between redundant sensors. If a sensor failure occurs the "Control STAR" automatically transfers to the valid redundant sensor. The operator does not have manual selection capability between the redundant sensors which input to "Control STAR"; however, specific sensors can be selected by special maintenance techniques.

Manual reactivity control is available at all power levels. Loss of electrical power to the ICS Automatic control reverts the control system to manual.

Maloperation or failure of any ICS subsystem places no automatic limitations on reactor operation because the ICS reverts to the manual mode. Therefore other ICS subsystems follow the limited subsystem.

The design of the NNI/ICS System in conjunction with procedures and training allow the operator to cope with various loss of power situations. Also, alarm indications provide information to the operator of various instrument and control functions. Emergency procedures provide assurance of positive responses by the operator.

Failure of the ICS does not diminish the safety of the reactor. None of the functions provided by the ICS are required for reactor protection or for actuation of the ESPS. The reactor protection criteria, used in the analysis of accidents presented in Chapter 15 can be met irrespective of ICS action.

7.6.1.2.3.1 Modes of Control

The Integrated Control System is designed to revert to a "Tracking" mode to tie the unit to the subsystem on manual or to the subsystem being limited. In the startup control mode, the reactor is prevented from automatic rod withdrawal below 1.5 percent power.

The controls will limit steam bypass to the condenser when condenser vacuum is inadequate.

7.6.1.2.3.2 Loss-of-Load Considerations

The nuclear unit is designed to accept 10 percent step load rejection without safety valve action or turbine bypass valve action. The combined actions of the control system and the turbine bypass valve permit a load reduction from 40 percent load without safety valve action. The controls will limit steam dump to the condenser when condenser vacuum is inadequate, in which case the steam safety valves may operate. The combined actions of the control system, the turbine bypass valves and the steam safety valves permit separation from the external transmission system without a reactor trip for power levels less than 50 percent.

The features that permit continued operation under load rejection conditions include:

Integrated Control System

During normal operations, the Integrated Control System controls the unit load in response to the core thermal power demand (CTPD) set by the operator. During loss of load, the CTPD is limited to a maximum 20 percent. The ICS will control reactor power, feedwater flow and bypass valve position to maintain the CTPD, Tave and steam pressure. The turbine governor takes control to regulate frequency.

100 Percent Relief Capacity in the Steam System

This provision acts to reduce the effect of large load drops on the Reactor System.

Consider, for example, a sudden load rejection from a power level above 20 percent. When the turbine-generator starts accelerating, the governor valves and the intercept valves close to maintain set frequency. As the governor valves close, steam pressure rises, forcing reduced energy transfer from the primary system and causing reactor coolant average temperature to rise. At the same time, a power demand runback is initiated to 20 percent power by the CTPD, causing reduction in the feedwater and reactor demand signals. The rise in reactor coolant temperature will help initially reduce reactor power along with the reduction in demand. The bypass valves will open in response to the increased steam pressure to reject the excess steam flow to the condenser. In addition, when the load rejection is of sufficient magnitude, the safety valves open to exhaust steam to the atmosphere. If transient conditions warrant, the feedwater system will increase feedwater flow to mitigate the undercooling condition caused by the sudden reduction in steam flow from the loss of load.

As operation continues with the turbine- generator carrying the in-house electrical loads, the turbine control will operate in the frequency control mode, the reactor and feedwater will operate to maintain proper reactor conditions at reduced demand and the bypass system will reject the excess steam flow to the condenser to control steam pressure.

7.6.1.2.3.3 Loss of Power Supply Considerations

The ICS/NNI system power supply is arranged such that it is normally powered from a dedicated static inverter system, which receives a DC input from the Vital I & C batteries, and is backed by an AC input

from one of the plants regulated non-load shed buses (Chapter 8). Both automatic and manual transfer switching is provided to select between these supplies.

In addition to the power supply reliability for the ICS, essential plant parameters necessary for shutdown have been arranged with their power supplies independent of the ICS source. Also, a "display group" has been developed and defined on the plant operator aid computer such that upon a loss of ICS power, the operator may quickly have full and complete information on key primary and secondary system parameters. Emergency procedures have also been developed to designate alternate sources of information on key plant parameters if the computer is unavailable, thus assuring the operator can obtain sufficient systems information. The reliable ICS power supply and the development of operator information are consistent with NRC Bulletin 79-27, "Loss of Non-Class IE I&C Power System Bus During Operation," as described in Reference 1.

If a loss of power event occurs, the ICS/NNI is designed to send the plant to a "Known Safe State" (KSS) by initiating a trip of both main feedwater pumps via the failsafe design of the high steam generator level monitoring circuits. These circuits are designed such that upon a loss of both "hand" and "auto" power they will initiate a trip of the main feedwater pumps and main turbine which will also trip the reactor via the Anticipatory Reactor Trip System (ARTS) circuitry. Emergency feedwater is also initiated upon loss of both feedwater pumps as described in Section 7.4.3. Upon loss of either "hand" or "Auto" power, steady state operation is maintained.

7.6.2 Incore Monitoring System

The Incore Monitoring System has been upgraded to meet the requirements of NUREG 0737 Item II.F.2.

7.6.2.1 Description

The Incore Monitoring System provides neutron flux detectors to monitor core performance. Incore self-powered neutron detectors measure the neutron flux in the core to provide a history of power distributions during power operation. Data obtained provides power distribution information and fuel burnup data to assist in fuel management decisions. The plant computer provides normal system readout and a backup readout system is provided for selected detectors.

7.6.2.2 System Design

The Incore Monitoring System consists of assemblies of self-powered neutron detectors and temperature detectors located at preselected positions within the core. Each core can contain up to 52 incore assemblies. The incore monitoring locations are shown on Figure 7-20. In this arrangement, an incore detector assembly consisting of seven local flux detectors, one background detector, one thermocouple and a calibration tube is installed in an instrumentation guide tube. The local detectors are positioned at seven different axial elevations to indicate the axial flux gradient. The outputs of the local flux detectors are referenced to the background detector output so that the differential signal is a true measure of neutron flux. The temperature detectors located just above the top of the active fuel in the fuel assemblies measure core outlet temperature.

Multi-point recorder readouts of selected detectors are provided independent of the computer.

When the reactor is depressurized, the incore detector assemblies can be inserted or withdrawn through guide tubes which originate at a shielded area in the Reactor Building as shown in Figure 7-21. These guide tubes enter the bottom head of the reactor vessel where internal guides extend up to the instrumentation tubes of 52 selected fuel assemblies. The instrumentation tube serves as the guide for the incore detector assembly. During refueling operations, the incore detector assemblies are withdrawn approximately 13 feet to allow free transfer of the fuel assemblies. After the fuel assemblies are placed in their new location, the incore detector assemblies are returned to their fully inserted positions.

7.6.2.3 Calibration Techniques

The nature of the detectors permits the manufacture of nearly identical detectors which produces a high relative accuracy between individual detectors. The detector signals are compensated continuously for burnup of the neutron-sensitive material.

Calibration of detectors is not required. The incore self-powered detectors are controlled to precise levels of initial sensitivity by quality control during the manufacturing stage. The sensitivity of the detector changes over its lifetime due to such factors as detector burnup, control rod position, fuel burnup, etc. The results of experimental programs to determine the magnitude of these factors have been incorporated into calculations and are used to correct the output of the incore detectors for these factors. Operation of these detectors in both power and test reactors has demonstrated that this compensation program, when coupled with the initial sensitivity, provides detector readout accuracies sufficient to eliminate the need for a calibration system.

7.6.2.4 System Evaluation

7.6.2.4.1 Operational Experience

Self-powered incore neutron detectors have been operated since 1962. Such detectors have been assembled and irradiated in a Babcock & Wilcox development program that began in 1964.

The B&W Development Program included these tests:

1. Parametric studies of the self-powered detector.
2. Detector ability to withstand PWR environment.
3. Multiple detector assembly irradiation tests.
4. Background effects.
5. Readout system tests.
6. Mechanical withdrawal-insertion tests.
7. Mechanical high pressure seal tests.
8. Relationship of flux measurement to power distribution experiments.

Conclusions drawn from the results of the test programs are as follows:

1. The detector sensitivity, resistivity, and temperature effects are satisfactory for use.
2. A multiple detector assembly can provide axial flux data in a single channel and can withstand reactor environment.
3. Background effects will not prevent satisfactory operation in a PWR environment.
4. Plant computer systems are successful as read-out system for in-core monitors.

For Incore Monitoring System development program results and conclusions, refer to B&W Topical Report BAW-10001A; "Incore Instrumentation Test Program."

7.6.2.4.2 Deleted Per 1997 Update

7.6.2.5 Detection and Control of Xenon Oscillations

Under normal operating conditions, the incore detectors supply information to the operator in the control room.

Each individual detector measures the neutron flux at its locality and is used to determine the local power density. The individual power densities are then averaged and a peak-to-average power ratio calculated. This information can be used to indicate possible power oscillations.

7.6.3 References

1. NRC Letter to Duke dated December 7, 1989, Oconee: Audit for Verification of Resolution of IE Bulletin 79-27 concerns

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.6.

THIS PAGE LEFT BLANK INTENTIONALLY

7.7 Operating Control Stations

Following proven power station design philosophy, all control station, switches, controllers, and indicators necessary to start up, operate, and shut down Oconee l and 2 are located in one control room. Controls for Oconee 3 are located in a separate control room. Control functions necessary to maintain safe conditions after a loss-of-coolant accident are initiated from the centrally located control rooms. Controls for certain auxiliary systems are located at remote control stations when the system controlled does not involve unit control or emergency functions.

7.7.1 General Layout

The control room for Oconee 1 and 2 is designed so that one man can supervise operation of both units during normal steady state conditions. During other than normal operating conditions, other operators are available to assist the control operator. Figure 7-26 shows the control room layout for Oconee l and 2. Oconee 3 has similar accessibility to the various controls. The control boards are subdivided to show the location of control stations and to display information pertaining to various sub-systems.

7.7.2 Information Display and Control Functions

Consideration is given in the control board layout to the fact that certain systems normally require more attention from the operator. The Integrated Control System is therefore located nearest the center line of the boards (Section l on Figure 7-26).

On Section 2 of the control board, one indicator will be provided for each control rod. Fault detectors in the Rod Drive Control System are used to alert the operator should an abnormal condition exist for any individual control rod. Displayed in this same area are limit lights for each control rod group and all nuclear instrumentation information required to start up and operate the reactor. Control rods are manipulated from the Section 2 bench position. Plant computer readout facilities for alarm monitoring and sequence monitoring are located here to aid the operator.

A plant computer is used on each unit to provide fuel management measurements and calculations. These computers also provide for alarm monitoring, performance monitoring, data logging, and sequence monitoring during start-up and shut-down of the turbine-generator. Monitoring and display functions of the plant computer which audit Nuclear Steam Supply System parameters of major interest are duplicated elsewhere in the control rooms. This type of computer application has been successfully applied to units presently in operation on the Duke system.

Variables associated with operation of the secondary side of the station are displayed and controlled from Section 1 and 3 of the control board. These variables include steam pressure and temperature, feedwater flow and temperature, electrical load, and other signals involved in the Integrated Control System. Section 3 of the control board also contains indication and controls of the Reactor Coolant System parameters.

The Engineered Safeguards System is controlled and monitored from Sections 3 and 4 unit boards and Section 8 of the vertical boards. Indicating lights are provided as a means of verifying the proper operation of the Engineered Safeguards System. Control switches located on these panels allow manual operation of equipment that is not controlled elsewhere in the control room or test of individual units.

Control and display equipment for station auxiliary systems are located on Section 6 of the control board.

Reactor coolant pump controls located on Section 5 of the control boards consists of the pump controls and auxiliary instrumentation required for pump operation. Also mounted on this section are the Auxiliary Electrical System controls required for manual switching between the various power sources described in Section 8.2 and Section 8.3.

Controls and indications for all normal ventilation systems are located on Section 7 of the control boards.

In order to maintain the desired accessibility for control of the station, miscellaneous recorders not required for station control are located on the vertical recorder boards where they are visible to the operator. Radiation monitoring information is also indicated there.

Radiation monitoring display and transient monitoring system are combined in the process monitoring computer (PMC). The radiation monitoring display provides supervisory control and display of information from field mounted radiation monitoring equipment. The transient monitoring system automatically records pre-selected plant parameters (temperatures, pressures, flowrates, etc.) for analysis and diagnoses of plant transients or reactor trip. Like the OAC, most of the information provided by the PMC is either duplicated elsewhere in the control room, or deemed not significant enough to have a dedicated display device. The PMC is not QA-1, redundant, or single failure proof. The PMC is independent of the OAC. The PMC is not relied upon to initiate a reactor trip, mitigate an accident, or actuate a safety system, and performs only supervisory control to field mounted radiation monitoring and sampling equipment.

A description and results of the Unit 1, 2, and 3 control room review (per Generic Letter 82-33) were provided in the document "Response to Supplement 1 to NUREG-0737" which was submitted on April 14, 1983 by letter from H. B. Tucker to H. R. Denton.

7.7.3 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 Reactor Building 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. Alarms are provided to warn security of unauthorized entry into vital areas.

7.7.4 Communications

7.7.4.1 Control Room to Inside Station

The telephones for the site are connected to a Private Automatic Branch Exchange (PABX) located inside the Oconee Office Building. The PABX has capability of up to 10,000 lines and provides access for communications and paging. The equipment provides 4-digit dialing, dial tone, ring-back tone and busy tone. The PABX is powered by 48VDC batteries, which are charged through an inverter/charger combination, fed by a 480VAC supply. Upon loss of normal AC power, the system batteries will provide required power for a minimum of four (4) hours. Alternate power is automatically provided from the emergency diesel generator provided for the building.

The public address system is accessible through plant telephones by dialing a access code. In the event of PABX failure, the PA system is operable through eleven handsets installed at strategic locations within the station.

A radio transmitter/receiver communication system is provided between the control room and the rest of the station. This system is used during normal plant operation and during outage, security or fire situations. Radio transmission is only available in a reactor building when an antenna is activated by the unit 1 & 2 control room. Usage of the radio communication system in the reactor building is limited to times when the unit is open for access.

A sound powered telephone system was supplied during original plant design, but radio utilization allows this system to be an available but nonessential system. This system consists of a network of conductor

pairs converted to jacks throughout the plant. Sound powered handsets are plugged into the jacks to form talking paths with separate talking paths available for each unit. The system is completely independent from any other telephone system and involves no external power supply.

7.7.4.2 Control Room to Outside Station

The commercial telephone network and the Duke Power fiber optic network provide communication to outside the station area. An interface is provided between the PABX and the commercial telephone lines and another interface is provided between the PABX and the Duke Power fiber optic network which includes access to the General Office at Charlotte, Transmission Control Center, System Operating Center, and Lee Steam Station. Ringdown phone service (independent of the PABX) is also provided through the fiber optic network to the Transmission Control Center, System Operating Center, and Lee Steam Station.

The control room is also equipped with a transmitter-receiver which operates at 800 megahertz to provide communication between the control room and the System Operating Center, Transmission Control Center, and Bad Creek, Jocassee, and Keowee Hydro Stations.

7.7.4.3 Deleted per 1998 Revision

7.7.5 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 rooms for maximum hypothetical accident conditions. Each Control Room Ventilation System is provided with radiation detectors and appropriate alarms. See Section 9.4.1 for control room ventilation systems description. Emergency lighting is provided.

The potential magnitude of a fire in either 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 IEEE 383-1974. (Reference IPCEA S-19-81 & ASTMD 2220-68)
3. Qualified trained personnel, adequate extinguishers, and accessibility to all control room areas are provided.

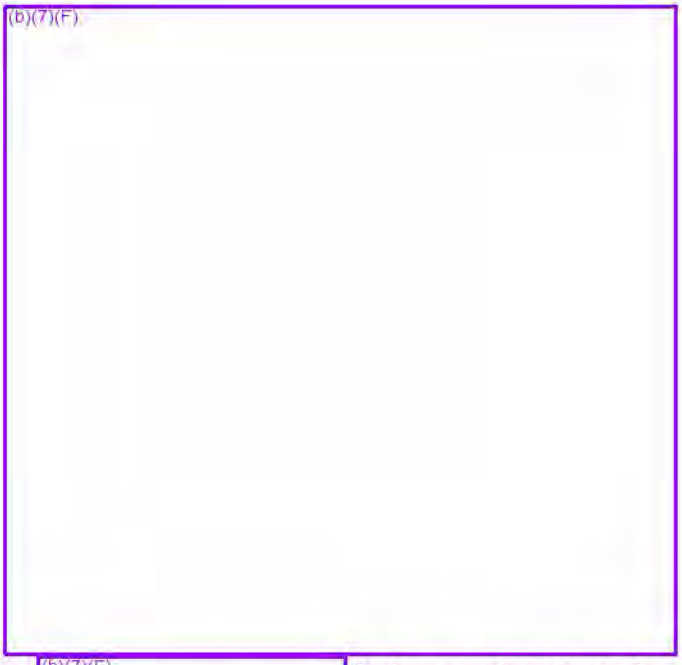
A fire, if started, would be of such a small magnitude that it could be extinguished by the operator using a hand fire extinguisher. The resulting smoke and vapors would be removed by the ventilation system in the case of Unit 3. For Units 1 & 2, the control room would be purged with portable equipment.

Essential auxiliary equipment is controlled by either stored energy, closing-type, air circuit breakers which are accessible and can be manually closed in the event DC control power is lost, or by AC motor starters which have individual control transformers.

7.7.5.1 Emergency (Auxiliary) Shutdown Panel

If temporary evacuation of the control room is required while operating at any power, the operator will trip the control rods and start the Keowee hydro units prior to evacuating the control room. (b)(7)(F) (b)(7)(F) After evacuation, the operator can establish and maintain a hot shutdown condition from the emergency shutdown panel located (b)(7)(F) The following instrumentation and controls are available on the emergency shutdown panel:

(b)(7)(F)



If (b)(7)(F) is in operation, it can be tripped from the 4.16 KV switchgear located on elevation 796' + 6". The operator has control of (b)(7)(F) at the emergency shutdown panel. Makeup to the letdown storage tank can be obtained, if desired, from one of the following sources:

1. RC Bleed Holdup Tank
2. Concentrated Boric Acid Storage Tank
3. Boric Acid Mix Tank

The necessary pumps can be controlled from the waste disposal control panel.

7.7.5.2 Standby Shutdown Facility

The Standby Shutdown Facility (SSF) provides a secondary alternate and independent means to achieve and maintain a hot shutdown condition for scenarios in which the Control Room is unavailable or equipment it controls is unavailable. The SSF was designed for safe shutdown during postulated fire, Turbine Building flooding, and physical security events. The following instrumentation and controls are available on the SSF:

SSF DIESEL GENERATOR AND STATION RELATED CONTROLS AND INSTRUMENTATION

1. Diesel Generator Annunciator Panel
2. Diesel Generator Controls
3. Diesel Generator Metering
4. Diesel Generator Syncroscope
5. SSF Power Systems Breaker Controls and Indicating Lights
6. SSF Power Systems Metering
7. SSF Diesel Engine Service Water Pump Control
8. SSF Diesel Engine Service Water Pump Discharge Flow Meter
9. SSF Auxiliary Service Water Pump Control

10. SSF Auxiliary Service Water Pump Discharge Flow Meter
11. SSF Sump Pump Controls

SSF UNIT RELATED CONTROLS AND INSTRUMENTATION

1. Unit Annunciator
2. Unit Recorder
3. (b)(7)(F)
4. Unit Process Indicators
   a. Pressurizer Level
   b. Pressurizer Pressure
   c. RC Loop A and B Hot Leg Temperatures
   d. RC Loop A and B Cold Leg Temperatures
   e. RC Loop A and B Pressure
   f. Steam Generator Level A and B
   g. Steam Generator Auxiliary Service Water Flow
5. (b)(7)(F)
6. Power Systems Alignment Indicating Lights

Reference Tables 9-15 and 9-16 for additional details on SSF controls and instrumentation.

7.7.6 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. The control functions initiated from local control stations do not directly involve either the Engineered Safeguards System if actuated or the Reactor Control System. Sufficient indicators and alarms are provided so that the Oconee control room operator is made aware of abnormal conditions involving remote control stations.

7.7.7 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 safeguards section 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 7.7.

7.8 Anticipated Transients Without SCRAM (ATWS) Mitigation System

7.8.1 Design Basis

The ATWS system that is installed at the Oconee Nuclear Station is based upon the B&WOG Generic ATWS Design Basis Document 47-1159091-00 dated October 9, 1985, subsequent B&WOG ATWS Committee submittal dated December 1, 1987, the Safety Evaluation Report on B&WOG 47-1159091-00 contained in the NRC letter to DPCo dated July 26, 1988, and the September 7, 1988 letter G. Holohan (NRC) to L. Stalter (B&WOG). The ATWS system was installed as required by the ATWS Rule, 10CFR50.62, "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants."

7.8.2 Systems Design

The ATWS Mitigation System is composed of two parts, the ATWS Mitigating Systems Actuation Circuitry (AMSAC) and the Diverse SCRAM System (DSS).

The ATWS Mitigation System Actuation Circuitry (AMSAC) and Diverse Scram System (DSS) consist of two Programmable Logic Controllers (PLC's) for the logic control circuits and two Uninterruptible Power Sources (UPS) connected to offsite power. Inputs from the field sensors are wired to the PLC's and outputs to the final actuation devices are wired using interfacing relays housed with the ATWS equipment cabinets and powered from the UPS. The UPS's are powered from a 120 VAC local panelboard backed by the Oconee Station emergency source (Keowee Hydroelectric Generating Station). The 2 UPS's are isolated from the emergency source by individual fuses coordinated with the panelboard circuit breakers and the upstream distribution network.

The AMSAC/DSS System consists of a two channel energize-to-trip design with the AMSAC portion actuated on low Feedwater Pump Turbine (FDWPT) control oil pressure or low Feedwater Pump (FDWP) discharge pressure while the DSS portion is actuated upon high Reactor Coolant System (RCS) Pressure.

All AMSAC/DSS PLC's and UPS power supplies are located in a stand-alone cabinet located above the Control Room in what is called the Ventilation Room. This location is convenient to the Control Room and allows easy access for testing and maintenance. This location is a Mild Environment.

All AMSAC/DSS process monitoring inputs are provided by existing Oconee instrumentation and control systems. RCS pressure inputs to the DSS which are analog signals are currently displayed on the Main Control Boards. Annunciator alarms are provided in the Control Room to alert the operator that one channel for either AMSAC or DSS has actuated.

7.8.2.1 AMSAC

Each channel of AMSAC uses existing inputs from the Feedwater System which monitor FDWPTA(B) hydraulic control oil pressure and FDWPA(B) discharge pressure signals (one per pump to each channel) from pressure switches which are part of the original Oconee feedwater system design.

These signals are multiplied using relays to provide the contact inputs which will be wired directly to the PLC's. These signals are processed using programmable logic resident in the PLC to provide the outputs to the Main Turbine and the Emergency Feedwater System.

AMSAC interfaces with the following systems and devices:

FROM	TO	ISOLATION
AMSAC PLC Interfacing Relays	Main Turbine Trip Solenoid	NE to NE
AMSAC PLC Interfacing Relays	EFDW Pump Start Circuits	NE to 1E
AMSAC Channels Actuation	Control Room Annunciator	NE to NE
NE = Non-Class 1E	1E = Class 1E	

Feedwater Pump Turbine Oil Pressure is sensed by pressure switches in the Feedwater Pump Turbine Control Console on the turbine standard. These switches are then multiplied using control relays for output to various plant control, monitoring and alarm circuits. AMSAC will be one of the end users of these signals.

Feedwater Pump Discharge Pressure is sensed by pressure switches in the discharge lines of each individual pump. These switches are then multiplied using control relays for output to various plant control, monitoring and alarm circuits. AMSAC will be one of the end users of these signals.

7.8.2.2 DSS

Each channel of DSS uses a Wide Range RCS Pressure signal supplied via an analog isolator from the Westinghouse supplied Reactor Vessel Level Indication System (RVLIS). These signal loops also provide the Regulatory Guide 1.97 wide range RCS pressure indications on the main control board. The DSS utilizes the signal conditioning equipment which is resident in the RVLIS cabinet through an isolation device that separates the Class 1E RVLIS from the Non-Class 1E DSS. DSS trip actuation is initiated at a setpoint of 2450 ± 25 psig using the logic in the PLC. Outputs from both channels of the PLC's are combined to make the required two-out-of-two logic. DSS provides two digital inputs (one per channel) to the CRD system. Upon actuation of both channels of DSS, the CRD system opens a normally-closed solid-state relay contact in each of the 138 Single Rod Power Supply (SRPS) modules. This interrupts power to the CRDM's causing all control rods (except the captured APSR's) to fall into the core resulting in a reactor trip. DSS also signals the ICS to raise the Turbine Bypass Valve pressure setpoint to ensure shutdown margin requirements are maintained.

DSS interfaces with the following systems and devices:

FROM	TO	ISOLATION
DSS Interfacing Relays	Single Rod Power Supplies	NE to NE
DSS Interfacing Relays	TBV's Control Setpoint	NE to NE
Deleted Row(s) per 2009 Update		
DSS Channel Actuation	Control Room Annunciator	NE to NE
WR RCS Pressure (RVLIS)	DSS PLC Channels	1E to NE
NE = Non-Class 1E	1E = Class 1E	

The Control Rod Drive (CRD) System also provides an input from the CRD Diamond panel located in the main Control Room into the DSS logic for reset of the CRD SRPS modules.

7.8.2.3 Testing

Inputs are also provided from the ATWS test panel. The panel is resident in the PLC cabinet along with other ATWS equipment.

Periodic testing will use a Bypass/Enable switch located on the test panel for testing each channel of AMSAC and DSS logic in the PLC. Whenever this switch is not in the ENABLE position, a continuous indicator in the Control Room will be illuminated and a computer alarm will be generated for display in the Control Room on a CRT. Status indication of all inputs and outputs are on the test panel.

These systems are designed so that both are two out of two logic actuated systems, and provisions are incorporated which allow disabling of the system output when one of the channels is placed in test. This prevents accidental initiation of the systems during individual channel testing.

7.8.2.4 AMSAC and DSS I/O

Each input to the AMSAC and DSS logic is provided with complete indications and alarms that alert the operator to an off-normal status that might preclude proper response to an ATWS event. Each plant variable that inputs into the AMSAC and DSS is monitored as part of the existing plant indications and provide the operator with information relevant to the status of each variable prior to reaching the AMSAC or DSS set point.

Outputs from the PLC's are provided through interfacing relays located in the ATWS equipment cabinets. These relays provide the outputs to the Main Turbine, Turbine Bypass Valve Set Point, the Emergency Feedwater Pumps, and the Control Rod Drive System for Single Rod Power Supplies via the CRD system PLC. The relays used are powered by the UPS. Each PLC channel output relays will be wired to the above devices in a manner such that both channels of AMSAC/DSS are required for the devices to trip, start, or drop. The relays also provide output status information to the operator.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.8.

THIS PAGE LEFT BLANK INTENTIONALLY.

7.9 Automatic Feedwater Isolation System (AFIS)

7.9.1 Design Basis

The Automatic Feedwater Isolation System (AFIS) circuitry is designed to address containment over-pressurization concerns, unacceptable thermal stresses to the steam generator tubes, and significant core overcooling by isolating main and emergency feedwater to the faulted steam generator during a Main Steam Line Break event. AFIS is credited in the steam line break containment response analysis (Section 6.2.1.4) and the steam line break tube stress analysis (Section 5.2.3.4). AFIS is not credited for the steam line break core response analyses (Sections 15.13 and 15.17). The design basis of the system includes the items of Section 7.1.2 with the following additions:

7.9.1.1 Loss of Power

1. The loss of vital bus power to an analog channel will cause a loss of signal to that analog channel creating a 1-out-of-4 coincidence without AFIS actuation.
2. The loss of vital bus power to a digital channel will not initiate system actuation.

7.9.1.2 Equipment Removal

1. Removal of an isolation module from the AFIS system will require a bypass on 2 analog channels (for AFIS and Trip Confirm modules) in both digital channels or AFIS system actuation will occur.
2. Removal of a logic module from one protective digital channel does not affect the other protective digital channel and does not initiate system action.

7.9.1.3 Control Logic of AFIS System

AFIS has priority over the automatic actuation/operation of systems affected. All systems receiving the AFIS signal remain controlled by AFIS unless manual control is taken. The affected EFW pumps can be operated manually to override the AFIS actuation. A separate deliberate action is required to place the affected systems in manual prior to performing a reset of the AFIS functions.

7.9.2 System Design

7.9.2.1 System Logic

The AFIS instrumentation is designed to provide automatic termination of feedwater and emergency feedwater flow to the affected steam generator. The AFIS instrumentation automatically terminates Main Feedwater (MFW) by tripping both MFW pumps and closing the affected steam generator's main and startup feedwater control valves (MFCV and SFCV) and block valves. Although the main and startup feedwater block valves are automatically closed, their closure is not credited for mitigation of a MSLB. The AFIS logic automatically terminates emergency feedwater (EFW) by stopping the turbine-driven emergency feedwater pump (TDEFWP) and tripping the motor-driven emergency feedwater pump (MDEFWP) aligned to the affected steam generator. Manual overrides for the TDEFWP and MDEFWPs are provided to allow the operator to subsequently start the EFW pumps if necessary.

In addition, AFIS actuation limits EFW pump runout in the event of a MSLB and certain large break MFW line breaks with the pump in the automatic mode of operation.

Main Steam header pressures are used as input signals to the AFIS circuitry. There are four QA-1 pressure transmitters per header with each feeding a steam pressure signal to a signal isolator. The output

of the signal isolator provides an analog signal to a processor module that actuates isolation functions at desired setpoints. One pressure transmitter per header and associated cabling and resistors constitute an AFIS detection analog channel.

The four AFIS analog channels per header feed two redundant AFIS digital channels. Each digital channel provides independent circuit functions to isolate each steam generator. If the logic is satisfied, a trip output is energized. The use of an energized-to-trip processor module ensures that a loss of power to the digital channel will not result in inadvertent feedwater isolation. If either digital channel is actuated, feedwater is isolated to the affected steam generator. Energizing the trip outputs results in the actuation of contacts in various control circuits for systems and components used for the MSLB and feedwater line break mitigation. Therefore, when the trip outputs are actuated, the systems and components perform their isolation functions. Other features of the digital channels include header specific manual initiation pushbuttons, a header specific ENABLE/OFF switch, and redundant "trip confirm" modules for each digital channel. The AFIS digital channel is defined as the analog isolation modules, the (4) digital 2-out-of-4 logic modules (Framatome STAR), the ENABLE/OFF pushbutton, the manual initiation pushbutton, the associated trip relays, the trip relay outputs to the feedwater pumps, the switchgear trips for the MDEFWP, the solenoid valves for the MFCV and SFCV, the trip solenoid valves for the feedwater pumps, and the TDEFWP trip function. While AFIS provides isolation of the feedwater block valves, this is not a credited function and is not a requirement for digital channel operability.

The AFIS digital channels are enabled and disabled administratively rather than automatically. Appropriate operating procedures contain provisions to enable/disable the digital channels.

7.9.2.2 Trip Setpoints

Trip setpoints are the nominal values that are user defined in AFIS software. An AFIS analog channel is considered to be properly adjusted when the AS LEFT value is within the band for channel calibration accuracy.

The trip setpoints used in the AFIS software are selected such that adequate protection is provided when all sensor and processing time delays are taken into account. The trip setpoints are set for low main steam pressure and a high rate of depressurization associated with a specific steam generator. To allow for calibration tolerances, instrumentation uncertainties, instrument drift, the allowable values specified are conservatively adjusted with respect to the analytical limits. The actual nominal trip setpoint entered into the software is controlled procedurally.

7.9.2.3 Availability of Information

All system analog signals are indicated within the system cabinets and are monitored by the plant computer. All BWNT STAR module outputs are indicated within the cabinets and their state monitored by the plant computer. Plant annunciators provide the operator with immediate indication of changes in the status of the processor module inputs and outputs. The following conditions are annunciated for the AFIS system:

1. Digital Channel 1 Test/Disable
2. Digital Channel 2 Test/Disable
3. AFIS Initiate Header A
4. AFIS Initiate Header B
5. AFIS Analog Channel Trip

Initiation of Header A (3) or Header B (4) requires simultaneous detection by both the "primary" and "trip confirm" modules of either of the Digital Channels for the Low Pressure Trip. Inadvertent actuation

of the "primary" low pressure trip without confirmation from the "trip confirm" function or actuation of the "trip confirm" by itself will not result in an AFIS system actuation but will be annunciate on the appropriate "trouble" annunciator (1 or 2). The STAR modules indicate when any "one out of four" analog channel trip occurs, which the annunciator (5) will be illuminated.

7.9.2.4 Summary of Protective Action

The AFIS circuitry is designed to address containment over-pressurization concerns and thermal stresses on steam generator tubes by isolating feedwater to the faulted steam generator during a Main Steam Line Break event. Two conditions apply for AFIS actuation:

1. Low main steam pressure
2. Low main steam pressure and a high rate of depressurization

In response to the first condition of low main steam pressure, the AFIS circuitry trips the main feedwater pumps and trips or prevents the turbine driven emergency feedwater pump from automatically starting by redundantly and independently closing valves, MS-93 and MS-95. The AFIS circuitry also closes the main and startup feedwater control and block valves on the affected header.

In response to the second condition, AFIS circuitry performs the same actions as in the first condition with the addition of redundant trip signals to the motor driven emergency feedwater pump associated with the faulted steam generator.

7.9.3 System Evaluation

The four AFIS analog channels per steam generator feed two redundant feedwater digital channels. Each digital channel provides independent circuit functions to isolate each steam generator. If the logic is satisfied, a trip output is energized. The use of an energized-to-trip processor module ensures that a loss of power to the digital channels will not result in inadvertent feedwater isolation. If either digital channel is actuated, feedwater to the affected steam generator is isolated. Energizing the trip outputs results in actuation of contacts in various control circuits for systems and components used for the MSLB and feedwater line break mitigation. Therefore, when the trip outputs are actuated, the systems and components perform their isolation functions. While AFIS provides isolation of the feedwater block valves, this is not a credited function and is not a requirement for digital channel operability.

There is redundancy of sensors, logic, and equipment, excluding the main feedwater equipment. The redundancy is preserved and kept effective by independence of sensors, instrument strings, logic, and control elements in the final actuator. These characteristics enable the system to tolerate single failures at all levels.

To prevent a single-failure from causing loss of feedwater flow to one or both headers inadvertently, a redundant trip confirm function is provided that must also detect the low pressure trip condition in order to create an AFIS low pressure trip.

The system protective devices require electrical power in order to operate and perform their functions. The power for the STAR modules is taken from the plant's system of battery-backed vital buses since loss of power at this level could affect the performance capability of the system. The system will tolerate the loss of one vital bus without loss of protective capability.

7.9.3.1 Redundancy and Diversity

The system as evaluated above is shown to have sufficient diversity and redundancy to withstand single failures at every level, excluding the main feedwater components associated with AFIS.

7.9.3.2 Electrical Isolation

The use of analog isolation will effectively prevent adverse affects of faults (shorts, grounds, or cross connection of signals) on any analog signal leaving the system from being reflected into or propagating through the system. The isolation amplifier circuits have been qualified to isolate the output signal from input circuit faults. The STAR module employs diverse software to mitigate common mode failures.

Separation of redundant AFIS functions is accomplished by maintaining isolation for the power, control, equipment location, and cable routing between channels.

AC power for AFIS channels is supplied from independent vital power panels. Analog channel 1 is supplied from Vital Power Panelboard KVIA. Analog channel 2 is supplied from Vital Power Panelboard KVIB. Analog channel 3 is supplied from Vital Power Panelboard KVIC. Analog channel 4 is supplied from Vital Power Panelboard KVID. The digital channels, 1 and 2, are supplied from AC panelboards, KVIC and KVID, respectively. The devices controlled by the digital channels are supplied by redundant and independent QA-1 sources of power. These are described in Section 8.3.

7.9.3.3 Physical Separation

The arrangement of modules within the system cabinets is designed to reduce the chance of physical events impairing system operation. Channel specific control wiring between the STAR modules and the final actuating devices is physically separated and protected against damage, which could impair system operation. The equipment is separated to limit the possibility of spurious actuation.

Separation between redundant channels of equipment, control cables, and power cables provides defense of redundant AFIS functions. Power and control cables for redundant elements of AFIS equipment are routed in separate cable trays.

7.9.4 Periodic Testing and Reliability

The redundancy of the logic and the division of protective devices between channels form a system having two parallel protective channels either of which is capable of performing the required functions. These characteristics are basic to an inherently reliable system.

The built-in test facilities permit an electrical actuation test of each analog instrument string by the substitution of signals at the STAR module inputs. The AFIS STAR module provides both manual and automated test capability, and self-diagnostic tests performed during start-up and operation. The front panel of each of the STAR module has LED indicators, which indicate module status.

When testing, chance of an inadvertent initiation of an AFIS low pressure trip is minimized by the trip confirm function which requires actuation by both the primary and trip confirm modules.

When an analog instrument string is placed in test or bypass, the logic assigned to the digital control module changes the actuation logic to a 2-in-3 coincidence. This assures that placing an analog channel in test cannot defeat the protective action.

On-line checks of the system will confirm the normal state of the system, principally by comparative readings of similar analog indications between redundant measurements and by the status lamps on the logic modules.

7.9.5 Manual Initiation

A manual initiation switch is provided in each Automatic Feedwater Isolation System digital channel. The manual initiation switches are capable of actuating trip outputs without relying on the STAR outputs. There are two control switches on the control room board for the disabling of each digital channel and two control switches for manually initiating the respective header circuitry.

7.9.6 Bypassing

Bypassing must be initiated manually within a fixed pressure band above the protective system actuation point. The removal setpoints are above the actuation setpoints in order to obtain a pressure band in which the system actuation may be bypassed during a normal cooldown and startup. The bypasses do not prevent automatic actuation of the emergency feedwater pumps. Bypassing is under administrative control. Once a bypass has been initiated, the plant annunciator indicates the condition on Unit 1 only and by the OAC for all units.

After actuation of AFIS, the turbine driven and motor driven emergency feedwater pumps can be manually actuated or restarted from their respective control switches.

7.9.7 Deleted Per 2002 Update

7.9.8 Deleted Per 2002 Update

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.9.

THIS PAGE LEFT BLANK INTENTIONALLY.

7.10 Diverse Low Pressure Injection Actuation System (DLPIAS)

7.10.1 Design Basis

A Defense-in Depth and Diversity (D^3) Analysis was performed per the guidelines of BTP HICB - 19. This analysis resulted in the inclusion of a Diverse Low Pressure Injection Actuation System (DLPIAS). The system is designed as diverse backup for ESPS during the unlikely event of a Large Break Loss of Coolant Accident (LBLOCA) concurrent with a Software Common Mode Failure (SWCMF) of the ESPS digital equipment.

7.10.2 System Design

The DLPIAS is a combination of both safety-related and non-safety-related components. The DLPIAS design does not require the use of any software. All DLPIAS process monitoring inputs are provided by existing Oconee instrumentation and control systems. The DLPIAS utilizes analog pressure input signals from the Reactor Coolant System (RCS), which are displayed on the Main Control Boards. RCS input pressure signals are isolated from the safety-related signals by the ESPS signal isolators. The signal is split on the front end of the ESPS and is not affected by the software of the ESPS computers. The analog RCS pressure signals provide input to the DLPIAS bistable trip units which output to a 2-out-of-3 relay logic circuit to actuate the ESPS Channel 3 and 4 devices. Power for the bistables and relay logic is non-safety-related.

The DLPIAS is actuated on low RCS Pressure. The system is designed as a diverse backup for ESPS during the unlikely event of a LBLOCA concurrent with a SWCMF of the ESPS digital equipment. A low RCS pressure condition is the most appropriate indication that a LBLOCA has occurred. Because the DLPIAS is a backup system for LBLOCA, the setpoint for actuation of the DLPIAS is chosen such that the ESPS actuation of the LPI components will occur prior to DLPIAS actuation.

Physical separation is maintained between safety-related and non-safety-related components per IEEE Std 384-1992 separation criteria. The bistables and relays are rail mounted components. Electrical separation between safety-related and non-safety-related components is maintained by the use of signal isolators for the analog signals and relays. All equipment associated with the DLPIAS, with the exception of the RCS pressure transmitters and associated cabling, is located in the Control Room and is qualified for a mild environment.

The DLPIAS 2-out-of-3 relay logic minimizes an inadvertent actuation of the LPI components. The circuit relays are energized to actuate, therefore loss of power will not result in actuation of the trip circuit. The design includes a DLPIAS Bypass Switch located on the Unit Control Board. The switch is used to bypass the DLPIAS system for both maintenance and operations.

Procedures require that the DLPIAS be bypassed on controlled shutdowns at the same time the LPI Bypass is initiated for the ESPS. The interface with the LPI actuation circuit is safety- related. The design includes indications in the Control Room for a DLPIAS trip, DLPIAS Bypass, and DLPIAS Bistable Tripped. The indication circuits are non-safety-related.

A DLPIAS Override switch is located on the unit board which allows operators to override the DLPIAS in case of an inadvertent actuation. Once the override is initiated, operators are able to manually position ESPS components.

Manual initiation of LPI is accomplished with the existing ESPS Trip/Reset buttons located on the main control board. The logic for this manual trip bypasses the ESPS logic and allows the Operator to initiate actuation on a per channel basis.

7.10.3 Testing

Periodic testing of DLPIAS will use the Bypass Switch located on the Control Board for testing each output channel of DLPIAS. Whenever this switch is in the Bypass position, an indicator in the Control Room will be illuminated continuously.

These systems are designed so that a 2-out-of-3 relay logic actuates the system, and provisions are incorporated which allow disabling of the system output when the protective channels are placed in test. This prevents accidental initiation of the system during protective channel testing.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.10.

7.11 Diverse High Pressure Injection Actuation System (DHPIAS)

7.11.1 Design Basis

Duke committed to install a Diverse High Pressure Injection Actuation System (DHPIAS). This system is designed as a diverse backup for ESPS during the unlikely event of a Small Break Loss of Coolant Accident (SBLOCA) concurrent with a Software Common Mode Failure (SWCMF).

7.11.2 System Design

The DHPIAS is a combination of both safety-related and non-safety-related components. The DHPIAS design does not require the use of any software. All DHPIAS process monitoring inputs are provided by existing Oconee instrumentation and control systems. The DHPIAS utilizes analog pressure input signals from the Reactor Coolant System (RCS), which are displayed on the Main Control Boards. RCS input pressure signals are isolated from the safety- related signals by the ESPS signal isolators. The signal is split on the front end of the ESPS and is not affected by the software of the ESPS computers. The analog RCS pressure signals provide input to the DHPIAS bistable trip units which output to a 2-out-of-3 relay logic circuit to actuate ESPS Channel 1 and 2 devices. Power for the bistables and relay logic is non-safety-related.

The DHPIAS is actuated on low RCS Pressure. This system is designed as a diverse backup for ESPS during the unlikely event of a SBLOCA concurrent with a SWCMF of ESPS digital equipment. A low RCS pressure condition is the most appropriate indication that a SBLOCA has occurred. Because the DHPIAS is a backup system, the setpoint for actuation of the DHPIAS is chosen such that the ESPS actuation of the HPI components will occur prior to DHPIAS actuation.

Physical separation is maintained between safety-related and non-safety-related components per IEEE Std 384-1992 separation criteria. The bistables and relays are rail mounted components. Electrical separation between safety-related and non-safety-related components is maintained by the use of signal isolators for the analog signals and relays. All equipment associated with DHPIAS, with the exception of the RCS pressure transmitters and associated cabling, is located in the Control Room and is qualified for a mild environment.

The DHPIAS 2-out-of-3 relay logic minimizes an inadvertent actuation of the HPI components. The circuit relays are energized to actuate, therefore loss of power will not result in actuation of the trip circuit. The design includes a DHPIAS Bypass Switch located on the Unit Control Board. The switch is used to bypass the DHPIAS system for both maintenance and operations.

Procedures require that the DHPIAS be bypassed on controlled shutdowns at the same time the HPI Bypass is initiated for the ESPS. The interface with the HPI actuation circuit is safety- related. The design includes indications in the Control Room for a DHPIAS trip, DHPIAS Bypass, and DHPIAS Bistable Tripped. The indication circuits are non-safety-related.

A DHPIAS Override switch is located on the unit board which allows operators to override the DHPIAS in case of an inadvertent actuation. Once the override is initiated, operators are able to manually position ESPS components.

Manual initiation of HPI is accomplished with the existing ESPS Trip/Reset buttons located on the main control board. The logic for this manual trip bypasses the ESPS logic and allows the Operator to initiate actuation on a per channel basis.

7.11.3 Testing

Periodic testing of DHPIAS will use the Bypass Switch located on the Control Board for testing each protective channel of DHPIAS. Whenever this switch is in the Bypass position, an indicator in the Control Room will be illuminated continuously.

These systems are designed so that a 2-out-of-3 relay logic actuates the system, and provisions are incorporated which allow disabling of the system output when the protective channels are placed in test. This prevents accidental initiation of the system during protective channel testing.

THIS IS THE LAST PAGE OF THE TEXT SECTION 7.11.