7 INSTRUMENTATION AND CONTROLS

7.1 INTRODUCTION

Complete supervision of both the nuclear and turbine-generator sections of the plant is accomplished by the instrumentation and control systems from the control room. This supervision includes the capability to periodically test the operability of the Reactor Trip System (RTS) while on-line.

In 1996, the NRC issued Generic Letter 96-01 (*Reference 3*) to notify licensees about problems with testing of safety-related logic circuits and to request that surveillance procedures be reviewed and modified as necessary to ensure that all portions of the logic circuitry, including parallel logic, interlocks, bypasses and inhibit circuits, are adequately covered to fulfill Technical Specification requirements. RG&E's response to GL 96-01 (*Reference 4*) stated that the NRC's requested actions would be complied with. In *Reference 5*, RG&E informed the NRC that the safety-related circuits had been evaluated and tested utilizing the criteria of GL 96-01 and that identified procedural deficiencies had been corrected and identified procedural weaknesses would be resolved within the allotted time period stipulated in GL 96-01. RG&E in *Reference 6* notified the NRC that all required actions for GL 96-01 had been completed. The NRC in *Reference 7* reviewed and accepted RG&E's response and closed out GL 96-01.

7.1.1 IDENTIFICATION OF SAFETY-RELATED SYSTEMS

The protection systems consist of both the Reactor Trip System (RTS) and the engineered safety features. Equipment supplying signals to any of these protective systems is considered a part of that protective system.

Design criteria for protection systems should permit maximum effective use of process measurements both for control and protection functions, thus enhancing the capability to provide an adequate system to deal with the majority of common-mode failures as well as to provide redundancy for critical control functions. The design approach provides a protection system which monitors numerous system variables by different means, i.e., protection system diversity. This diversity has been evaluated for a wide variety of postulated accidents (*Reference 1*).

Instrumentation and controls essential to avoid undue risk to the health and safety of the public are provided to monitor and maintain neutron flux, primary coolant pressure, flow rate, temperature, and control rod positions within prescribed operating ranges.

The non-nuclear regulating process and containment instrumentation measures temperatures, pressure, flow, and levels in the reactor coolant system, steam systems, containment, and other auxiliary systems. Process variables required on a continuous basis for the startup, operation, and shutdown of the plant are indicated, recorded, and controlled from the control room into which access is supervised. The quantity and types of process instrumentation provided ensure safe and orderly operation of all systems and processes over the full operating range of the plant.

7.1.2 IDENTIFICATION OF SAFETY CRITERIA

7.1.2.1 General Design Criteria

During the licensing of Ginna Station the criterion which applied in common to all instrumentation and control systems was General Design Criterion 12 (GDC 12) which was included in the Atomic Industrial Forum (AIF) version of proposed criteria issued by the AEC for comment on July 10, 1967. The AIF criteria including AIF-GDC 12 are discussed in detail in Section 3.1.1.

The design of the instrumentation and control systems was reviewed in 1972 (*Reference 2*) on the bases of the General Design Criteria contained in Appendix A to 10 CFR 50 and the criteria included in IEEE 279-1971, both of which were promulgated after the licensing of Ginna Station. Compliance of the design with 1972 General Design Criteria of Appendix A to 10 CFR 50 is discussed in Section 3.1.2.

Evaluation of the design with respect to guidance provided in Safety and Regulatory Guides effective in 1972 is discussed in Section 1.8.

7.1.2.2 Compliance with IEEE 279-1971

Compliance with IEEE 279-1971 Criteria for Protection Systems For Nuclear Power Generating Stations is discussed below.

7.1.2.2.1 **Design Basis**

The Ginna Station conditions which require protective system action are enumerated in the Technical Specifications. The Ginna Station variables that are required to be monitored and the levels that when reached will require protective action are also described in the Technical Specifications. The protection system is designed to perform automatically with precision and reliability to initiate appropriate protective action when required.

The source, intermediate, and power range sensors, their locations and range of operation, are described in Section 7.7.3. The neutron sensors are the only Ginna Station protective system components possessing a spatial dependence. The number of source, intermediate, and power range neutron-flux-measuring sensors, which can be inoperable without deleterious effect on the safety of continued Ginna Station operation are described in the Technical Specifications.

The instrumentation systems are designed to perform their functions while accommodating system response times and inaccuracies. The Technical Specifications list the limiting safety system settings for protective instrumentation. Instrument errors, setpoint errors, instrument delay times, and calorimetric errors are taken into account in transient analyses, which are discussed in Chapter 15.

Prudent operational limits for each variable referenced above are interpreted to be those levels, which will produce alarms but will not necessarily produce a protective system action. Each process variable referenced above has, in addition to its alarm function, a level providing protection system action. These values are called out and verified in the

preoperational tests that were performed. The operational modes in which these are applicable are specified in the Technical Specifications.

The range of transient and steady-state conditions of both the energy supply and the environment during normal, abnormal, and accident circumstances throughout which the system must perform has been evaluated and appropriate features have been incorporated to accommodate them. The Reactor Trip System (RTS) is designed to fail safe, i.e., to produce a protective action in the event of loss of power to the protection system. All system components are designed to operate indefinitely under the environmental conditions to which they are exposed under both steady-state and transient, and normal and anticipated abnormal station operating conditions. Reactor Trip System (RTS) components, which can be exposed to excessive heat, humidity, and pressure due to the accidents described in Chapter 15, are qualified to perform their required functions for the duration of time required for engineered safety features operation and postaccident monitoring. Environmental qualification is discussed in Section 3.11.

Because of the design, physical separation and electrical isolation, fire, missiles, and natural phenomena are not likely to affect a sufficient number of channels so as to compromise the system functions. Compliance with the separation and single-failure criteria and "fail safe" design ensure that the system will operate reliably on demand. All channels of the Reactor Trip System (RTS) are subject to the same environmental conditions in the control room although channel separation and electrical isolation are maintained. Should evacuation of the control room be required, alternative means of safely shutting down Ginna Station from outside the control room are provided. These are discussed in Section 7.4.3.

The protection system seismic design requirements are such that the safe shutdown earthquake will not result in loss of the system function. Seismic qualification is discussed in Section 3.10.

7.1.2.2.2 **Requirements**

7.1.2.2.2.1 Operability

The Ginna Station protection systems, with precision and reliability, automatically initiate appropriate protective action whenever a condition monitored by the system reaches a preset level. The Reactor Trip System (RTS) will automatically initiate load cutbacks, inhibit rod withdrawal, or trip the reactor depending on the severity of the condition. The instrumentation used to initiate action other than trip is generally similar to the Reactor Trip System (RTS). The protection systems are further described in Section 7.2.

As described in Section 7.2, the protection systems not only accommodate any single failure without loss of function but also provide protection against spurious actuation because of the coincident logic design.

The quality of instruments and components for use in the protection system was specifically examined during the design to ensure that they were consistent with the objectives of minimum maintenance and low failure rates.

Channel independence is carried through the system extending from the sensor to the relay providing the logic. The ac power supplies to the channels are excited by four separate instrument buses. Independence is maintained by use of separate channel penetrations, cable trays, and equipment compartments.

Control and protection systems employ the same measurement where applicable. The protection is separate and distinct from the control system. Control signals which are derived from the protection system measurements are transferred through isolation amplifiers. This prevents a failure in the control circuitry from affecting the protection system. The isolation amplifiers are classified protection system components and have been qualified by testing under conditions of maximum postulated faults.

The design is such that a single random failure which could cause a control system action resulting in a station condition requiring protection is seen as a trip demand in the channel designed to protect against the condition. The remaining redundant protection channels may be degraded by a second random failure or removed from service without loss of the protection function.

The design provides a protection system which monitors a wide spectrum of process variables by different means. Equipment, location, and measurement diversity protects against multiple failures from a credible single event.

Routing and separation standards applicable to existing cables are those that were invoked at the time of cable installation. For more information, see Section 8.3.1.4.

7.1.2.2.2.2 Testability

The entire protection system has the capability of being tested and calibrated with the reactor at power. Testing is discussed in Section 7.2. All instrumentation has the capability for sensor checks. Sensor testing can be done by perturbing the system variable, introducing a substitute input or by comparing sensors which measure a like variable.

The system is designed to permit any one channel to be maintained and when required, tested or calibrated during power operation without system trip. During such operation, the active parts of the system continue to meet the single-failure criterion. Exception is made in the one-of-two systems that are permitted to violate the single-failure criterion during channel bypass provided that acceptable reliability of operation can be otherwise demonstrated.

Operating bypasses that are removed automatically are restored automatically when permissive conditions are not met. Manual bypasses (located on the control board) that are immediately available to the operator are automatically reset or may be manually reestablished by the operator. Manual bypasses that are not automatically reset are designed to permit administrative control over their use. In all cases, there is continuous indication in the control room if the trip function of some part of the system has been bypassed or taken out of service.

7.1.2.2.2.3 Control of Protective Actions

The protection system is designed so that once initiated, a protective action will go to completion. The return of the plant to MODES 1 and 2 will require deliberate operator action.

Administrative control of the means of manually bypassing a channel or protective function is provided by controlling access to the control room and areas where a bypass can be affected.

Where multiple setpoints have been designed into the Ginna Station protection system, the design is in accordance with the other criteria of this standard. Means are provided for manual initiation of the protective system action. Failures in the automatic system do not prevent the manual actuation. The manual actuation requires the operation of a minimum of equipment.

Access to setpoint adjustment, calibration, and test points are designed to be under administrative control.

All protective actions are indicated and identified down to the channel level. Also, each is designed to provide the operator with accurate, complete, and timely information pertinent to its own status.

REFERENCES FOR SECTION 7.1

1. T. W. T. Burnett, Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors, WCAP-7306, Westinghouse Corporation, April 1969.

2. Rochester Gas and Electric Corporation, Technical Supplement Accompanying Application for Full-Term Operating License, August 1972.

3. Generic Letter 96-01, Testing of Safety-Related Logic Circuits, dated January 10, 1996.

4. Letter from R. C. Mecredy, RG&E, to A. R. Johnson, NRC, Subject: Response to Generic Letter 96-01, dated April 18, 1996.

5. LER 96-005, Subject: Deficient Procedures for Testing of Safety-Related Logic Circuits, Identified Using Criteria of NRC Generic Letter 96-01, Resulted in Condition Prohibited by Technical Specifications, dated June 17, 1996.

6. Letter from R. C. Mecredy, RG&E, to G. S. Vissing, NRC, Subject: Notification of Completion of Requested Actions for 1996, Testing of Safety-Related Logic Circuits, dated December 19, 1997.

7. Letter from G. S. Vissing, NRC, to R. C. Mecredy, RG&E, Subject: Completion of Licensing Action for Generic Letter 96-01, "Testing of Safety-Related Logic Circuits", dated January 14, 1998.

7.2 REACTOR TRIP SYSTEM (RTS)

7.2.1 DESIGN BASES

7.2.1.1 Design Criteria

The following design criteria were used during the licensing of Ginna Station. They represent the Atomic Industrial Forum (AIF) version of proposed criteria issued by the AEC for comment on July 10, 1967 (see Section 3.1.1). Conformance with 1972 General Design Criteria of 10 CFR 50, Appendix A, is discussed in Section 3.1.2. The criteria discussed in Section
3.1.2 as they apply to the Reactor Trip System (RTS) include 2, 4, 13, 19, 20, 21, 22, 23, 24, 25, and 29. Conformance with IEEE 279-1971 is discussed in Section 7.1.2.

7.2.1.1.1 Fuel Damage Limits

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

The Reactor Trip System (RTS) is designed to trip the reactor, when necessary, to prevent or limit fission product release from the core.

The reactor possesses high-speed Westinghouse magnetic-type control rod drive mechanisms. The reactor internal components, fuel assemblies, control rod assemblies, and unlatching mechanisms for the drive system components are designed as Seismic Category I equipment.

Two reactor trip breakers are provided to interrupt power to the control rod drive mechanisms. The breaker main contacts are connected in series with the power supply to the mechanism coils. The trip breakers are opened by the trip devices described in Section 7.2.2.1.5. Each protection channel actuates two separate trip logic trains, one for each reactor trip breaker. The electrical state of the devices providing signals to the trip breakers causes these breakers to trip in the event of power loss. Opening either trip breaker interrupts power to the magnetic latch mechanisms on each control rod drive, causing them to release the rods and allowing the rods to insert by gravity into the core. The reactor shutdown function of the rods is completely independent of the normal control functions because the trip breakers completely interrupt the power supply to the rod mechanisms and thereby negate any possibility of response to control signals. The control rods must be energized to remain withdrawn from the core. An automatic reactor trip occurs on loss of power to the control rods. All components that are required to perform the reactor trip function are classified as safety-related equipment

The Reactor Trip System (RTS) receives, from plant instrumentation, signals that are indicative of an approach to an unsafe operating condition, actuates alarms, prevents control rod motion, initiates load runback, and/or opens the reactor trip breakers, depending on the severity of the condition.

The basic reactor trip philosophy is to define a region of power and coolant temperature conditions allowed by the primary trip functions, the overpower delta T trip, the overtemperature delta T trip, and the nuclear overpower trip. The allowable operating region within these trip

settings is provided to prevent any combination of power, temperature, and pressure that could result in a departure from nucleate boiling with all reactor coolant pumps in operation. Additional trip functions such as a high pressurizer pressure trip, low pressurizer pressure trip, high pressurizer water level trip, loss-of-flow trip, steam generator low-low water level trip, turbine trip, safety injection trip, nuclear source and intermediate range trip, and manual trip are provided to back up the primary trip functions for specific accident conditions and mechanical failures.

A rod stop is initiated by a dropped rod signal to provide additional core protection. The dropped rod is indicated by individual rod position indicators and by a rapid flux decrease on any of the power range nuclear channels.

Rod stops from nuclear overpower, overpower delta T, overtemperature delta T, and T_{AVG} deviation are provided to prevent abnormal power conditions which could result from excessive control rod withdrawal initiated by a malfunction of the reactor control system or by operator violation of administrative procedures. The automatic rod withdrawal function of the reactor control system has been disabled. Rod stops (blocks) for automatic rod withdrawal are no longer required.

7.2.1.1.2 **Reliability and Testability**

CRITERION: Protection systems shall be designed for high functional reliability and inservice testability necessary to avoid undue risk to the health and safety of the public (AIF-GDC 19).

The reactor uses a higher speed version of the Westinghouse magnetic-type control rod drive mechanisms (CRDM) used in the San Onofre and Connecticut Yankee plants. The replacement control rod drive mechanisms (CRDM) provided by PCR 2001-0042 are Westinghouse design, manufactured by Framatome, Jeumont Plant. Upon a loss of power to the coils, the lead screws are released, allowing the control rods to fall by gravity into the core.

The reactor internals, fuel assemblies, rod cluster control assemblies, and drive system components (as required for trip) are designed as Seismic Category I equipment. The rod cluster control assemblies are fully guided through the fuel assembly for the maximum travel of the control rod into the guide tube. Furthermore, the rod cluster control assemblies are never fully withdrawn from their guide thimbles in the fuel assembly. Due to this and the flexibility designed into the rod cluster control assemblies, abnormal loadings and misalignments can be sustained without impairing operation of the rod cluster control assemblies.

The rod cluster control rod guide system throughout its length is locked together with pins, bolts and welds to ensure against misalignments which might impair control rod movement under normal operating conditions and credible accident conditions.

All reactor protection channels are supplied with sufficient redundancy to provide the capability for channel calibration and test at power. Bypass removal of one trip circuit is accomplished by placing that circuit in a half-tripped mode; i.e., a two-out-of-three circuit becomes a one-out-of-two circuit. Testing does not trip the system unless a trip condition exists in another channel.

Reliability and independence is obtained by redundancy within each tripping function. In a two-out-of-three circuit, for example, the three channels are equipped with separate primary sensors. Each channel is continuously fed from its own independent electrical sources. Failure to deenergize a channel when required would be a mode of malfunction that would affect only that channel. The trip signal furnished by the two remaining channels would be unimpaired in this event.

Routing and separation standards applicable to existing cables are those that were invoked at the time of cable installation. For more information, see Section 8.3.1.4.

7.2.1.1.3 Redundancy and Independence

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

Two reactor trip breakers are provided to interrupt power to the control rod drive mechanisms. The breaker main contacts are connected in series with the power supply to the mechanism coils. Opening either breaker interrupts power to the magnetic latch mechanism on each control rod drive, causing them to release the rods to fall by gravity into the core. Each breaker is opened through an undervoltage coil. Each protection channel actuates two separate trip logic trains, one for each reactor trip breaker undervoltage trip coil. The protection system is thus inherently safe in the event of a loss of rod control power.

The coincident trip philosophy is carried out to provide a safe and reliable system since a single failure will not defeat the function of a redundant channel and will also not cause a spurious plant trip. Channel independence is carried throughout the system extending from the sensor to the relay providing the logic. In most cases, the safety and control functions when combined are combined only at the sensor (and power supply). Both functions are fully isolated in the remaining part of the channel, control being derived from the primary safety signal path through an isolation amplifier. As such, a failure in the control circuitry does not affect the safety channels. This approach is used for pressurizer pressure and water level channels, steam-generator water level, T_{AVG} and delta T channels, steam flow, and nuclear power range channels.

The power supplies to the channels are fed from four instrument buses. Two of the buses are supplied by constant voltage transformers and two are supplied by inverters.

Routing and separation standards applicable to existing cables are those that were invoked at the time of cable installation. For more information, see Section 8.3.1.4.

7.2.1.1.4 Effects of Adverse Conditions

CRITERION: The effects of adverse conditions to which redundant channels or protection systems might be exposed in common, either under normal conditions or those

of an accident, shall not result in loss of the protection function or shall be tolerable on some other basis (AIF-GDC 23).

The components of the protection system are qualified such that the mechanical and thermal adverse environment resulting from any emergency situations during which the components are required to function does not prevent accomplishing their safety function.

7.2.1.1.5 Testing While In Operation

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

Each protection channel in service at power is capable of being calibrated and tripped independently by simulated signals for test purposes to verify its operation. This includes checking through to the trip breakers which necessarily involves the trip logic. Thus, the operability of each trip channel can be determined conveniently and without ambiguity.

7.2.1.1.6 Fail Safe Design

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

Each reactor trip channel is designed so that trip occurs when the channel is deenergized; an open circuit or loss of channel power therefore causes the system to go into its trip mode. In a two-out-of-three circuit, the three channels are equipped with separate primary sensors, and each channel is energized from independent electrical buses. Failure to deenergize when required is a mode of malfunction that affects only one channel. The trip signal furnished by the two remaining channels is unimpaired in this event.

Reactor trip is implemented by interrupting power to the magnetic latch mechanisms on each drive, allowing the rod clusters to insert by gravity. The protection system is thus inherently safe in the event of a loss of power.

7.2.1.1.7 Single Failure Criterion

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

Reactor shutdown with rods is completely independent of the normal control functions since the trip breakers completely interrupt the power to the rod mechanisms regardless of existing control signals. Details of the effects of continuous withdrawal of a rod cluster control assembly and of continuous deboration are described in Section 7.7 and Section 9.3.4.

7.2.1.2 Seismic Design

The seismic design for Class 1E electrical equipment was analyzed during the conduct of the Systematic Evaluation Program (SEP) Topic III-6, "Seismic Considerations." This evaluation was based on a zero-period ground acceleration of 0.2g. As described in NUREG/CR-1821, "Seismic Review of the R. E. Ginna Nuclear Power Plant as Part of the SEP," floor response spectra were generated for all Ginna Station structures/levels and the equipment evaluated for potential effects. The review concluded that, for the most part, electrical equipment would withstand seismic forces. Upgrades for certain equipment such as the battery racks, main control board panels, and some equipment anchorages were performed as part of the SEP. (See Section 3.10.)

7.2.1.3 Operating Environment

The protective channels are designed to perform their function when subjected to the most adverse environmental conditions expected when the protective function is required and to prevent loss of function resulting from environmental conditions anticipated during their lifetimes.

Type test data or reasonable engineering extrapolation based on test data are available to verify that Environmentally Qualified equipment, which must operate to provide protective system action, will meet on a continuing basis the functional requirements under the ambient conditions anticipated when the function is required.

The operating environment for equipment within the containment will normally be controlled to 125°F or lower. The Reactor Trip System (RTS) instrumentation within the containment is designed for continuous operation in an environment of 120°F, atmospheric pressure and 50% (nominal) relative humidity, and short transients above 120°F are acceptable. The portions of the Reactor Trip System (RTS) and Engineered Safety Features Actuation System (ESFAS) required to perform safety functions in a harsh postaccident environment are qualified to operate in accordance with the requirements of 10 CFR 50.49, as described in Section 3.11.

Postulated accident conditions at the location of the trip breakers are relatively mild (212°F, 0.25 psig, 100% relative humidity). Trip breakers are environmentally qualified since they perform their function within seconds.

They (Reactor Trip Breakers) are located two floors from the postulated pipe crack and long-term failure could not cause control rod withdrawal from the core.

The environment for the neutron detectors is limited to 150°F with a relative humidity of less than 90%. The detectors are designed for continuous operation in an environment of 180°F, 100% relative humidity, and 100 psig. The 100% humidity value assumes that the detector connections, in the instrument wells, are covered with nuclear grade (Raychem) sleeving.

Protective equipment outside of the containment and inside the control room is designed for continuous operation in an ambient temperature of 75°F and 50% relative humidity. The control room is maintained at the personnel comfort level; however, protective equipment in the control room operates within design tolerance up to a temperature of 104°F.

7.2.2 DESCRIPTION

The Reactor Trip System (RTS) automatically trips the reactor to protect against reactor coolant system damage caused by high system pressure and to protect the reactor core against fuel rod cladding damage caused by a departure from nucleate boiling.

The basic reactor tripping philosophy is to define a region of power and coolant temperature and pressure conditions allowed by the primary trip functions (overpower delta T trip, over-temperature delta T trip, and nuclear overpower trip). The allowable operating region within these trip settings is provided to prevent any combination of power, temperature, and pressure that would result in a departure from nucleate boiling with all reactor coolant pumps in operation.

Additional trip functions such as a high pressurizer pressure trip, low pressurizer pressure trip, high pressurizer water level trip, loss-of-flow trip, steam-generator low-low water level trip, turbine trip, safety injection trip, nuclear source and intermediate range trips, and manual trip are provided to back up the primary trip functions for specific accident conditions and mechanical failures.

The core protective systems in conjunction with inherent plant characteristics are designed to prevent anticipated abnormal conditions from causing fuel damage exceeding limits established in Chapter 4, or primary system damage exceeding effects established in Chapter 5.

Figure 7.2-1 is a block diagram of the Reactor Trip System (RTS).

The curves of Technical Specifications Figure 2.1.1-1 represent the loci of points of thermal power, coolant system pressure, and average temperature for which the minimum departure from nucleate boiling ratio, as defined in the Technical Specifications, is satisfied. The area of safe operation is below these lines.

Adequate margins exist between the worst steady-state operating point (including all temperature, calorimetric, and pressure errors) and required trip points to preclude a spurious plant trip during design transients.

Where operating requirements necessitate automatic or manual bypass of a protective function, the design is such that the bypass is removed automatically whenever permissive conditions are not met. Devices used to achieve automatic removal of the bypass of a protective function are part of the protection system and are designed in accordance with the criteria discussed in Section 7.2.1.

The protection system is so designed that, once initiated, a protective action goes to completion. Return to MODES 1 and 2 requires administrative action by the operator.

Where it is necessary to change to a more restrictive trip setting to provide adequate protection for a particular mode of operation or set of operating conditions, the design provides positive means of ensuring that the more restrictive trip setting is used. The devices used to prevent improper use of less restrictive trip settings are considered a part of the protective system and are designed in accordance with the other provisions of these criteria.

Interlocks and administrative procedures required to limit the consequences of fault conditions other than those specified as limits for the protective function comply with the protection system criteria.

Interlocking functions of the Reactor Trip System (RTS) inhibit manual control rod withdrawal on the occurrence of a specified parameter reaching a value before the value at which reactor trip is initiated.

The power supply for the entire protection system originates from four independent sources, one for each of the four channels. These sources are the 120-V ac instrument power buses of the electrical system.

7.2.2.1 Logic Train

The nuclear and process instrumentation systems send trip signals to the logic trains. There are two complete and independent sets of logic circuits to the Reactor Trip System (RTS) cabinets. Each set constitutes a logic train. When the setpoint values are sensed, a trip signal is sent to the protection cabinets. If a reactor trip is required, the protection cabinets will send a signal to the reactor trip breakers. Tripping of these breakers will remove power from the control rod drive mechanisms allowing the rods to drop into the reactor core. Additionally, the protection cabinets will actuate any required safeguards devices and also provide appropriate permissive signals to the logic trains to allow automatic or manually initiated interlocks and blocks.

The analog channels provide the input portion to the Reactor Trip System (RTS). The typical analog channel consists of a sensor, power supplies, and the process or nuclear instrumentation. The process and nuclear instrumentation contain signal conditioning circuits, controllers, signal comparators, and isolation amplifiers. The remainder of the Reactor Trip System (RTS) is composed of protection cabinets, relay logic cabinets, test panels, trip breakers, undervoltage coils, and shunt trip coils.

Separation of the redundant analog channels originates at the process sensors and continues through the field wiring and containment penetrations to the protection cabinets. Separation of field wiring is achieved by using separate wireways, cable trays, conduit runs, and containment penetrations for each redundant channel. At the protection cabinets, the components of the four channels are located in separate panels. Furthermore, power for each channel is supplied from separate buses.

Routing and separation standards applicable to existing cables are those that were invoked at the time of cable installation. For more information, see Section 8.3.1.4.

7.2.2.1.1 **Sensors**

The sensors measure plant process parameters such as pressure, temperature, levels, power flow, bus voltage, and frequency. They convert the measurement into an electrical signal proportional to that parameter when necessary. Typical sensors are resistance temperature detectors, pressure cells, differential pressure cells, ion chambers, and undervoltage and underfrequency devices.

7.2.2.1.2 Process and Nuclear Instrumentation

The process instrumentation receives the process signal from the detector and processes the received signal in one or more ways. These ways may include amplification, integration, differentiation, summation, exponential, square root, or lead-lag type functions. After processing, the signal is used for indication, control, and protection of the reactor. Control and indication circuits are electrically isolated from the process instrument output via an isolation amplifier, while the protection circuit connects directly to the output. This electrical isolation prevents feedback effects from grounds, opens, or shorts in the control circuitry from affecting the protection circuitry, thereby maintaining the reliability of the Reactor Trip System (RTS).

A bypass test panel is installed in the rear of each of the four NIS cabinets. Each Power Range bistable that produces a reactor trip, permissive, or rod stop signal has a bypass toggle switch and indicator on the panel. When a bistable is bypassed, the bypass test panel provides a 120 VAC signal to the reactor trip system and then disconnects the bistable output as a make-before-break system. The bypass test panel uses the same instrument bus AC power as the existing rack instrumentation. When a bypass test panel is energized via a keylock enable switch placed in the "bypass" position, the panel will provide a main control board "channel in test" alarm. The alarm will clear when the bypass panel is de-energized via the keylock enable switch placed in the "normal" position. Channel bypass status is also indicated locally with bypass lamps on the bypass test panels. Administrative controls are used to ensure that only one Reactor Protection Channel is placed in bypass at a time. Use of the bypass panel is procedurally controlled.

7.2.2.1.3 Protection Cabinets

Located at the south wall of the control room, there are four protection cabinets, one for each input from the respective instrumentation channel. They contain the protection bistables for both the reactor trip and safeguards actuation functions as well as the bistables for the permissive functions.

A bypass connection test panel is located in the rear bottom of each reactor protection cabinet in the Main Control Room. Each reactor protection channel consists of two cabinets. There is one bypass connection test panel in each cabinet, except for channel IV, cabinet Y2, which has two connection panels for the two separate power sources within that cabinet. The connection panels allow for a test box to be connected to bypass those reactor protection and ESFAS functions that could result in a reactor trip if a redundant instrument channel is placed in trip or fails in the trip state. The test box has individual switches for designated instrument functions to be bypassed. The test box uses the same instrument bus or inverter AC power as the existing rack instrumentation. When connected and powered up, the test box will provide a main control board "channel in test" alarm for the affected reactor protection channel. The alarm will clear when the test box power is secured. Administrative controls are used to ensure that only one Reactor Protection channel is placed in bypass at a time. An instrument channel cannot inadvertently be left in the bypass condition once the test box is disconnected. Connection and disconnection of the test box is procedurally controlled.

7.2.2.1.4 Logic Relay Cabinets

The logic relay cabinets are divided into two groups of cabinets, the reactor trip logic cabinets

and the safeguards actuation logic cabinets. The reactor trip logic cabinets consist of four separate cabinets for each train of protection with inputs from each of the four protection cabinets. Each protection cabinet sends its signal to two trip logic cabinets, one cabinet in each protection train. The front section of the reactor trip logic cabinet contains the logic, trip, and permissive relays. The rear section contains test relays that are used only during testing (see Section 7.2.4). The incoming protection signal to the logic cabinet passes through a set of test relay contacts. These contacts are shut during normal at power operation. A test relay actuates these contacts in the respective logic cabinet and is controlled from the logic test panels.

The protection signal supplies power directly to a logic relay, maintaining it energized during MODES 1 and 2. Should the specified setpoint value be detected by a channel, the protection signal would deenergize the logic relay. The logic relay contacts are wired in the proper logic matrix. This logic matrix contains the logic relay contacts from each channel's respective logic cabinet. Each logic matrix represents a specific trip function and two or more are normally wired in series. The logic matrices are also in series with one of eight trip relays and their power supplies. The trip relays are divided equally among the four cabinets in one train. When a reactor trip is needed, the logic relays deenergize, opening their contacts, which in turn deenergize the trip relays.

The permissive logic relays are arranged in the same fashion as the reactor trip logic relays. They are also controlled by bistables in the protection cabinets. When the permissive logic relays energize, their contacts shut. This allows a given permissive function to occur automatically or by manual operator action.

7.2.2.1.5 Trip Breakers

The reactor trip breakers are designed to quickly interrupt power supplied from the rod control motor-generator sets to the control rod drive mechanisms. Each breaker has the capability to insert a bypass breaker that allows for the testing of each main trip breaker. Each reactor trip breaker and bypass breaker has an undervoltage trip coil and shunt trip coil that trip the breaker through a mechanical linkage. Test switches can be used to independently verify the operation of both the undervoltage trip assembly and the shunt trip assembly.

Undervoltage coils deenergize to trip the breaker, while shunt trip coils energize to cause a breaker trip. Undervoltage and shunt trip coils in each train are powered from the Class 1E, 125-V-dc battery system associated with that train.

Each undervoltage coil is connected to its 125-V-dc power supply in series with all the trip relay contacts in the reactor trip logic cabinets and the manual trip switches on the main control board. As long as a complete electrical flow path is present, the undervoltage coils remain energized holding the trip breakers shut. Once a trip condition is detected, the respective trip relay will deenergize, thus opening its contacts and causing the 125-V-dc power to be interrupted to the undervoltage coils.

In order to minimize the likelihood of a failure of a breaker to trip, the two reactor trip breakers use a reverse tripping logic to automatically activate the existing trip coil concurrent with the deenergization of the undervoltage coil. This results in two simultaneous mechanical forces acting on the tripper bar instead of one.

Each reactor trip breaker (but not the bypass breaker) uses a reverse tripping logic to automatically energize the shunt trip coil concurrent with deenergization of the undervoltage coil.

Trip relays, which form the logic for the undervoltage coils, have both "a" and "b" type contacts. The "b" contacts close when the trip relays deenergize while the "a" contacts open. The "b" contacts are used to form the reverse logic that energizes the shunt trip coils. The reactor trip breaker shunt trip coil is energized by the same Reactor Trip System (RTS) signals that cause the undervoltage trip coil to deenergize. The RTS has a pushbutton testing feature in the now-defeated (jumpered) zirconium guide tube trip. The pushbutton temporarily reinstates the circuitry associated with the zirconium guide tube logic which can be used to directly trip the shunt trip attachment independent of the undervoltage trip attachment.

In addition to the automatic control of the shunt trip coil on the reactor trip breaker, the shunt trip coils on the reactor trip breakers and the bypass breaker are controlled by the manual reactor trip switches.

A simplified electrical diagram of the undervoltage trip coil and shunt trip assembly is shown in Figure 7.2-20.

7.2.2.2 Reactor Trips

7.2.2.2.1 General

Rapid reactivity shutdown is provided by the insertion of control rod assemblies by gravity fall to compensate for fast reactivity effects, e.g., doppler and moderator temperature effects. Duplicate series-connected circuit breakers supply all power to the control rod drive mechanisms. The control rod drive mechanisms must be energized to remain withdrawn from the core. Automatic reactor trip occurs upon the loss of power to the control rod drives. The trip breakers are opened by any of several trip signals.

Certain reactor trip channels are automatically bypassed at low power where they are not required for safety and to enable convenient operation for conditions such as startup and shutdown. Nuclear source range and intermediate range trips, which are specifically provided for protection at low power or subcritical operation, are bypassed at power operation to prevent spurious reactor trip signals and to prevent the degradation of the detectors at power levels above 8%.

During power operation, a sufficiently rapid shutdown capability in the form of control rods is administratively maintained through the control rod insertion limit monitors (see Section 7.7). Administrative control requires that all shutdown rods be in the fully withdrawn position during power operation.

[Historical] During MODE 6 (Refueling) in 1981, zirconium guide tubes were installed in the fuel assemblies. The different thermal expansion rates of zirconium versus stainless steel raised a potential problem of interference which could lead to damage of the rod drive mechanisms if a cooldown were to occur with the control rod drives latched. The automatic interlock installed for commercial reasons to ensure that the reactor trip breakers were open prior to cooling down was removed in 2020.

Technical Specification Table 3.3.1-1 lists the requirements necessary to preserve the effectiveness of the reactor control and protection system.

The logic diagram for the reactor trip signals is shown in Drawings 33013-1353, Sheet 1 and 33013-1353, Sheet 2. Drawing 33013-1353, Sheet 1 provides the index of the symbols used in all the logic diagrams.

7.2.2.2.2 Manual Trip

A manual reactor trip is provided to permit the operators to trip the reactor. The manual actuating devices are independent of the automatic reactor trip circuitry and are not subject to failures that could make the automatic circuitry inoperable. The manual trip logic is shown in Drawing 33013-1353, Sheet 14.

7.2.2.2.3 High-Nuclear-Flux (Power Range) Trip

This circuit trips the reactor when two out of the four power range channels read above the trip setpoint. The low setting can be manually bypassed (permissive P-10) when two out of the four power range channels read above approximately 8% power. Three out of the four channels below 8% automatically reinstate the trip. The high setting is always active. The high-nuclear-flux (power range) trip logic is shown in Drawing 33013-1353, Sheet 10.

7.2.2.2.4 High-Nuclear-Flux (Intermediate Range) Trip

This circuit trips the reactor when one out of the two intermediate range channels reads above the trip setpoint. This trip can be manually bypassed if two-out-of-four power range channels are above approximately 8%. Three-out-of-four channels below this value automatically reinstate the trip. The intermediate channels (including detectors) are separate from the power range channels in this plant design. The high-nuclear-flux (intermediate range) trip logic is shown in Drawing 33013-1353, Sheet 10.

7.2.2.2.5 High-Nuclear-Flux (Source Range) Trip

This circuit trips the reactor when one out of the two source range channels reads above the trip setpoint. It can be manually bypassed when one-out-of-two intermediate range channels reads above the source range cutoff value and is automatically reinstated when both intermediate range channels decrease below this value. This trip is also bypassed by two-out-of-four high power range signals.

The trip point is set between the source range cutoff power level and the maximum source range power level.

The high-nuclear-flux (source range) trip logic is shown in Drawing 33013-1353, Sheet 10.

7.2.2.2.6 Overtemperature Delta T Trip

The purpose of this trip is to protect the core against departure from nucleate boiling. In the protection system, the indicated loop delta T is used as a measure of reactor power and is compared with a setpoint that is automatically varied, depending on T_{AVG}, pressurizer pressure, and axial flux difference. The circuit trips the reactor on coincidence of two out of the four signals, with two channels per loop.

The overtemperature delta T trip logic is shown in Drawing 33013-1353, Sheet 14.

7.2.2.2.7 Overpower Delta T Trip

The purpose of this trip is to protect against excessive power (fuel rod rating protection) and subsequent fuel rod failure. The indicated delta T is used as a measure of reactor power and is compared with a setpoint that is automatically varied depending on T_{AVG} This circuit trips the reactor on coincidence of two out of the four signals, with two channels per loop.

The overpower delta T trip logic is shown in Drawing 33013-1353, Sheet 14.

7.2.2.2.8 Low Pressurizer Pressure Trip

The low pressurizer pressure trip is designed to protect against departure from nucleate boiling, and also serves to limit the range of the overtemperature delta T trip by establishing a lower limit on reactor coolant pressure. Four pressurizer pressure channels are used in a two-out-of-four logic. The low pressurizer pressure trip is automatically bypassed below 8% power since the protection afforded by the trip is not essential at this low power level due to the lower reactor coolant system temperature. The low pressurizer pressure trip logic is shown in Drawing 33013-1353, Sheet 12.

7.2.2.2.9 High Pressurizer Pressure Trip

The high pressurizer pressure trip is designed to protect the reactor coolant system from an overpressure condition. There are three pressure channels sensing pressure in the pressurizer and arranged in a two-out-of-three logic. The trip setting is above the Pressurizer Power Operated Relief Valves (PORV) setting to prevent an unnecessary reactor trip for those pressure increases that can be controlled by the valves. The trip, along with the Pressurizer Power Operated Relief Valves (PORV) and Main Steam Safety Valves (MSSV), prevents overpressurization. The high pressurizer pressure trip logic is shown in Drawing 33013-1353, Sheet 12.

7.2.2.2.10 High Pressurizer Water Level Trip

The high pressurizer level trip is provided as a backup to the high pressure trip. It is also used to prevent potential damage to the pressurizer safety valves and discharge piping which could be caused by water hammer if these valves lift to pass water instead of steam. Three high level channels are arranged in a two-out-of-three logic. The high pressurizer water level trip logic is shown in Drawing 33013-1353, Sheet 12.

7.2.2.2.11 Low Reactor Coolant Flow Trip

The low flow trips are provided to protect the core from departure from nucleate boiling following a loss-of-flow accident. The means of sensing a low flow condition are as follows:

1. Measured low flow in the reactor coolant piping.
2. Sensing an undervoltage condition on the reactor coolant pump buses.
3. Sensing an underfrequency condition on the reactor coolant pump buses.
4. Sensing reactor coolant pump circuit breakers open.

The low flow trip signal is actuated by the coincidence of two-out-of-three signals for each reactor coolant loop. The loss of flow in either loop causes a reactor trip.

Below the permissive power setpoint P-8, loss of flow in both loops would cause a reactor trip. This permits an orderly plant shutdown under administrative control following a single loop loss of flow during low power operation. Since the plant will not be maintained in operation above permissive power setting P-7 without both loops in service, independent accidents simultaneous with a single loop loss of flow at low power are not considered in the protection system design. The loss of reactor coolant flow trip logic is shown in Drawing 33013-1353, Sheet 14.

The undervoltage on the reactor coolant pump buses trip is provided for protection following a complete loss of power to the reactor coolant pumps. A voltage condition below 3150 volts, as sensed by undervoltage relays (one-out-of-two logic) on both reactor coolant pump buses, will directly trip the reactor to prevent departure from nucleate boiling. This trip is bypassed below 8% power by permissive P-7.

The underfrequency on the pump power supply trip provides reactor protection following a major grid frequency disturbance. If an underfrequency condition below 57.7 Hz (one-out-of-two logic) exists on both reactor coolant pump buses, all reactor coolant pump breakers and the reactor are tripped. This is done because an underfrequency condition will slow down the pumps thereby reducing their coastdown time following a pump trip.

The undervoltage and underfrequency trip logic is shown in Drawing 33013-1353, Sheet 4.

7.2.2.2.12 Safety Injection System Actuation Trip

A reactor trip occurs on the actuation of the safety injection system. The means of actuating the safety injection system trips are described in Section 7.3.2.

7.2.2.2.13 Turbine Trip/Reactor Trip

Turbine trip causing a reactor trip is provided to anticipate probable plant transients and to avoid the resulting thermal transients. If the reactor were not tripped by the turbine trip, the overtemperature delta T or high pressure trip would prevent reactor safety limits from being exceeded. By utilizing this trip, undesirable excursions are prevented rather than terminated.

The trip is sensed by a decrease in emergency trip system oil pressure or all stop valves shut. Three switches are mounted on the emergency trip oil header and their outputs are tied together in a two-out-of-three logic. This logic will initiate a reactor trip (auto-stop oil pressure less than 45 psig) provided the reactor is operating above 50% power as sensed by permissive P-9. It is not necessary to trip the reactor if it is operating below 50% power since rod control in conjunction with steam dump can accommodate a 50% load rejection without a reactor trip (Section 10.7.1). Turbine trip leading to reactor trip logic is shown in Drawing 33013-1353, Sheet 3.

7.2.2.2.14 Low-Low Steam-Generator Water Level Trip

The purpose of this trip is to protect the steam generators for the case of a sustained steam/ feedwater flow mismatch. The trip is actuated on two-out-of-three low-low water level signals in either steam generator. The trip logic is shown in Drawing 33013-1353, Sheet 13.

7.2.2.3 Interlocks

A number of reactor trips applicable to power range operation are automatically bypassed to permit reactor startup and low power operation. The following trip functions are blocked by a coincidence of three-out-of-four power range nuclear flux channels reading less than 8% power and one-out-of-two low turbine load (turbine impulse chamber pressure) signals:

A. Low reactor coolant flow (both loops).

B. Reactor coolant pump breaker trip (both loops).

C. Turbine trip with P-9 permissive present.

D. Undervoltage.

E. Underfrequency.

F. Low pressurizer pressure.

Similarly, the high-nuclear-flux source range and high-nuclear-flux intermediate range trips applicable to startup and low power operation are bypassed during power operation.

7.2.2.4 Permissive Circuits

Various permissive signals are generated throughout the plant for the purpose of providing both automatically and manually initiated interlocks and bypass circuits. Actuation of the permissives is indicated on the permissive status panel. The permissives associated with the Reactor Trip System (RTS) are listed in Table 7.2-2 and are described below. The logic diagram is shown in Drawing 33013-1353, Sheet 11.

7.2.2.4.1 P-1 Permissive

The P-1 permissive, rod stop on overpower, blocks automatic and manual rod withdrawal. The overpower rod stops are initiated by one-out-of-four high nuclear flux of 103%; one-out-of-two high flux at 20% current equivalent power; two-out-of-four high overtemperature delta T at 3% of rated loop ΔT below trip setpoints; and high overpower delta T at 3% of rated loop ΔT below the trip setpoint with two-out-of-four logic. High overpower delta T and overtemperature delta T will also initiate a turbine runback at 200%/min for 1.5 sec every 30 sec. With automatic rod withdrawal disabled, the P-1 permissive block on automatic rod withdrawal is no longer applicable.

7.2.2.4.2 P-2 Permissive

The P-2 permissive blocks automatic rod withdrawal at low power. It is initiated by one-out-of-one first stage turbine pressure less than 12.8% turbine power. Automatic rod withdrawal has been disabled. The P-2 permissive is not used.

7.2.2.4.3 P-3 Permissive

The P-3 permissive blocks automatic rod withdrawal on a rod drop signal. A rod drop signal is initiated by a rapid decrease of nuclear flux of 5%. Logic of one-out-of-four power-range detectors will satisfy this permissive. Additionally a rod drop signal is initiated if a rod is indicating 0 steps when any rod in its bank or any subsequent programmed bank indicates 24 steps or greater. Automatic rod withdrawal has been disabled. The P-3 permissive is not used.

7.2.2.4.4 P-4 Permissive

The P-4 permissive arms the steam dump system for operation upon sudden decrease in turbine load actuated on one-out-of-one first stage turbine pressure decrease equivalent to a 10% full power decrease.

7.2.2.4.5 P-6 Permissive

The P-6 permissive permits bypassing the source range channel high flux trip during an approach to power. It is derived from a bistable circuit of the intermediate range channels.

The bistable circuit will initiate the permissive if either intermediate range channel is above a power level of 1×10^{-10} amp and illuminates the "Power Above P-6" light. In order to block the source range high flux trip, however, two buttons must be depressed after the permissive is effective. One is supplied for each logic train. After both buttons are depressed, the "Source Range Trip Blocked" light will be illuminated. If both intermediate range channels drop below 5×10^{-11} amp, the permissive will automatically be defeated. The permissive may be manually defeated if power is below P-10 by simultaneously depressing both defeat pushbuttons. Either method will reinstate the trip capability.

7.2.2.4.6 P-7 Permissive

The P-7 permissive is used to bypass the low pressurizer pressure reactor trips during low power or startup operation. It is also used to bypass reactor coolant low flow trips. It is derived from a bistable circuit indicating less than 8.5% power as measured by both first stage turbine pressure (two-out-of-two) and power range (two-out-of-four). The power range input is supplied by the P-10 permissive.

7.2.2.4.7 P-8 Permissive

The P-8 permissive allows the loss of flow trip logic to change so that a loss of a single loop below P-8 setpoint will not cause a reactor trip. P-8 is set at 25% reactor power as sensed by two-out-of-four power range instruments of the nuclear instrumentation system.

7.2.2.4.8 P-9 Permissive

The P-9 permissive prevents a reactor trip when the turbine trips if nuclear power is below 50%. The permissive has two-out-of-four logics and it also allows for the unnecessary reactor trip when the steam dump is available.

7.2.2.4.9 P-10 Permissive

The P-10 permissive is used to bypass the intermediate range channel and low-level power range channel trips during an approach to power. It is also used as a backup to P-6, to block out the source range instrumentation, and in the development of P-7. It is derived from a bistable circuit indicating greater than 8% power as measured by the power range channels (two-out-of-four). In order to block the intermediate range high flux and low power high flux trips, two buttons for each trip must be depressed on the control panel. If power falls below 6% on three or four channels, the nuclear instrument trips will be automatically unblocked.

7.2.2.5 Alarms

Alarms will also be used to alert the operator to deviation from normal operating conditions so that, where possible, the operator may take corrective action to avoid a reactor trip. Further, actuation of any rod stop or trip of any reactor trip channel will actuate an alarm.

Any of the following conditions actuates an alarm:

A. Reactor trip (first-out annunciator).
B. Trip of any reactor trip channel.
C. Actuation of any permissive circuit (get a light) or override.
D. Significant deviation of any major control variable (pressure, T_{AVG}, pressurizer water level, and steam-generator water level).
E. Incompleted administrative test procedures in any reactor trip channel (and control channel, where feasible).

7.2.2.6 Design Features

7.2.2.6.1 Isolation of Redundant Protection Channels

7.2.2.6.1.1 Channelized Design

The Reactor Trip System (RTS) is designed on a channelized basis to achieve isolation between redundant protection channels. The channelized design, as applied to the analog as well as the logic portions of the protection system, is illustrated by Figure 7.2-12 and is discussed below. Although shown for four-channel redundancy, the design is applicable to two-and-three-channel redundancy. Figure 7.2-12 shows only the undervoltage coil associated with each trip breaker; a similar circuit for each breaker, consisting of a dc power feed, relay contacts, and a shunt trip coil is omitted for clarity.

Isolation of redundant analog channels originates at the process sensors and continues back through the field wiring and containment penetrations to the analog protection racks. Physical separation in cable trays, conduit, and containment penetrations is used to the maximum practical extent to achieve isolation. Analog equipment is isolated by locating redundant components in different protection racks.

Routing and separation standards applicable to existing cables are those that were invoked at the time of cable installation. For more information, see Section 8.3.1.4.

The power supplies to the channels are fed from four instrument buses. Two of the buses are supplied by constant voltage transformers, and two are supplied by inverters. Each channel is energized from a separate ac power feed. Each reactor trip circuit is designed so that a trip occurs when the circuit is deenergized. An open circuit or the loss of channel power, therefore, causes the system to go into its trip mode. Reliability and independence are obtained by redundancy within each tripping function. In a two-out-of-three circuit, the three channels are equipped with separate primary sensors and each channel is energized from an independent electrical bus. A single failure may be applied in which a channel fails to deenergize when required; however, such a malfunction can affect only one channel. The trip signal furnished by the two remaining channels is unimpaired in this event.

All reactor protection channels are supplied with sufficient redundancy to provide the capability for channel calibration and testing at power. Bypass removal of one trip circuit is accomplished by placing that circuit in a half-tripped mode; that is, a two-out-of-three circuit becomes a one-out-of-two circuit. Testing does not trip the system unless a trip condition concurrently exists in a redundant channel.

Certain reactor trip channels are automatically bypassed at low power, to allow for such conditions as startup and shutdown, and where they are not required for safety. Nuclear source range and intermediate range trips, which specifically provide protection at low power or sub-critical operation, are bypassed at power operation to prevent spurious reactor trip signals and to improve reliability.

7.2.2.6.1.2 Separation

The reactor trip bistables are mounted in the protection racks and are the final operational component in an analog protection channel. Each bistable drives two logic relays (C and D). The contacts from the C relays are interconnected to form the required actuation logic for trip breaker No. 1 through dc power feed No. 1. The transition from channel identity to logic identity is made at the logic relay coil/relay contact interface. As such, there is both electrical and physical separation between the analog and the logic portions of the protection system. The above logic network is duplicated for trip breaker No. 2 using dc power feed No. 2 and the contacts from the D relays. Therefore, the two redundant reactor trip logic channels are physically separated and electrically isolated from one another. Overall, the protection system is comprised of identifiable channels that are physically, electrically, and functionally separated and isolated from one another to the extent practical.

Components, cabling, and panel wiring for reactor trip breaker undervoltage and shunt trip circuitry are grouped into two redundant trains and physically separated. Each of the two manual reactor trip switches activates undervoltage and shunt trips for both trains. Wiring to these switches is separated to the maximum extent possible in the main control board. Channel separation is maintained between the control wiring for the undervoltage trip coils and the shunt trip coils. A fault on any one control circuit will not degrade both redundant trains.

7.2.2.6.2 **Channel Bypass or Removal from Operation**

The system is designed to permit any one channel to be maintained, and when required, tested or calibrated during power operation without system trip. During such operation, the active parts of the system continue to meet the single-failure criterion.

Exception: "One-out-of-two" systems are permitted to violate the single-failure criterion

during channel bypass provided that acceptable reliability of operation can be otherwise demonstrated.

A. Cross-checking between identical channels or between channels which bear a known relationship to each other and which have readouts available.

The design permits the administrative control of the means for manually bypassing channels or protective functions.

The design permits the administrative control of access to all trip settings, module calibration adjustments, test points, and signal injection points.

7.2.2.6.3 Information Readout and Indication of Bypass

The protective systems are designed to provide the operator with accurate, complete, and timely information pertinent to their own status and to plant safety. Indication is provided in the control room if the trip function of some part of the system has been administratively bypassed or taken out of service.

Trips are indicated and identified down to the channel level.

7.2.2.6.4 Physical Isolation

The physical arrangement of all elements associated with the protection system reduces the probability of a single physical event impairing the vital functions of the system.

System equipment is separated between instrument cabinets so as to reduce the probability of damage to the total system by some single event.

Wiring between vital elements of the system outside of equipment housing is routed and protected so as to maintain the true redundancy of the systems with respect to physical hazards.

The RG&E wire and cable routing for safety channels has been separated in general by the following means:

A. Redundant circuits run in separate conduits.

B. Redundant circuits run in separate cable trays.

C. Redundant circuits run in opposite sides of cable trays that have been partitioned with a metal barrier plate.

Routing and separation standards applicable to existing cables are those that were invoked at the time of cable installation. For more information, see Section 8.3.1.4.

7.2.2.6.5 Sensor Line Separation

Physical separation between redundant protection instrument sensing lines is generally achieved by providing 4 ft of separation for vertical runs and 18 in. for horizontal runs. Where physical separation could not be obtained due to space limitations or obstructions, protection has been achieved by barriers and/or enclosed sectional raceways. The barriers and/or raceways are made of heavy gauge metal.

7.2.2.6.6 Instrument Line Identification

The identification of electrical circuits, cables, conduits, and cable trays is generally accomplished as shown in the following list:

A. Individual wires are tagged with an oblong fiber tag at each wire end. This tag carries the wire number as listed in the wiring schedule sheets.

B. Individual cables are tagged with a round fiber tag attached to the cable close to the end of the cable outer sheath where it has been stripped back to expose the individual wires. This tag carries the cable number corresponding to the cable schedule sheet number.

C. Each conduit is tagged with a brass numbering check attached at each end of the conduit and at intermediate points in the run as specified in the conduit layout drawings.

D. Each cable tray is stenciled with a tag number at each end with the identifying number shown on the cable tray layout drawings.

E. Sensors in the protection channels are identified by tag numbers at the sensor location.

7.2.3 ANALYSIS

7.2.3.1 Reactor Trip System (RTS) and Departure From Nucleate Boiling

The following is a description of how the Reactor Trip System (RTS) prevents departure from nucleate boiling (DNB).

The plant variables affecting the DNB ratio (DNBR) are

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

7.2.2.6.7 Capability for Test and Calibration

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

The analog portion of a protective channel (e.g., sensors and amplifiers) provides analog signals of reactor or plant parameters. The following means are provided to permit checking the analog portion of a protective channel during reactor operation:

A. Varying the monitored variable.

B. Introducing and varying a substitute transmitter signal.

7.2.3.2 Core Protection System

The basic overpower-overtemperature protection mentioned in conjunction with the power capability discussion consists of the delta T trip functions based on the differences between measurements of the hot-leg and cold-leg temperatures, which are proportional to core power.

The delta T trip functions are provided with a nuclear flux feedback to reflect a measure of power distribution. This will assist in preventing an adverse distribution which could lead to exceeding allowable core conditions. The overpower-overtemperature protection and the power distribution feedback are described below. (See Figures 7.2-14 and 7.2-15.)

7.2.3.2.1 Overpower Protection

In addition to the nuclear power range trips, a delta T trip is provided (two-out-of-four logic) to limit the maximum overpower. This trip is modified as described in Section 7.2.2.2.7.

In addition, a rod stop function and turbine runback function is provided in the form:

$\Delta T_{(rod\ stop)} = \Delta T_{(trip)}$ - constant

with a programmed turbine runback until $\Delta T < \Delta T_{(rod\ stop)}$

This function serves to maintain essentially a constant margin to trip and gives the operator the opportunity to make appropriate adjustments before a reactor trip occurs.

7.2.3.2.2 Overtemperature Protection

A second delta T trip (two-out-of-four logic) provides a trip which protects against departure from nucleate boiling. This trip is modified as described in Section 7.2.2.2.6.

Four long ion chamber pairs are provided and each one independently feeds a separate delta T trip channel. Thus, a single failure neither defeats the function nor causes a spurious trip.
The axial flux difference penalty function is only in the direction of decreasing the trip setpoint; it cannot increase the setpoint.

If the difference between the top and bottom detectors exceeds a preset limit indicative of excess power generation in the upper or lower half of the core, a proportional signal is transmitted to the delta T trip to reduce its setpoint.

A similar rod stop and turbine runback function is provided as discussed in Section 7.2.3.2.1.

7.2.4 REACTOR TRIP SIGNAL TESTING

Provisions are made to manually place the output of the bistable in a tripped condition for "at power" testing of all portions of each trip circuit including the reactor trip breakers. Administrative procedure requires that the final element in selected trip channels (required during power operation) is placed in the trip mode before that channel is taken out of service for repair or testing so that the single-failure criterion is met by the remaining channels. This provision applies to bistable functions that do not result in a reactor trip or ESFAS actuation if a redundant channel is placed in a trip condition intentionally or due to a failure.

Administrative procedures will allow selected Reactor Trip System (RTS) and Engineered Safety Features Actuation System (ESFAS) bistables to be bypassed during surveillance

testing (Channel Operational Test and Channel Calibration). The bypass circuitry applies to bistable functions that do result in a reactor trip or ESFAS actuation if a redundant channel is placed in a trip condition intentionally or due to a failure. Bypass circuitry allows a channel to be tested without tripping the channel by imposing a 120 VAC power signal in parallel, thus maintaining the Relay Protection System in an untripped condition. Nuclear Instrumentation System power range functions may be bypassed with permanently-installed bypass test panels located within the rear of the NIS Cabinets. Other RTS and ESFAS system functions will be capable of being bypassed utilizing a portable test box that connects to permanent connectors in the Reactor Protection cabinets.

Provision is made for the insertion of test signals in each analog loop. Verification of the test signal is made by station instruments at test points specifically provided for this purpose.
This enables testing and calibration of meters and bistables. Transmitters and sensors are checked against each other and against precision readout equipment during normal power operation.

7.2.4.1 Analog Channel Testing

The basic elements comprising an analog protection channel are shown in Figure 7.2-16 and consist of a transmitter, power supply, bistable, bistable trip switch and proving lamp, test signal injection switch, test signal injection jack, and test point.

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

Administrative procedures require that selected bistables in the channel under test be placed in the tripped mode prior to test. This provision applies to bistable functions that do not result in a reactor trip or ESFAS actuation if a redundant channel is placed in a trip condition intentionally or due to a failure. This places a proving lamp across the bistable output so that the bistable trip point can be checked during channel calibration. The bistable trip switches must be manually reset after completion of a test. Closing the test panel cover will not restore these switches to the untripped mode.

Administrative procedures will allow selected Reactor Trip System (RTS) and Engineered Safety Features Actuation System (ESFAS) bistables to be bypassed during surveillance testing (Channel Operational Test and Channel Calibration). The bypass circuitry applies to bistable functions that do result in a reactor trip or ESFAS actuation if a redundant channel is placed in a trip condition intentionally or due to a failure. Bypass circuitry allows a channel to be tested without tripping the channel by imposing a 120 VAC power signal in parallel, thus maintaining the Relay Protection System in an untripped condition. Nuclear Instrumentation System power range functions may be bypassed with permanently-installed bypass test panels located within the rear of the NIS Cabinets. Other RTS and ESFAS system functions will be capable of being bypassed utilizing a portable test box that connects to permanent connectors in the Reactor Protection cabinets.

Administrative controls prevent the nuclear instrumentation source range and intermediate range protection channels from being disabled during periodic testing. Power range over-power protection cannot be disabled since this function is not affected by the testing of circuits. Administrative controls also prevent the power range dropped rod protection from being disabled by testing. In addition, the rod position system would provide indication and associated corrective actions for a dropped rod condition.

Actual channel calibration will consist of injecting a test signal from an external calibration signal source into the signal injection jack. Where applicable, the channel power supply will serve as a power source for the calibration source and permit verifying the output load capacity of the power supply. Test points are located in the analog channel and provide an independent means of measuring the calibration signal level.

7.2.4.2 Logic Channel Testing

7.2.4.2.1 **Planned Tests**

The trip logic channels for a typical two-out-of-three and two-out-of-four trip function are shown in Figure 7.2-17. The analog portions of these channels are shown in Figure 7.2-18. Each bistable drives two relays (A and B for level and C and D for pressure). Contacts from the A and C relays are arranged in a two-out-of-three and two-out-of-four trip matrix for trip breaker No. 1. The above configuration is duplicated for trip breaker No. 2 using contacts from the B and D relays. Figure 7.2-17 shows only the circuits associated with the undervoltage trip coils; the energize-to-trip shunt trip coils and associated relay contacts are omitted for clarity, however the configuration is the same.

The planned logic system testing includes exercising the individual reactor trip breakers at least once to demonstrate system integrity. Subsequent logic tests will use installed indicating lights to verify proper logic functions. A bypass breaker is installed at both cells to allow opening the normal trip breaker. During MODES 1 and 2, the bypass breakers are maintained racked-out in their respective cells for reactor trip breakers A and B. Only one bypass breaker will be racked-in at any time in conjunction with testing of the reactor trip breakers. One annunciator window on the main control board will indicate that the bypass breaker is closed in either cell. Direct red and green light indication on the main control board shows the bypass breaker position. Interlocks are provided to prevent bypass breakers from being used simultaneously in the cell for reactor trip breaker A and the cell for reactor trip breaker B.

As shown in Figure 7.2-17, the trip signal from the logic network is simultaneously applied to the main trip breaker associated with the specific logic chain as well as the bypass breaker associated with the alternate trip breaker. Should a valid trip signal occur while AB-1 is bypassing TB-1, TB-2 will be opened through its associated logic train. The trip signal applied to TB-2 is simultaneously applied to AB-1, thereby opening the bypass around TB-1. TB-1 would either have been opened manually as part of the test or would be opened through its associated logic train which would be operational or tripped during a test.

An auxiliary relay is located in parallel with the undervoltage coils of the trip breakers. This relay is tied to an event recorder which is used to indicate transmission of a trip signal through the logic network during testing. Lights are also provided to indicate the status of the individual logic relays.

7.2.4.2.2 Test Procedure

The following procedure illustrates the method used for testing trip breaker No. 1 and its associated logic network.

1. With the bypass breaker being tested (AB-1) racked-in, manually close and trip bypass breaker AB-1 to verify operation.
2. Manually re-close bypass breaker AB-1. Trip the associated reactor trip breaker (TB-1) using a selected logic combination.
3. Sequentially deenergize the trip relays (A1, A2, and A3) for each logic combination (1-2, 1-3, and 2-3). Verify that the logic network deenergizes the undervoltage coil on the reactor trip breaker TB-1 for each logic combination. Temporarily installed indicator lamps monitor the signal applied to the undervoltage coil, operation of the undervoltage coil can be determined from the indicator.
4. Repeat step (3) for every logic combination in each matrix, except Source Range Trip when at power.
5. Close the associated reactor trip breaker (TB-1). Then open and rack-out the bypass breaker (AB-1).

7.2.4.2.3 Logic Channel Test Panels

In order to minimize the possibility of operational errors from either the standpoint of tripping the reactor inadvertently or only partially checking all logic combinations, each logic network includes a logic channel test panel. This panel includes those switches, indicators, and recorders needed to perform the logic system test. The arrangement is shown in Figure 7.2-19. The test switches used to deenergize the trip bistable relays operate through inter-posing relays as shown in Figure 7.2-16 and Figure 7.2-18. This approach avoids violating the separation philosophy used in the analog channel design. Thus, although test switches for redundant channels are conveniently grouped on a single panel to facilitate testing, physical and electrical isolation of redundant protection channels are maintained by the inclusion of the interposing relay, which is actuated by the logic test switches. Identification of instrumentation protection systems is made by colored name plates on the cabinets.

7.2.4.3 Trip Breaker Testing and Preventive Maintenance

Preventive maintenance is performed on the reactor trip breakers each refueling outage. Preventive maintenance procedures conform to the intent of the guidance developed by the Westinghouse Owner's Group.

Response time testing of each reactor trip breaker is performed at each refueling outage in an off-line condition. Breaker response time is determined by deenergizing the undervoltage coil with the shunt trip coil blocked and then by energizing the shunt trip coil with the undervoltage coil blocked. Breaker clearing times are recorded and trended for signs of degradation. The measured response times are less than the 10 cycles assumed for accident analysis. Breaker response time averages about 6 cycles for the undervoltage trip attachment and about 3.5 cycles for the shunt trip attachment. Should the as-found response times show an upward trend and reach 8 cycles, the breaker components or the breaker itself will be replaced or repaired to maintain acceptable performance.

In addition to response time, the parameters of undervoltage trip attachment dropout

voltage, trip force, and breaker insulation resistance are trended in order to detect degradation.

Functional testing of the reactor trip breakers is performed periodically per the Surveillance Frequency Control Program. The tests include independent testing of the undervoltage trip attachments and shunt trip attachments of the reactor trip breakers.

7.2.5 INTERACTION OF CONTROL AND PROTECTION SYSTEMS

7.2.5.1 Introduction

The design basis for the control and protection systems permits the use of a sensor for both protection and control functions. Where this is done, all equipment common to both the protection and control circuits is classified as part of the protection system. Isolation amplifiers prevent a control system failure from affecting the protection system. In addition, where failure of a protection system component can cause a process excursion which requires protective action, the protection system can withstand another independent failure without loss of function. Generally, this is accomplished with two-out-of-four trip logic. Also, wherever practical, provisions are included in the protection system to prevent a plant outage because of single failure of a sensor.

Evaluation of the Ginna Station Reactor Trip System (RTS) isolation was performed as part of the SEP, Topic VII-1.A. The safety evaluation concluded (*Reference 1*) that the Reactor Trip System (RTS) is adequately isolated from non-safety systems and satisfies the criteria set forth in 10 CFR 50, Appendix A (GDC 24), and IEEE-279 (1971), Section 4.7.2.

7.2.5.2 Specific Control and Protection Interactions

7.2.5.2.1 **Nuclear Flux**

Four power-range nuclear flux channels are provided for overpower protection. (See Drawings 33013-1353, Sheet 2 and 33013-1353, Sheet 10.) Isolated outputs from all four channels are averaged for automatic control rod regulation of power. If any channel fails in such a way as to produce a low output, that channel is incapable of proper overpower protection. In principle, the same failure would cause rod withdrawal and overpower. Two-out-of-four overpower trip logic will ensure an overpower trip if needed even with an independent failure in another channel.

In addition, the control system will respond only to rapid changes in indicated nuclear flux; slow changes or drifts are overridden by the temperature control signal. Also, a rapid decrease of any nuclear flux signal will block automatic[a] rod withdrawal as part of the rod drop protection circuitry. Finally, an overpower signal from any nuclear channel will block automatic[a] and manual rod withdrawal. The setpoint for this rod stop is below the reactor trip setpoint.

7.2.5.2.2 **Coolant Temperature**

Four T_{AVG} channels are used for overtemperature-overpower protection. Isolated output signals from all four channels are also averaged for automatic control rod regulation of power and temperature. In principle, a spuriously low temperature signal from one sensor would partially defeat this protection function and also cause rod withdrawal and overtemperature. Two-out-of-four trip logic is used to ensure that an overtemperature trip will occur if needed even with an independent failure in another channel.

In addition, channel deviation alarms in the control system will block automatic rod motion (insertion or withdrawal[b]) if any temperature channel deviates significantly from the others. Automatic[b] and manual rod withdrawal blocks will also occur if any two of four nuclear channels indicates an overpower delta T condition or if any two of four temperature channels indicates an overtemperature delta T condition. Finally, as shown in Section 15.4.2, the combination of trips on nuclear overpower, high pressurizer water level, and high pressurizer pressure also serves to limit an excursion for any rate of reactivity insertion.

---

a. The automatic rod withdrawal function of the reactor control system has been disabled. Rod blocks for automatic rod withdrawal on rod drops are no longer required.

b. The automatic rod withdrawal function of the reactor control system has been disabled. Rod blocks for automatic rod withdrawal are no longer required.

7.2.5.2.3 Pressurizer Pressure

Three high pressure and four low pressure channels are used for high pressure and low pressure protection and for overpower and overtemperature protection.

Isolated output signals from these channels also are used for pressure control. These are discussed separately below.

A. Control of rod motion: the discussion for coolant temperature is applicable, i.e., two-out-of-four logic for overpower-overtemperature protection as the primary protection, with backup from multiple rod stops and "backup" trip circuits.

B. Pressure control: spray, Pressurizer Power Operated Relief Valves (PORV), and heaters are controlled by isolated output signals from the pressure protection channels.

Low pressure

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

In addition, interlocks are provided in the pressure control system such that a relief valve will close if either of two independent pressure channels indicates low pressure. Spray reduces pressure at a lower rate and sometimes is available for operator action (about 3 minutes at maximum spray rate before a low pressure trip is required).

High pressure

The pressurizer heaters are incapable of overpressurizing the reactor coolant system. Maximum steam generation rate with heaters is about 7500 lb/hr, compared with a total capacity of 576,000 lb/hr for the two safety valves and a total capacity of 358,000 lb/hr for the two Pressurizer Power Operated Relief Valves (PORV). Therefore, overpressure protection is not required for a pressure control failure. Two-out-of-three high pressure trip logic is therefore used.

In addition, either of the two Pressurizer Power Operated Relief Valves (PORV) can easily

maintain pressure below the high-pressure trip point. The two Pressurizer Power Operated Relief Valves (PORV) are controlled by independent pressure channels, one of which is independent of the pressure channel used for heater control. Finally, the rate of pressure rise achievable with heaters is slow, and ample time and pressure alarms are available for operator action.

7.2.5.2.4 Pressurizer Level

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

The pressurizer level instrument utilizes an open reference leg, which is maintained full by condensing steam from the pressurizer vapor space. Three pressurizer level transmitters are fed from independent reference legs. Channel independence is maintained from the reference leg to the sensors to the relays providing the trip logic as required by Section 7.1.2. This design is adequate for controlling pressurizer level and for safely performing all protection and safeguards functions.

High level

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

Low level

A signal of low level from either of two independent level control channels will isolate letdown, thus preventing the loss of coolant. Ample time and alarms exist for operator action.

7.2.6 ANTICIPATED-TRANSIENT-WITHOUT-SCRAM MITIGATION SYSTEM ACTUATION CIRCUITRY

10 CFR 50.62 requires that all PWRs provide a means that is diverse and independent from the existing Reactor Trip System (RTS) for tripping the main steam turbine and initiating auxiliary feedwater flow following an anticipated transient without scram (ATWS) event. Anticipated transients include loss of normal feedwater flow, loss of electrical load that results in closure of the turbine stop valves, and loss of offsite power. Rochester Gas & Electric has installed a system providing ATWS mitigation system actuation circuitry (AMSAC) at Ginna Station that satisfies the 10 CFR 50.62 requirement (*Reference 2*). The AMSAC is based on low feedwater flow logic. The AMSAC is a non-Class 1E system designed to trip the turbine and start the motor-driven (MDAFW) and turbine-driven (TDAFW) auxiliary feedwater pumps if main feedwater flow is lost with reactor power above 40%. The actuation signal has a variable time delay that is a function of reactor power, to permit time to recover from partial loss of feedwater flow, if possible, without initiating AMSAC. In addition, a power level lock-in feature latches the timing value of the variable timer, for that power, at the moment an ATWS event actuates. Existing feedwater flow and turbine first-stage pressure instruments provide the necessary input signals. The AMSAC system is powered from the technical support center battery.

Four feedwater flow signals, two per loop, are used to detect the loss of main feedwater. Any three of the four channels indicating a loss of flow will call for initiation of auxiliary feedwater and a turbine trip.

The actuation signals are blocked (C-20 permissive) below a level of 40% reactor power, as determined by one of two turbine first stage pressure signals being below predetermined setpoints. Both of the turbine first-stage pressure signals exceeding their setpoint (corresponding to 40% reactor power) will arm the AMSAC logic and permit actuation of the turbine trip and auxiliary feedwater start circuits. To ensure the AMSAC system remains armed sufficiently long to perform its function in the event of a turbine trip, the C-20 permissive signal will be maintained via a preset time delay for at least 30 sec longer than the value of the variable timer at 40% nominal reactor power after the turbine trip has occurred. This interlock is provided since it has been demonstrated that the reactor coolant system pressure does not approach the ASME stress level C limit of 3200 psig when an ATWS event occurs below 40% reactor power. This is to ensure that spurious AMSAC actuations do not occur at low power operations and during startup. The block will automatically be removed as reactor power increases above the 40% level and reinstated as reactor power decreases below the 40% level.

The AMSAC signal processing hardware is Foxboro Spec 200 and Spec 200 Micro and is housed in a Spec 200 instrument rack (Fox 3 Rack) in the relay room. The existing feedwater flow and turbine first-stage pressure signals are input to the AMSAC from racks in the control and relay rooms via the relay room cable trays. In addition, AMSAC status lights and a manual bypass switch are installed on the main control board. The AMSAC output actuation signals are input to the existing turbine trip and auxiliary feedwater start logic via qualified output relays. The AMSAC equipment power supply must be independent of existing Reactor Trip System (RTS) power supplies and shall not fail upon loss of offsite power. The technical support center battery satisfies these requirements. The AMSAC 120-V ac power supply is obtained from a static inverter, which receives its input from the technical support center battery.

During power operations, operability of the AMSAC is testable from each analog input to

the final output actuation relay. The AMSAC actuation logic can be bypassed by the manual bypass switch to preclude actually tripping the turbine and starting auxiliary feedwater flow. Indication that the AMSAC is in the bypass mode is continuously displayed in the control room. During shutdown, operability of the system can be tested from the analog inputs to verification of turbine trip and initiation of auxiliary feedwater flow. Maintenance and testing at power is also possible by placing the system in the bypass mode.

REFERENCES FOR SECTION 7.2

1. Letter from D. M. Crutchfield, NRC, to L. D. White, Jr., RG&E, Subject: SEP Topic VII-1.A; Reactor Protection System Isolation, dated December 12, 1980.

2. Letter from C. Stahle, NRC, to R. C. Mecredy, RG&E, Subject: Safety Evaluation Report on Compliance with ATWS Rule, 10 CFR 50.62(c)(1), dated March 16, 1989.

Table 7.2-1
Table DELETED

Table DELETED

Table 7.2-2
PERMISSIVE CIRCUITS

Permissive Number	Function	Input
1	Rod stop on overpower	1/4 high nuclear flux (power range); 1/2 high nuclear flux (intermediate range); 2/4 overtemperature delta T; or 2/4 overpower delta T.
2	Auto-rod withdrawal stop at low powers	1/1 low MWe load signal
3	Auto-rod withdrawal stop on rod drop	1/4 rapid decrease of nuclear flux or rod bottom indication
4	Steam dump interlock	1/1 rapid decrease of MWe load signal
5[a]		
6	Manual block of source range level trip	1/2 high intermediate range allows manual block, 2/2 low intermediate range defeats block
7	Permissive power (block various trips)	3/4 low-low nuclear flux or 1/2 low MWe load signal
8	Block single primary loop loss of flow trip	3/4 low nuclear power
9	Block reactor trip on turbine trip	3/4 low nuclear flux and steam bypass unblocked
10	Manual block of low power trip and intermediate range trip	2/4 high nuclear flux allows manual block, 3/4 low nuclear flux defeats manual block

a. Not applicable to this plant.

Table 7.2-3
REACTOR TRIP FUNCTION SETPOINTS

Reactor Trip Function	Limiting Safety System Setting	Protection
Source range high flux	≤ $1x10^5$ CPS	Shutdown reactivity change start-up accident
Intermediate range high flux	current equivalent to ≤ 25.7% rated thermal power	Start-up accident
Power range high flux (low setpoint)	a	Start-up accident
Power range high flux (high setpoint)	a	Overpower
Single loop low flow	a	DNB
Two loop low flow	a	DNB
Manual	NA	Operator judgement
4-kV bus undervoltage	≥ 3101 volts	Anticipatory loss of RCS flow, DNB
4-kV bus under frequency	a	Anticipatory loss of RCS flow, DNB
Overtemperature ΔT	a	DNB
Overpower ΔT	a	Excessive kW/ft

Reactor Trip Function	Limiting Safety System Setting	Protection
Pressurizer low pressure	a	DNB limits range of overtemperature ΔT
Pressurizer high pressure	a	RCS overpressure
Steam generator low-low level	a	Loss of heat sink
Turbine trip		Limits temperature and pressure transients on reactor imposed by turbine trip
Autostop oil pressure or	≥ 45 psig	
Turbine stop valves	Closed	
Safety injection	Any of 4 safety injection signals	Trips reactor to limit DNB
Pressurizer high level	a	Prevent water relief through pressurizer safety valves and RCS integrity

a. Technical Specifications Table 3.3.1-1 specifies the limiting Trip Setpoint for Reactor Trip functions credited in the accident analyses.

7.3 ENGINEERED SAFETY FEATURES SYSTEMS

The engineered safety features systems are used to provide protection against the release of radioactive materials in the event of a loss-of-coolant accident or a secondary line break accident. The engineered safety features systems function to maintain the reactor in a shutdown condition. They also provide sufficient core cooling to limit the extent of fuel and fuel cladding damage and to ensure the integrity of the containment structure. These functions rely on the Engineered Safety Features Actuation System (ESFAS) and associated instrumentation and controls.

7.3.1 DESIGN CRITERIA

The design criteria discussed in Section 7.2.1 for the Reactor Trip System (RTS) are equally applicable for the engineered safety features actuation. The following criteria were used during the licensing of Ginna Station. They represent the Atomic Industrial Forum (AIF) version of proposed criteria issued by the AEC for comment on July 10, 1967 (see Section 3.1.1). Conformance with 1972 General Design Criteria of 10 CFR 50, Appendix A is discussed in Section 3.1.2. The criteria discussed in Section 3.1.2 as they apply to the engineered safety features systems include 2, 4, 13, 19, 20, 21, 22, 23, 24, and 29.

7.3.1.1 Protection Systems

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

The Engineered Safety Features Actuation System (ESFAS) provides actuation of the following functions: safety injection, containment isolation, steam line isolation, containment spray and feedwater isolation, automatic diesel startup, and preferred auxiliary feedwater pump startup.

The safety injection system delivers water to the reactor core following a loss-of-coolant accident. The principal components of the safety injection system are two passive accumulators (one for each loop), three high-head safety injection pumps, two low-head safety injection (residual heat removal) pumps, and the essential piping and valves. The accumulators are passive devices which discharge into the cold leg of each loop.

The safety injection system may be actuated by two-out-of-three low-pressurizer-pressure signals, two-out-of-three low-steam-line-pressure signals, two-out-of-three high-containment-pressure signals; or the system can be actuated manually. Any of the safety injection system signals will open the system isolation valves, start the high-head safety injection pumps and the low-head (residual heat removal) pumps (see Section 6.3).

The steam line isolation valves are closed upon receipt of high steam line flow in conjunction with a safety injection system signal, by containment pressure, or by manual initiation. See Section 6.2.4.3 and Section 7.3.2.2.1 for a more detailed description of steam line isolation.

The containment spray system consists of two pumps, one spray additive tank, valves, piping, and spray nozzles. Containment spray is initiated by coincident signals from two sets of two-out-of-three containment pressure signals monitoring containment high-high pressure. The

actuation signal starts the pumps and opens the discharge valves to the spray header. Valves for the spray additive tank open after a very short time delay.

Containment isolation is initiated by an automatic safety injection system signal or manually. Actuation of containment isolation trips the containment sump pumps, closes containment isolation valves (as discussed in Section 6.2.4 and listed in Tables 6.2-29 and 6.2-32), and trips the purge supply and exhaust fans. Containment ventilation isolation and depressurization valves are also isolated on high containment activity (R-11 and R-12), any safety injection signal, or from a manual containment spray signal. See Section 6.2.4.3 for a more detailed description of containment isolation and containment ventilation isolation.

The feedwater isolation system consists of the two main feedwater regulating valves, two main feedwater regulating valve bypass valves, and two main feedwater isolation valves. The main feedwater regulating valves and the main feedwater regulating bypass valves close when they receive a safety injection system signal or an engineered safety feature sequence initiation signal. They fail closed if power or air is lost. The two main feedwater isolation valves close when they receive a safety injection signal. They fail close if power or instrument air is lost. See Section 7.3.2.2.2 for a more detailed description of feedwater isolation.

Automatic diesel startup will be caused by undervoltage at the engineered safety features buses in addition to being caused by the safety injection signal.

The motor-driven auxiliary feedwater pumps (MDAFW) start upon a safety injection signal, either steam-generator low-low level, loss of both main feedwater pumps, or ATWS Mitigation System Actuation Circuitry (AMSAC) actuation. The turbine-driven auxiliary feedwater pump (TDAFW) will start on low-low level in both steam generators and loss of bus voltage on 11A and 11B. See Section 7.3.2.2.2 and Section 7.2.6 for a more detailed description of auxiliary feedwater pump starts.

7.3.1.2 Redundancy and Independence

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

The initiation of the engineered safety features provided for loss-of-coolant accidents (e.g., high-head safety injection and residual heat removal pumps, and containment spray systems) is accomplished from several signals derived from reactor coolant system and containment instrumentation. Channel independence is carried throughout the system from the sensors to the signal output relays including the power supplies for the channels. (Routing and separation standards applicable to existing cables are those that were invoked at the time of cable installation. For more information, see Section 8.3.1.4.) The initiation signal for containment spray comes from coincidence of two sets of two-out-of-three high-high containment pressure signals. The containment fan cooler recirculation system is initiated by a safety injection signal and the dampers are aligned to make use of the charcoal filters.

The signal for containment isolation of non-vital valves, i.e., the isolation valves trip signal, is derived from an automatic safety injection signal. This setpoint for safety injection input from coincident two-out-of-three containment high-pressure signals is below that for containment spray actuation.

Strict administrative control prevents the opening of large penetrations during reactor operation. For example, personnel locks are interlocked to ensure that one door is always closed, with verification by signals in the main control room. Ventilation purge valves also must be maintained closed at all times while the reactor is critical and cannot be opened until the reactor has been subcritical for at least 1 hr. (See Section 6.2.4.4.9. for a description of current containment purging methodology.)

The Ginna onsite emergency ac power system consists of two redundant diesel-generator power trains. Diesel generator 1A supplies 480-V buses 14 and 18 and diesel generator 1B supplies 480-V buses 16 and 17.

Manual means exist to tie buses 17 and 18 through a tie breaker and to tie buses 14 and 16 through two tie breakers. The control circuit for each electrically operated breaker provides interlocks such that the breaker cannot be closed if more than one diesel generator or normal supply breaker is closed on either bus. Additionally, if the tie breakers are closed, they will trip upon a safety injection signal or when an undervoltage signal is received from both buses the breaker ties together. Restoration of normal supply or diesel generator supply breakers onto a bus requires the respective bus tie breaker to be opened. For buses 14 and 16, manual operation would be required to physically insert and close the manually operated bus tie breaker at bus 14. For buses 17 and 18, manual operation would be required to physically insert the bus tie breaker prior to electrically closing the breaker.

7.3.1.3 Testing While In Operation

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

The testability of the protection channels at power is discussed in Section 7.2.1.

Periodic testing of the diesel generators is routinely performed to ensure their operability. During power operation, surveillance testing verifies that the fuel transfer system is operational, the diesels start from normal standby conditions, the generators are properly synchronized and loaded, and that proper alignment is made so that the diesel generators could supply safeguards bus power. During shutdown conditions, the diesel generators are tested to ensure they can restore safeguards bus voltage in a timely manner by automatically actuating breakers in the time period required.

7.3.1.4 Fail Safe Design

CRITERION: The protection systems shall be designed to fail into a safe state or into a state established as tolerable on a defined basis if conditions such as disconnection of the systems, loss of energy (e.g., electrical power, instrument air), or adverse

environments (e.g., extreme heat or cold, fire, steam, or water) are experienced (AIF-GDC 26).

The design criterion for the protection systems in general is addressed in Section 7.2.1.

7.3.2 SYSTEM DESCRIPTION

The function of the instrumentation and control associated with the engineered safety features is to supply component trip signals and to initiate the engineered safety features.

The Engineered Safety Features Actuation System (ESFAS) logic and sequence are shown in Drawing 33013-1353, Sheets 6 through 9. The major difference between the engineered safety features instrumentation and the Reactor Trip System (RTS) instrumentation (Section 7.2.2) is that each protective action is initiated by two pairs of coincident input signals which actuate the engineered safety features equipment. Protective action is initiated when either of the two channels becomes deenergized.

Sensors, process and nuclear instrumentation, and protection cabinets are discussed in Section 7.2.2.1. The Engineered Safety Features Actuation System (ESFAS) logic controls are arranged and operate in a similar manner to that of the reactor trip logic cabinets. There are four cabinets for each protection train. Each cabinet receives protection signals from the safeguards bistables in the protection cabinets. All of the cabinets are divided into two sections by a metal divider plate. The safeguards logic relays are located in the front section, and master and auxiliary relays are positioned in the rear of the cabinets. The safeguards logic relay coils are powered by the actuation bistables in the protection cabinets and are energized during normal operations. As in the reactor trip logic cabinets, the logic relay contacts are arranged in a logic matrix, a major difference being the safeguards logic relay contacts are shut when the respective coil is deenergized. The logic matrices are wired in series with the master relay and a power supply, which therefore regulate the relays state of operation. The master relay contacts control the power supplied to the auxiliary relays. One master relay controls several auxiliary relays. The auxiliary relays in turn control the automatic operation of various pieces of engineered safety features equipment.

When a condition within the reactor plant occurs that requires engineered safety features actuation, the protection bistables will switch to the OFF state at the output. Once this occurs, the safeguards logic relays will deenergize, shutting their contacts. When the required number of logic relay contacts within the logic matrix shut, the master relay will energize, closing its contacts and activating the auxiliary relays. As the auxiliary relays contacts shut, different pieces of engineered safety features equipment start up or operate to mitigate the detected unsafe condition.

7.3.2.1 Initiating Circuitry

The Engineered Safety Features Actuation System (ESFAS) circuitry and hardware layout are designed to maintain circuit isolation through the bistable-operated logic relays. The channelized design follow-through is shown in Figure 7.3-4.

The safeguards bistables, mounted in the analog protection racks, drive both A and B logic matrix relays. Each matrix contains its own test light and test circuitry. Control power for

logic channels A and B is supplied from dc sources 1 and 2, respectively. These redundant actuating channels operate the various engineered safety features components that are required, with the large loads sequenced as necessary.

Manual reset of the Engineered Safety Features Actuation System (ESFAS) relays may be accomplished at any time following their operation. Once reset action is taken, the master relay is reset and its operation blocked until the engineered safety features initiating signal clears, at which time it is automatically unblocked and restored to service.

Protection channel separation is maintained by metal barriers arranged as shown in Figure 7.3-4. Protection channel identity is lost in the intermixing of the relay matrix wiring. Separation of A and B logic channels is maintained by the separate logic racks.

7.3.2.2 System Functions

The engineered safety features instrumentation automatically performs the following vital functions:

1. Starts operation of the safety injection system.
2. Operates the containment isolation and ventilation isolation valves.
3. Starts the containment spray system upon detection of a higher containment pressure signal than required in item 2 above, based on coincidence of two sets of two-out-of-three high-pressure signals.
4. Starts the containment fan cooler recirculation system.

7.3.2.2.1 **Steam Line Isolation**

Either of the following signals will initiate steam line isolation:

1. One-out-of-two high-high steam flow in a particular steam line in coincidence with any safety injection signal will close the main steam isolation valve in that line. One-out-of-two high steam flow in a steam line in coincidence with two-out-of-four indications of low T_{AVG} and any safety injection signal will also close the main steam isolation valve in that line.
2. Two-out-of-three high-high-containment-pressure signals will close both main steam isolation valves.
3. Manual steam line isolation (pushbutton) will close the associated main steam isolation valve.

7.3.2.2.2 **Feedwater Line Isolation**

The feedwater isolation system consists of two main feedwater isolation valves, two main feedwater regulating valves, and two main feedwater regulating bypass valves. The main feedwater regulating valves and the bypass valves close when they receive a safety injection system signal or an engineered safety feature sequence initiation signal. They fail close if power or air is lost. Any safety injection signal will redundantly isolate the feedwater lines by (1) venting the supply air to all main feedwater regulating valves causing valves to close, (2)

closing the main feedwater isolation valves, and (3) tripping the main feedwater pumps, including closure of the feedwater pump discharge valves.

Additional safety features are provided to prevent emergency conditions from becoming accident conditions. These are:

1. Automatic diesel startup will be caused by low voltage on the feeder lines to the engineered safety features buses in addition to being caused by the safety injection signal.
2. The motor-driven auxiliary feedwater pumps (MDAFW) start upon a safety injection signal, steam generator low-low level on either steam generator, trip of both main feedwater pumps, or ATWS Mitigation System Actuation Circuitry (AMSAC) actuation.
3. The turbine-driven auxiliary feedwater pump (TDAFW) will start on low-low level in both steam generators, loss of voltage on both 4160-V buses 11A and 11B, or AMSAC actuation.
4. The TDAFW pump dc Lube Oil Pump can be powered by a portable diesel generator (DC) in the emergency event of a loss of site AC and DC power, to maintain proper steam generator level.
5. The Main Feedwater Regulating Valves (MFRV) and bypass valves will close after a reactor trip in coincidence with low T_{AVG}, if the valves are in automatic control.
6. The MFRV and bypass valve for a steam generator will close on high steam generator level in the associated steam generator.

The 4-k V buses 11A and 11B loss of voltage trip setpoint for the start of the turbine driven auxiliary feedwater (TDAFW) pump is 2870-Volts.

The trip logic for the Engineered Safety Features Actuation System (ESFAS) is shown in Drawing 33013-1353, Sheets 6, 7, and 9.

7.3.2.3 Sensing and Display Instrumentation

The following instrumentation helps to monitor the effective operation of the engineered safety features:

7.3.2.3.1 Reactor Vessel Level Indication System

Redundant differential pressure transducers are used to monitor reactor vessel coolant level during all phases of plant operation, including postaccident conditions with quasi-steady-state conditions and during relatively slow developing transients. The system provides trending of reactor vessel coolant inventory to ensure adequate core cooling during these postaccident and transient conditions. (Section 7.6.5.)

7.3.2.3.2 Containment Pressure

Six channels monitoring containment pressure reflect the effectiveness of engineered safety features.

7.3.2.3.3 Containment Sump Level

Redundant containment sump B level indicators (LI-942 and LI-943) show that water has been delivered to the containment following an accident and that, subsequently, the residual heat removal pumps will be effective in providing recirculation flow. These containment sump B level indicating switches are designed to withstand accident conditions.

7.3.2.3.4 Accumulator Level and Pressure

Redundant pressure and level transmitters for each accumulator provide information about the ability of the accumulators to discharge their contents into the reactor coolant system cold legs following a loss-of-coolant accident.

7.3.2.3.5 Refueling Water Storage Tank Level (RWST)

Two channels indicate that safety injection and containment spray have removed water from the storage tank and provide information on when to initiate the sump switchover emergency procedure.

7.3.2.3.6 Sodium Hydroxide Tank Level and Flow

Transmitters provide information necessary to determine the quantity of NaOH injected into the containment spray system during the injection and recirculation phases following a loss-of-coolant accident.

7.3.2.3.7 Safety Injection Pumps Discharge Pressure and Flow

These channels clearly show that the safety injection pumps are operating and delivering sufficient flow to the proper loops. The pressure transmitters are outside the containment; the flow transmitters are inside the containment.

7.3.2.3.8 Residual Heat Removal (Low-Head Safety Injection) Flow

Redundant transmitters provide the capability to determine the effectiveness of these pumps to deliver the necessary flow.

7.3.2.3.9 Pump Energization

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

7.3.2.3.10 Valve Position

All active engineered safety features valves have position indication on the control board to show proper positioning of the valves. Air-operated and solenoid-operated valves are selected so as to move in a preferred direction on the loss of air or power. Motor-operated valves remain in their positions at the time of loss of power to the motor.

7.3.2.3.11 Residual Heat Exchangers

Combined exit flow is indicated and combined inlet temperature is recorded on the control board to monitor operation of the residual heat exchangers. In addition, the exit temperature of each heat exchanger is locally indicated. These transmitters are outside reactor containment.

7.3.2.3.12 Alarms

Visual and audible alarms are provided to call attention to abnormal conditions. The alarms are of the individual acknowledgement type; that is, the operator must recognize and silence the audible alarm for each alarm point. For most control systems, the sensing device and circuits for the alarms are independent, or isolated from, the control devices.

7.3.2.3.13 Air Coolers

The cooling water discharge flow and exit temperature of each of the four containment fan coolers are alarmed in the control room if the flow is low or if the temperature is high. The transmitters are outside the reactor containment. In addition, the exit flow is monitored for radiation and alarmed in the control room if high radiation should occur. This is a common monitor and the faulty cooler can be detected locally by manually valving each one out in turn.

7.3.2.3.14 Local Instrumentation

In addition to the above, the following local instrumentation is available:

- Residual heat removal (RHR) pumps discharge pressure.
- Residual heat exchanger exit temperatures.
- Containment spray (CS) test lines total flow.
- Safety injection (SI) test line flow and SI pump pressure.

7.3.2.4 Engineered Safety Features Reset Controls

Safety Injection Circuit. This circuit has a reset switch which gives the operator the means of resetting safety injection 1 minute or longer after initiation. Actuation of the reset switch only does not change the state of any equipment but permits the operator to place the equipment affected by safety injection to the position desired.

Containment Ventilation Isolation Circuit. This circuit has been modified to ensure that no equipment changes state upon the actuation of the containment ventilation isolation reset switch. Once the reset switch has been actuated, the operator must then operate the control module switch/indicator on the containment isolation reset pushbutton panel for equipment requiring change of state.

Containment Isolation Circuit. This circuit has been modified to ensure that no equipment changes state upon the actuation of the containment isolation reset switch. Once the reset switch has been actuated the operator must then operate the control module switch/indicator on the containment isolation reset pushbutton panel for equipment requiring change of state.

Containment Spray Circuit. This circuit has a reset switch which gives the operator the means of resetting containment spray. Once the reset switch has been actuated, the spray additive tank discharge valves will return automatically to the position called for by their controllers.

The containment spray pumps and their discharge valves would require operator action to change state. This capability is necessary so the operator has flexibility in dealing with postaccident conditions within containment (i.e., loss-of-coolant accident or steam line break).

7.3.3 DESIGN EVALUATION

7.3.3.1 Engineered Safety Features Systems Isolation

The engineered safety features control logic and design were evaluated under the Systematic Evaluation Program (SEP), Topic VII-2 (*Reference 1*), as it conforms to 10 CFR Part 50, Appendix A; General Design Criteria 22 and 24; and IEEE 279-1971. The evaluation concluded that nonsafety systems which are electrically connected are properly isolated from the engineered safety features and that the isolation devices meet the above licensing criteria.

7.3.3.2 Loss of Voltage or Degraded Voltage on Engineered Safety Features Bus

The loss of voltage and degraded voltage trips ensure operability of engineered safety features equipment during a postulated design-basis event concurrent with a degraded bus voltage condition.

The undervoltage setpoints are selected so that engineered safety features motors will start and accelerate the driven loads (pumps) within the required time and will be able to perform for long periods of time at degraded conditions above the trip setpoints without significant loss of design life. All control circuitry or safety-related control centers and load centers, except for motor control centers M and L, are dc. Therefore, degraded grid voltages do not affect these control centers and load centers. Motor control centers M and L, which supply the standby auxiliary feedwater system, are fully protected by the undervoltage setpoints. Further, the standby system is normally not in service and is manually operated only in the event of a total loss of feedwater and preferred auxiliary feedwater. Degraded and loss of voltage conditions are discussed in Sections 8.3.1.1.4.1. and 8.3.1.2.7.

7.3.4 TESTING

7.3.4.1 Analog Channel Testing

The basic elements comprising an analog protection channel are shown in Figure 7.3-6. This system consists of a transmitter, power supply, bistable, bistable trip switch and proving lamp, test signal injection switch, test signal injection jack, and test point.

Each protection rack will include a test panel containing those switches, test jacks, and related equipment needed to test the channels contained in the rack. A hinged cover encloses the signal injection switch and signal injection jack of the test panel.

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

Administrative procedures will require that selected bistables in the channel under test be placed in the tripped mode prior to test. This provision applies to bistable functions that do not result in a reactor trip or ESFAS actuation if a redundant channel is placed in a trip condition intentionally or due to a failure. This places a proving lamp across the bistable output so that the bistable trip setting can be checked during channel calibration. The bistable trip switches must be manually reset after completion of a test. Closing the test panel cover will not restore these switches to the untripped mode. To prevent safety injection trip, procedures limit bistable testing to one circuit at a time.

Administrative procedures will allow selected Reactor Trip System (RTS) and Engineered Safety Features Actuation System (ESFAS) bistables to be bypassed during surveillance testing (Channel Operational Test and Channel Calibration). The bypass circuitry applies to bistable functions that do result in a reactor trip or ESFAS actuation if a redundant channel is placed in a trip condition intentionally or due to a failure. Bypass circuitry allows a channel to be tested without tripping the channel by imposing a 120 VAC power signal in parallel, thus maintaining the Relay Protection System in an untripped condition. Nuclear Instrumentation System power range functions may be bypassed with permanently-installed bypass test panels located within the rear of the NIS Cabinets. Other RTS and ESFAS system functions will be capable of being bypassed utilizing a portable test box that connects to permanent connectors in the Reactor Protection cabinets.

Actual channel calibration will consist of producing a test signal using the transmitter power supply external calibration device which plugs into the signal injection jack. In this application, where specified, the channel power supply will serve as a power source for the calibration device to permit verifying the output load capacity of the power supply. Test points are located in the analog channel and provide an independent means of measuring and/or monitoring the calibration signal level.

7.3.4.2 Logic Channel Testing

Figure 7.3-6 shows the basic logic test scheme. Test switches will be located in the associated relay racks rather than in a single test panel. The following procedures will be used for testing the logic matrices:

A. Following administrative procedure, test channel A or B one at a time.

B. Select a matrix and turn the test switches to TEST, then depress the push button. Test lights will glow upon actuation of the matrix being tested. Release pushbutton and return test switch to OPERATE. ON TEST lights glow any time any switch is in a test position. Test lights can be tested by depressing the lens.

C. Verify master actuating relay coil integrity by connecting ohmmeter across coil terminals.

REFERENCES FOR SECTION 7.3

1. Letter from D. M. Crutchfield, NRC, to J. E. Maier, RG&E, Subject: SEP Topic VII-2, Engineered Safety Features System Control Logic and Design, Safety Evaluation for Ginna, dated December 28, 1981.

7.4 SYSTEMS REQUIRED FOR SAFE SHUTDOWN

7.4.1 DESCRIPTION

In the Systematic Evaluation Program (SEP) review of safe shutdown systems for Ginna Station, the NRC Staff and RG&E developed a list of the minimum systems necessary to take the reactor from operating conditions to MODE 5 (Cold Shutdown). Although other systems may be used to perform shutdown and cooldown functions, the following list is the minimum number of systems required to fulfill the criteria of Branch Technical Position RSB 5-1 (*Reference 1*).

1. Reactor Trip System (RTS).
2. Auxiliary feedwater system.
3. Main steam system.
4. Service water (SW) system.
5. Chemical and volume control system.
6. Component cooling water (CCW) system.
7. Residual heat removal system.
8. Electrical instrumentation and power systems for the above systems.

Five basic tasks, or functions, are required to proceed from plant power operation to MODE 3 (Hot Shutdown) to MODE 5 (Cold Shutdown). These functions and their associated alternate methods are identified in Table 7.4-1.

7.4.1.1 Reactor Trip System (RTS)

The Reactor Trip System (RTS) is described in Section 7.2.

The Reactor Trip System (RTS) is designed on a channelized basis to achieve isolation and independence between redundant protection channels. Channel independence is carried throughout the system extending from the sensor to the relay providing the logic. Isolation of redundant analog channels originates at the process sensors and continues back through the field wiring and containment penetrations to the analog protection racks. When safety and control functions are combined, both functions are fully isolated in the remaining part of the channel, control being derived from the primary safety signal path through an isolation amplifier. As such, a failure in the control circuitry does not affect the safety channel. Reactor Trip System (RTS) channels are supplied with sufficient redundancy to provide the capability for channel calibration and testing at power. Bypass removal of one trip circuit is accomplished by placing that circuit in a half-tripped mode, i.e., a two-out-of-three circuit becomes a one-out-of-two circuit. Testing does not trip the system unless a trip condition concurrently exists in a redundant channel.

The power supplies to the channels are fed from four instrument buses. Two of the buses are supplied by constant voltage transformers and two are supplied by inverters. Each channel is energized from a separate ac power feed. Each reactor trip circuit is designed so that a trip occurs when the circuit is deenergized. An open circuit or the loss of channel power causes

the system to go into its trip mode. Reliability and independence are obtained by redundancy within each tripping function. In a two-out-of-three circuit, the three channels are equipped with separate primary sensors and each channel is energized from an independent electrical bus. A single failure may be applied in which a channel fails to deenergize when required; however, such a malfunction can affect only one channel. The trip signal furnished by the two remaining channels is unimpaired in this event.

7.4.1.2 Auxiliary Feedwater Systems

The auxiliary feedwater systems are described in Section 10.5.

The preferred auxiliary feedwater system is divided into two independent trains. There are two motor-driven pumps powered from separate redundant 480-V safeguards emergency buses which can receive power from either onsite or offsite sources. Each motor-driven pump can provide 100% of the preferred auxiliary feedwater system flow required for decay heat removal and can be cross-connected to provide flow to either steam generator. There is also a turbine-driven pump which can receive motive steam from each steam line and provide flow to either or both steam generators. The turbine-driven pump provides 200% of the flow required for decay heat removal.

A standby auxiliary feedwater system (SAFW) provides flow in case the preferred auxiliary feedwater system pumps are inoperable. The standby auxiliary feedwater system (SAFW) uses two motor-driven pumps which can be aligned to separate service water (SW) system loops. The standby auxiliary feedwater system (SAFW) has the same features as the preferred auxiliary feedwater system pumps with regard to functional capability and power supply separation. The system is manually actuated from the control room.

The standby pumps (SAFW) are electrically interlocked with the primary motor-driven pumps (MDAFW). The interlocks prevent inadvertent actuation of either standby pump when its associated motor-driven auxiliary feedwater pump (MDAFW) is available. Standby auxiliary feedwater pump (SAFW) C cannot be manually started if preferred motor driven auxiliary feedwater pump (MDAFW) A is operating, and standby pump D cannot be started if preferred motor driven auxiliary feedwater pump (MDAFW) B is operating. The primary purpose of the interlocks is to prevent both pumps (A and C or B and D) from being energized simultaneously and overloading the emergency diesel generator on loss of offsite power.

7.4.1.3 Main Steam System

The main steam system is described in Section 10.3.

The safety-grade shutdown components associated with the main steam system are the main steam isolation valves, the steam safety valves, and the steam atmospheric dump valves. Each of the two steam generators is equipped with an air-operated, solenoid-controlled main steam isolation valve, four steam safety valves, and one air-operated atmospheric dump valve. The main steam isolation valves will shut upon loss of control air. For core decay heat removal with natural circulation of the reactor coolant, only one steam generator and one of its four safety valves are required to remove core decay heat a few seconds after reactor trip. One atmospheric steam dump, which can be operated from the control room, is also sufficient

for maintaining MODE 3 (Hot Shutdown) or to achieve cooldown of the reactor coolant system below MODE 3 (Hot Shutdown) conditions.

Boiling of feedwater in the steam generator is the dominant mode of removing primary system heat. Normally, the energy in the steam is removed in the turbine and the main condenser. After the turbine is tripped, the turbine bypass system provides a controlled steam release directly to the condenser. The ultimate heat sink for the condenser is the circulating water system. When the condenser is not available, the steam is released directly to the atmosphere through either the steam safety valves or the atmospheric dump valves. As the steam is lost, a continuing source of feedwater is required.

7.4.1.4 Service Water System

The service water (SW) system is described in Section 9.2.1.

The service water (SW) system circulates water from the screen house to various heat exchangers and systems in the containment, auxiliary, and turbine buildings. The system has four pumps, three of which have the capacity to supply normal cooling loads. One pump is sufficient to supply essential loads during the injection phase of a LOCA. Two pumps are sufficient to supply essential loads during the recirculation phase of an accident. The service water (SW) system piping is arranged so that either pump train can provide flow to each essential load; through a single loop header; nonessential loads are automatically isolated on a safety injection (SI) signal concurrent with an associated 480-V safeguards bus undervoltage condition. Valving is provided to isolate any single active failure and to permit continued operation of the system. The service water (SW) system consists of a single loop header supplied by two separate, 100% capacity, safety related pump trains. The physical design of the service water system is such that one 100% capacity pump from each class 1E electrical bus (buses 17 and 18) is arranged on a common piping header which then supplies the service water (SW) loop header. A service water (SW) train is based on electrical source only.
Motor-operated valves, which isolate nonessential service water (SW) system loads, as well as the system pumps, are operable from the control room. Power for the service water (SW) system pumps is provided by the 480-V safeguards emergency buses which can be supplied by onsite (emergency diesels) or offsite power. One service water (SW) system pump per emergency diesel is automatically started during postaccident diesel load sequencing.

7.4.1.5 Chemical and Volume Control System

The chemical and volume control system is described in Section 9.3.4.

The chemical and volume control system provides borated water from the boric acid storage tanks or from the refueling water storage tank (RWST) through three positive displacement charging pumps to the reactor coolant system. The capacity of one pump (60 gpm) is sufficient to compensate for contraction of the reactor coolant system coolant during normal cooldown. One charging pump alone or with one boric acid transfer pump can provide MODE 5 (Cold Shutdown) boration requirements following reactor shutdown. Borated water for the charging pumps can be controlled locally or from the control room. Power for the charging pumps is supplied via the emergency buses from either onsite or offsite power sources. The charging pumps discharge into a common pulse dampening accumulator. In

the event of a single failure in the common portion of the system, a redundant method of charging and boration exists by means of the high-pressure safety injection system. Any of the three high-pressure safety injection pumps can be lined up from the control room to take suction from the refueling water storage tank (RWST) and to inject borated water into the reactor coolant system via the high-pressure safety injection lines, once reactor coolant system pressure is reduced below 1500 psi.

7.4.1.6 Component Cooling Water System (CCW)

The component cooling water (CCW) system is described in Section 9.2.2.

The component cooling water (CCW) system consists of two pumps, two heat exchangers, a surge tank, and connecting valves and piping. During normal full power operation, one component cooling water pump and one component cooling water heat exchanger can accommodate the heat removal loads. The standby pump and heat exchanger provide 100% backup.
Both pumps and both heat exchangers are utilized to remove the residual and sensible heat during plant shutdown. If one of the pumps or one of the heat exchangers is not operative, the time for cooldown is extended. The component cooling water (CCW) pumps receive power from the redundant 480-V safeguards emergency buses which can be supplied by onsite or offsite power. The component cooling water (CCW) system is normally operated from the control room. The surge tank accommodates expansion, contraction, and in-leakage of water, and ensures a continuous component cooling water (CCW) supply until a leaking cooling line can be isolated. Because the surge tank is normally vented to the atmosphere, a radiation monitor in the component cooling system annunciates in the control room and closes a valve in the vent line in the event that the radiation level reaches a preset level above the normal background.

7.4.1.7 Residual Heat Removal System

The residual heat removal system is described in Section 5.4.5.

The residual heat removal system consists of a single drop line from the reactor coolant system hot leg through two redundant pumps and their associated heat exchangers and back to the reactor coolant system via a single header. Each pump can be manually cross-connected to the alternate heat exchanger for increased reliability. Normal cooldown of the reactor coolant system is accomplished by operating both pumps and heat exchangers; however, a lesser cooldown rate can be achieved with only one pump. With a lake temperature of 80°F or less, one heat exchanger can effect cooldown approximately 30 hr after shutdown. For a maximum lake temperature of 85°F, cooldown to cold shutdown conditions with one residual heat removal (RHR) heat exchanger would exceed 30 hr; however, cold shutdown conditions would still be reached in a reasonable period of time. Each residual heat removal pump is supplied with power from separate redundant 480-V safeguards emergency buses which can receive power from either onsite or offsite sources. The system is normally operated from the control room.

7.4.1.8 Electrical Instrumentation and Power Systems

Table 7.4-2 provides a list of the instruments used to conduct a safe shutdown. The list includes those instruments which provide information to the control room operator from which the proper operation of all safe shutdown systems can be inferred. These instruments show reactor coolant system pressure, reactor coolant system temperature, pressurizer level, and steam-generator level. Improper trending of these parameters would lead the operator to investigate the potential causes. Other instruments listed in the table provide the operator with a direct check on safe shutdown system performance and an indication of actual or impending degradation of system performance.

Offsite emergency power is provided by two independent transmission lines each connected to a separate station auxiliary (startup) transformer. A third (delayed access) source of offsite power can be made available via the unit auxiliary transformer by manually disconnecting flexible connections at the main generator terminals.

Onsite emergency power is furnished by two diesel-engine generating sets. Either diesel generator is capable of supplying sufficient safety loads. The diesel generators and loads are divided on a split-bus arrangement. There is no automatic tie between the two buses. Both diesels are started by a safety injection signal, and each diesel is started by an undervoltage condition at either of its 480-V safeguards buses. Each diesel can also be started locally or from the control room.

Table 7.4-3 lists the safe shutdown systems power source and location.

7.4.2 EVALUATION

In the SEP review of the safe shutdown systems for Ginna Station (Topic VII-3), the NRC staff noted that the systems required to take the reactor from MODE 3 (Hot Shutdown) to MODE 5 (Cold Shutdown) (assuming only offsite power is available or only onsite power is available with a single failure) are capable of initiation to bring the plant to safe shutdown and are in compliance with current licensing criteria and safety objectives. The staff concluded that with the installation of a redundant component cooling water (CCW) surge tank level alarms (See Section 9.2.2.5), Ginna Station satisfies all of the requirements for safe shut-down, including GDC 17 (10 CFR 50, Appendix A), because of the number and quality of systems provided, an 8-hr battery capacity, and the capability to establish a delayed access line by backfeeding through the main transformer in less than 8 hours (*Reference 2*). See Section 8.2.2.2.3 for additional details.

7.4.3 EMERGENCY SHUTDOWN CONTROL

7.4.3.1 General

The control building, equipment, and furnishings have been designed so that the likelihood of fire or other conditions making the main control room inaccessible even for a short time is extremely small.

As a further measure to ensure safety, provisions have been made so that plant operators can shut down and maintain the plant in a safe condition by means of controls located outside the

control room. During such a period of control room inaccessibility, the reactor will be tripped and the plant maintained in the MODE 3 (Hot Shutdown) condition. If the period extends for a long time, the reactor coolant system can be borated to maintain shutdown as xenon decays.

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

The functions for which local control provisions have been made are listed below along with the type of control and location in the plant. Transfer of certain components to local controls is annunciated in the control room.

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

A. Open both reactor trip breakers at the reactor trip switch gear.

B. Open both MG set breakers at Buses 13 and 15.

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

AA. Residual heat removal (Section 7.4.3.2).

BB. Reactivity control, i.e., boron injection to compensate for fission product decay (Section 7.4.3.3).

CC. Pressurizer pressure and level control (Section 7.4.3.4).

DD. Electrical systems as required to supply the above systems (Section 7.4.3.5).

EE. Other equipment, as described in Sections 7.4.3.2 through 7.4.3.7.

7.4.3.2 Residual Heat Removal

Following a normal plant shutdown, an automatic steam dump control system bypasses steam to the condenser and maintains the reactor coolant temperature at its no-load value. This implies the continued operation of the steam dump system, condensate circuit, condenser cooling water, preferred auxiliary feedwater pumps, and steam generator instrumentation. If the automatic steam dump control system is not available, independently controlled relief valves on each steam generator maintain the steam pressure. These relief valves are further backed up by code safety valves on each steam generator. The steam relief facility is adequately protected by redundancy and local protection. For decay heat removal, it is only necessary to maintain the control on one steam generator.

For the continued use of the steam generators for decay heat removal, it is necessary to provide a source of water of approximately 200 gpm, a means of delivering that water, and finally, instrumentation for pressure and level indication.

The normal source of water supply is the secondary feedwater circuit; this implies satisfactory operation of the condenser, air ejectors, condenser cooling circuit, etc. In addition to the normal feedwater circuit, the plant may use, as a backup, water from the condensate storage tanks, lake water via the service water (SW) system, or water provided from the yard fire hydrant loop.

Feedwater may be supplied to the steam generators by the preferred auxiliary feedwater pumps (two electric motor-driven and one steam turbine-driven) or the motor-driven standby auxiliary feedwater pumps (SAFW); these pumps and associated valves have local controls.

7.4.3.3 Reactivity Control

Following a normal plant shutdown to MODE 3 (Hot Shutdown) condition, soluble poison is added to the primary system to maintain subcriticality. For boron addition, the chemical and volume control system is used. Boration requires the use of the following:

A. Charging pumps and volume control tank, with boric acid transfer pumps and tanks, and associated piping; or the charging pumps could draw directly from the refueling water storage tank (RWST).

B. Regenerative heat exchanger, nonregenerative heat exchanger, and associated equipment component cooling and service water (SW) systems; or the steam generators could be used to remove decay heat, using auxiliary feedwater and steam dump.

C. Periodic operation of one main coolant pump, if available, or the auxiliary spray/heaters for pressurizer homogenization is desirable. However, natural circulation is acceptable.

D. Compressed air for valve operation; manual could be adopted if necessary.

With the reactor held at MODE 3 (Hot Shutdown) conditions, boration of the plant is not required immediately after shutdown. The xenon transient does not decay to the equilibrium level until some 10 to 15 hr after shutdown, and a further period would elapse before the 1% reactivity shutdown margin provided by the control rods had been cancelled. This delay would provide ample time for initiating boration.

7.4.3.4 Pressurizer Pressure and Level Control

Following a reactor trip, the primary temperature will automatically reduce to the no-load temperature condition as dictated by the steam generator temperature conditions. This reduction in the primary water temperature reduces the primary water volume and, if continued pressure control is to be maintained, makeup is required. This is supplied by the chemical and volume control system which also provides pressurizer level control in normal circumstances. This requires the charging pump for boration plus a borated water supply such as the normal boron regeneration equipment, the boric acid storage tanks, or the refueling water storage tank (RWST).

7.4.3.5 Electrical Systems

Offsite or onsite emergency power must be available to supply the above systems and equipment for the MODE 3 (Hot Shutdown) condition.

7.4.3.6 Startup of Other Equipment

The average ambient air temperature inside containment is maintained below 125°F. For this reason, the containment air recirculation fan coolers should be continued in operation, if possible.

At least one service water (SW) pump must normally be in operation while the diesel generators are operating. Hose connections have been installed from the fire water system to provide an alternate source of cooling water for the diesel generators that is independent of the service water (SW) system. (See Section 9.5.5.)

7.4.3.7 Indication and Controls Provided Outside the Control Room

The specific indication and controls provided outside the control room for emergency shut-down control are summarized as follows:

7.4.3.7.1 Local Panel Indication

A. The auxiliary feedwater pump panel provides indication of the following:
   - Steam generator wide-range water levels--the median of three wide-range level transmitters is displayed for each steam generator (2).
   - Steam generator pressures (2).
   - Pressurizer pressure.
   - Pressurizer level.

B. The feedwater bypass valve panel provides indication of steam generator wide-range water levels--the median of three wide-range level transmitters is displayed for each steam generator.

C. The charging pump panel provides indication of pressurizer level.

D. Standby auxiliary feedwater flow and pressure is provided in the standby auxiliary feedwater building.

E. The intermediate building emergency local instrument panel (near the turbine-driven auxiliary feedwater [AFW] pump) is a new panel installed in response to a 10 CFR 50 Appendix R review that provides the following indications.
   - Primary temperature-reactor coolant system loop A hot and cold leg.
   - Steam generator 1A wide-range level.
   - Steam generator 1A pressure.
   - Turbine-driven auxiliary feedwater flow.
   - Steam Generator 1B wide-range level.

F. Auxiliary building emergency local instrument panel installed in the charging pump room in response to the Appendix R review to provide for control of the primary coolant inventory. The panel provides the following indications.
   - Primary pressure.

- Pressurizer level.

G. Portable source range drawer to monitor neutron flux.

7.4.3.7.2 Local Motor Controls

Local stop/start pushbutton motor controls with a selector switch are provided at each of the following motors: motor-driven auxiliary feedwater pumps (MDAFW) and boric acid transfer pumps. Local trip/close pushbutton breaker controls with a selector switch are provided for each of the charging pumps. For the charging pumps, the pushbutton trips and closes the associated bus breaker, while local motor control is established at the associated variable frequency drive (VFD). The selector switch will transfer control of the switchgear from the control room to local at the motor. Placing the local selector switch in the local operating position will give an annunciator alarm in the control room and will turn out the motor control position lights on the control room panel.

A local start/stop switch and local/remote selector switch are located on the intermediate building emergency local instrument panel (IBELIP) for local control of the turbine-driven auxiliary feedwater pump turbine dc-lube-oil pump. This panel may be powered by a portable DC diesel generator during a loss of both AC and DC plant power.

Remote stop/start pushbutton motor controls with a selector switch are also provided for each of the containment air recirculation fan motors. These controls are grouped at one point in the intermediate building convenient for operation. The selector switch will transfer control of the switchgear from the control room to the remote point. Placing the selector switch to local operation will give an annunciator alarm in the control room and will turn out the motor control position lights on the control room panel.

Remote stop/start pushbutton motor controls with a selector switch located in the intermediate building were originally provided for each of the service water (SW) pump motors. In 1997, these controls were removed after an evaluation (*Reference 6*) yielded that a high energy line break (HELB) in the intermediate building could fail all dc control power to the service water (SW) pumps due to the existence of these controls and the associated wiring. Since local control for the service water (SW) pump motors was available at the 480 volt buses 17 and 18 located in the screen house, it was determined that the control devices in the intermediate building were not necessary.

7.4.3.7.3 Valve Control

A. Main feed regulators.

B. Auxiliary feed control valves. (These valves are operated locally at the preferred auxiliary feedwater pumps.)

C. Atmospheric dump. (Automatic control normally at MODE 3 (Hot Shutdown).)

D. All other valves requiring operation during MODE 3 (Hot Shutdown) can be locally operated at the valve.

E. Letdown orifices isolation valves operated locally to the charging pumps. Local stop and start buttons with selector switch and position lamp.

7.4.3.7.4 Pressurizer Heater Control

Stop and start buttons with selector switch and position lamp are located near the motor driven auxiliary feedwater pumps (MDAFW) for the backup heater group.

7.4.3.7.5 Lighting

Emergency lighting is provided in all operating areas. Additional lighting has been installed as part of the RG&E historic alternative shutdown effort (see Section 7.4.4) and portable self-contained electric lights are available to the operators to ensure access to and egress from required locations.

7.4.3.7.6 Communications

The communication system provides for communication between local operating stations without the use of the control room. Also, hand-held radios are available for operating personnel communications.

7.4.3.7.7 Electrical Systems

In the event of a main control room evacuation, combined with a loss of offsite power, one diesel generator must be operable. The 1A diesel generator is provided with an emergency local control panel that permits local control of the diesel generator following evacuation of the control complex. The emergency local control panel is equipped with isolation switches, start and stop controls, voltmeter, ammeter, speed indicator, and additional alternative controls. The use of this local control panel is covered by Ginna Station procedures. In addition to this provision, a new breaker has been installed between the 1B diesel generator and 480-V safeguards bus 17 for protection against both diesel generators failing because of a fire-induced circuit failure at buses 17 and 18 in the screen house.

7.4.4 POST-FIRE SAFE SHUTDOWN (SSD) CAPABILITY

7.4.4.1 System Description

The systems required for post-fire safe shutdown are described in the Fire Protection Program Report (*Reference 7*).

REFERENCES FOR SECTION 7.4

1. U.S. Nuclear Regulatory Commission, Branch Technical Position, RSB 5-1, Design Requirements of the Residual Heat Removal System, Revision 1.

2. U.S. Nuclear Regulatory Commission, Safety Evaluation Report Related to the Full-Term Operating License for R. E. Ginna Nuclear Power Plant, NUREG 0944, October 1983.

3. Deleted

4. Deleted

5. Deleted

6. Deleted

7. EPM-FPPR, Ginna Station Fire Protection Program Report, Volumes 1, 2, and 3.

Table 7.4-1
FUNCTIONS FOR SHUTDOWN AND COOLDOWN

Function	Method
Control of reactor power	Boration
	Chemical and volume control system
	High-pressure safety injection
	Control rods
	Controlled rod insertion
	Reactor trip
Core heat removal	Forced circulation (reactor coolant pumps)
	Natural circulation (using steam generators)
	Residual heat removal
	Chemical and volume control system letdown heat exchangers
	Pressurizer safety valves and safety injection
Steam generator heat removal	Main condenser (circulating water system)
	Atmospheric dumps (manual actuation)
	Safety valves
	Auxiliary feed system turbine
	Steam-generator blowdown
	Water-solid steam generator
Feedwater	Main feedwater pumps
	Steam-and motor-driven auxiliary feedwater pumps (TDAFW/ MDAFW)
	Standby auxiliary feedwater (SAFW) pumps
Primary system control	Chemical and volume control system
	Pressurizer safety valves

Table 7.4-2
SAFE SHUTDOWN INSTRUMENTS

Component/System	Instrument	Instrument Location
Main steam	Steam generator level LT-460; LI-460; LT-461; LI-461; LT-470; LI-470; LT-471; LI-471	LT inside containment LI control room[a]
Reactor coolant	Pressurizer level LT-426; LI-426; LT-427; LI-427; LT-428; LI-428; LT-433; LI-433A	LT inside containment LI control room[a]
	Pressurizer pressure PT-449; PI-449; PT-429; PI-429; PT-430; PI-430; PT-431; PI-431	PT inside containment PI control room[a]
	Reactor coolant system temperature TE 409A-1; TI 409A-1 TE 409B-1; TI 409B-1 TE 410A-1 (or TE-410A-2, TE-404A-2, or TE-408A-2); TI 410A-1 TE 410B-1; TI 410B-1	TE inside containment TI control room
Auxiliary feed	Preferred auxiliary feedwater system (AFW) flow FT-2001; FT-2002; FT-2006; FT-2007; FI-2021A; FI-2022A; FI-2023A; FI-2024A	FT intermediate building FI control room[a]
	Standby auxiliary feedwater system (SAFW) flow	FT auxiliary building addition

Component/System	Instrument	Instrument Location
	FT-4084; FT-4085; FI-4084B; FI-4085B	FI control room[a]
Service water	Pump discharge pressure	PT screen house
	PT-2027; FT-2028 PI-2160; PI-2161	PI control room
Chemical and volume control	Charging flow	FIT auxiliary building
	FIT-128; FI-128; FI-128B	FI control room
	Seal injection flow[b]	FIT and FT auxiliary building
	FIT-115; FIT-116; FT-115A; FIT-116A; FI-115A; FI-116A	FI control room
	Refueling water storage tank (RWST) level	LT auxiliary building with indications in the control room
	LT-920; LT-921	
Component cooling water (CCW)	System flow	FIT auxiliary building
	FIT-619	Low flow alarm in control room
	Surge tank level	LIT auxiliary building with alarms in control room
	LIT-618; LAH-618A; LAL-618B	
Residual heat removal	System flow	FT auxiliary building
	FT-626; FI-626; FT-689; FI-689	FI control room

Component/System	Instrument	Instrument Location
Diesel generator	Generator output voltage and current	Control room
Emergency ac power	480-V buses 14, 16, 17, 18, voltage indication	Control room
Emergency dc power	125-V dc buses 1 and 2 voltage indication	Control room

a. Some indicators are also available at local shutdown panels.

b. Seal injection flow indication is not required for safe shutdown. The RCP seal injection flow instrumentation is nonseismic except for the pressure boundary portion, which is Seismic Category I.

Table 7.4-3
SAFE SHUTDOWN SYSTEMS POWER SOURCE AND LOCATION

System	Power Source	Location Building (Elevation)
Reactor protection		
Breakers	dc power	Control room (289 ft)
Bistables	Instrument buses	
Main steam		
Safety valves	---	Intermediate building (278 ft)
Isolation valves	Air (fail closed)	Intermediate building (278 ft)
Atmospheric dump valves	Air, nitrogen bottles, or manual	Intermediate building (278 ft)
Auxiliary feed		
Motor-driven pumps A, B	A bus 14; B bus 16	Intermediate building (253 ft)
Turbine-driven pump	Not applicable	Intermediate building (253 ft)
Standby pumps C, D	C bus 14; D bus 16	Auxiliary building addition (270 ft)
Service water pumps A, B, C, D	A, C bus 18; B, D bus 17	Screen house (253 ft)
Chemical and volume control (charging) pumps A, B, C	A bus 14 B; C bus 16	Auxiliary building (235 ft) east
Refueling water storage tank (RWST)	---	Auxiliary building
Component cooling water		

System	Power Source	Location Building (Elevation)
Pumps A, B	A bus 14; B bus 16	Auxiliary building (271 ft)
Heat exchangers	---	Auxiliary building (271 ft)
Residual heat removal		
Pumps A, B	A bus 14; B bus 16	Auxiliary building (219 ft) residual heat removal pit
Heat exchangers	---	Auxiliary building (235 ft)
Diesel generators 1A, 1B	125-V dc control power	Diesel room north side of turbine building (253 ft)
480 V, bus 14	Diesel 1A or offsite power	Auxiliary building (271 ft)
480 V, bus 16	Diesel 1B or offsite power	Auxiliary building (263 ft)
480 V, bus 17	Diesel 1B or offsite power	Screen house (253 ft)
480 V, bus 18	Diesel 1A or offsite power	Screen house (253 ft)
Instrument buses 1A, 1B, 1C, 1D	1A-inverter 1 and 1B-480-V motor control center 1C-inverter 2 and 1D-480-V motor control center	Control room (289 ft)
Battery and inverter 1A	---	Battery room 1A (253 ft)
Battery and inverter 1B	---	Battery room 1B (253 ft)

Table 7.4-4
Table DELETED

7.5 SAFETY-RELATED DISPLAY INSTRUMENTATION

Process variables required on a continuous basis for the startup, operation, and shutdown of the unit are indicated, recorded, and controlled from the control room. The quantity and types of process instrumentation provided ensure safe and orderly operation of all systems and processes over the full operating range of the plant.

Certain controls that require a minimum of operator attention, or are only in use intermittently, are located on local control panels near the equipment to be controlled. Monitoring of the alarms of such control systems is provided in the main control room.

7.5.1 CONTROL ROOM

7.5.1.1 Description

7.5.1.1.1 General

Alarms and annunciators in the control room provide the operators with a warning of abnormal plant conditions that might lead to damage of components, fuel, or other unsafe conditions. Other displays and recorders are provided for indication of routine plant operating conditions and for the maintenance of records.

7.5.1.1.2 Main Control Board

Consideration is given to the fact that certain systems normally require more attention from the operator. The control system, therefore, is centrally located on the three-section board. Figure 7.5-1 shows the control room layout for the unit. The control board is divided into relative areas to show the location of control components and information display pertaining to various subsystems.

On the center section of the control board is the cathode ray tube (CRT) display for the microprocessor rod position indication system. The microprocessor rod position indication system monitors the position of all rods and causes a rod deviation alarm to be generated by the plant process computer system (PPCS) to alert the operator should an abnormal condition exist for any individual control rod. Displayed in this same area is nuclear instrumentation information required to start up and operate the reactor. Control rods are manipulated from the left section.
Variables associated with operation of the secondary side of Ginna Station are displayed and controlled from the center section of the control board. These variables include steam pressure, feedwater flow, main feedwater and feedwater bypass valve position, steam generator wide and narrow range level, steam flow, motor-and-turbine-driven auxiliary feedwater pump flow, and other signals involved in the plant control system. The center section of the control board also contains provisions for indication and control of the reactor coolant system.

Redundant indication is incorporated in the system design since pressure and temperature variables of the reactor coolant system are used to initiate safety features. Control and display equipment for station auxiliary systems is also located here.

The engineered safety features systems are controlled and monitored from the left section of the control board. Valve-position indicating lights are provided as a means of verifying the proper operation of the control and isolation valves following initiation of the engineered safety features. Control switches located on this panel allow manual operation or test of individual units. Also located on this section are the control switches, indicating lights, and meters for fans and pumps required for emergency conditions.

Controls and indications for all ventilation systems and containment isolation are located on the left section of the control board. A containment isolation and containment ventilation isolation reset panel has been installed near the radiation monitoring rack.

In addition, mounted on the right-hand section of the control board are the auxiliary electrical system controls required for manual switching between the various power sources described in Section 8.2.2.

Postaccident monitoring by use of the existing instrumentation is described in the Plant Procedures. All safety-related valves have position indication on the control board termed "status lights" and, in most cases, the valve position is also indicated by red and green lights over the valve control switch. The status lights are white. Valves that are in the safeguards position cause the corresponding status lights to be bright. Valves in the non-safeguards position cause the corresponding status lights to be dim. The status lights are controlled by the valve control switches.

See Table 6.3-7 for a listing of instrumentation readouts available to the operator in the control room during the recirculation phase of safety injection.

7.5.1.1.3 Other Control Room Displays

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

Computer readout and input handling facilities are located in the control room, facing the main control board. The operator will have close access to these facilities, which will aid in the safe and reliable operation of the plant. The computer is isolated from control circuits, and therefore any computer troubles will not affect control. The computer is only an aid to the operator and is not required for operation of the plant.

Audible alarms will be sounded in appropriate areas throughout the station if high radiation conditions are present at the continuous air monitor.

The auxiliary bench board includes the fire panel section and the control room habitability section. The fire panel section includes controls and indicators for certain components of the fire protection system. The control room habitability section includes certain controls and indicators for the control room HVAC system.

7.5.1.2 Design Review

Rochester Gas and Electric Corporation has conducted a control room design review program in response to NUREG 0737, Supplement 1, which required a detailed control room design review to identify and correct design deficiencies, and NUREG 0700, which provided human engineering guidelines. The program emphasized determination of the adequacy of information available to the operator to effectively mitigate emergency conditions and was also designed to improve controls and displays that were determined not to conform with good human factors practices. The review scope encompassed known future control room design changes (e.g., new plant process computer and safety parameter display systems) as well as the existing design. The NRC evaluated the detailed control room design review (DCRDR) program for Ginna and concluded in the Staff Safety Evaluation Report (*Reference 1*) that the program satisfied all DCRDR requirements of Supplement 1 to NUREG 0737.

7.5.2 SAFETY PARAMETER DISPLAY

The requirements for safety parameter display are contained in Regulatory Guide 1.97, Revision 3, as well as in NUREG 0737, Supplement 1.

Regulatory Guide 1.97, Revision 3, lists the minimum variables that should be available to control room personnel during and following an accident. NUREG 0737 requires that sufficient information be presented in order that emergency operating procedures may be carried out.

The NRC evaluated Rochester Gas and Electric's position relative to the guidance provided in Regulatory Guide 1.97, Revision 3, and concluded in the staff safety evaluation report (*Reference 2*) that Rochester Gas and Electric either conforms to or has provided acceptable justification for deviation from the guidance of Regulatory Guide 1.97. Instrumentation associated with postaccident neutron flux monitoring received separate NRC approval by *Reference 5*. Table 7.5-1 provides a comparison of Ginna Station postaccident instrumentation to Regulatory Guide 1.97, Revision 3, criteria, with the exception of those items removed by subsequent licensing basis changes (*References 6 and 7*).

The selection of NUREG 0737, Supplement 1, Post Accident Monitoring (PAM) Instrumentation parameters, is discussed in a detailed safety analysis and implementation plan submitted to the NRC on November 30, 1984 (*Reference 3*).

See Section 7.7.6 for a discussion of the plant process computer system (PPCS) and safety parameter display system (SPDS). The safety parameter display system (SPDS) meets the requirements of NUREG 0737, Supplement 1, for a Post Accident Monitoring (PAM) Instrumentation (*Reference 4*). The SPDS is integrated in the plant process computer system (PPCS).

REFERENCES FOR SECTION 7.5

1. Letter from A. R. Johnson, NRC, to R. C. Mecredy, RG&E, Subject: Safety Evaluation on the Ginna Detailed Control Room Design Review, dated June 14, 1990.

2. Letter from A. R. Johnson, NRC, to R. C. Mecredy, RG&E, Subject: Emergency Response Capability - Conformance to Regulatory Guide 1.97, Revision 3, dated February 24, 1993.

3. Letter from R. W. Kober, RG&E, to J. A. Zwolinski, NRC, Subject: NUREG 0737, Supplement 1, SPDS Parameter Safety Analysis, dated November 30, 1984.

4. Letter from A. R. Johnson, NRC, to R. C. Mecredy, RG&E, Subject: Response to NRC Generic Letter 89-06 on the Safety Parameter Display System [Post Accident Monitoring (PAM) Instrumentation] for Rochester Gas and Electric Corporation, dated June 29, 1990.

5. Letter from A. R. Johnson, NRC, to R. C. Mecredy, RG&E, Subject: Conformance to Regulatory Guide 1.97, Revision 2, Post-Accident Neutron Flux Monitoring Instrumentation, dated November 27, 1995.

6. Letter from Robert Clark (NRC) to Robert Mecredy (RG&E), R. E. Ginna Nuclear Power Plant-Amendment Re: Elimination of Post Accident Sampling System (TAC No. MB3387), dated January 17, 2002.

7. Letter from Donna Skay (NRC) to Maria Korsnick (Ginna), R. E. Ginna Nuclear Power Plant-Amendment Eliminating Requirements for Hydrogen Recombiners and Hydrogen Monitors using the Consolidated Line Item Improvement Process (TAC No. MC4195), dated May5, 2005.

Table 7.5-1
COMPARISON OF GINNA STATION POSTACCIDENT INSTRUMENTATION TO REGULATORY GUIDE 1.97, REVISION 3, CRITERIA

Table 7.5-1 consists of 13 entries for each variable: a sequential number (#), the variable type (TYPE), the variable description (VARIABLE), category (CAT), range (RANGE), the equipment environmental qualification status (EEQ), seismic qualification status (SEISMIC), the quality assurance program classification of the equipment (QA), the power source for the channel (P.S.), whether or not there is control room indication of the variable (CR IND), whether or not recording is provided via discrete recorders (CHART), or the plant process computer (COMP), and any comments on the variable (COMMENTS). Entries in bold are from Regulatory Guide 1.97, Revision 3. Entries below each bold entry depict Ginna Station configurations. Any entries in parentheses represent proposed configurations not currently installed. Details relating to each superscript are listed at the end of this table.

										RECORDER[a]		
#	TYPE[b]	VARIABLE	CAT.[c]	RANGE	EEQ[d]	SEISMIC[d]	QA[e]	P.S.[f]	C.R. IND.[g]	CHART	COMP	COMMENTS
1	**n.a.**	**Auxiliary Feedwater Flow**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**		
	A	FT-2001 (MDAFW/SGA)	1	0-275 gpm (0-138%)	Mild	Yes	SR	1A	FI-2021A	No	F2021	Two per redundant function provided Also satisfies item #69
		FT-2013 (MDAFW/SGA)	1	0-275 gpm (0-138%)	Mild	Yes	SR	1C	FI-2029	No	F2029	
		FT-2002 (MDAFW/SGB)	1	0-275 gpm (0-138%)	Mild	Yes	SR	1C	FI-2022A	No	F2022	
		FT-2014 (MDAFW/SGB)	1	0-275 gpm (0-138%)	Mild	Yes	SR	1A	FI-2030	No	F2030	
		FT-2006 (TDAFW/SGA)	1	0-500 gpm (0-125%)	Mild	Yes	SR	1C	FI-2023A	No	F2023	
		FT-2007 (TDAFW/SGB)	1	0-500 gpm (0-125%)	Mild	Yes	SR	1A	FI-2024A	No	F2024	
2		**Deleted**										
3	**n.a.**	**Core Exit Thermocouples**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**		
	A	T1-T39	1	0-2300°F	Yes	Yes	SR	1A 1C	CETA CETB	No	Yes	39 CETs are provided. Technical Specifications require a minimum of four operable per quadrant. 19 CETs are associated with the A train and 20 with the B train. Also satisfies items #30, 37
4		**Deleted**										
5		**Deleted**										
6	**n.a.**	**Containment Pressure**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**		
	A	PT-945	1	0-60 psig	Yes	Yes	SR	1A	PI-945	No	P0945	Also satisfies items #35, 41
		PT-946	1	10-200 psia	Yes	Yes	SR	1B	PI-946	No	P0946	
		PT-947	1	0-60 psig	Yes	Yes	SR	1C	PI-947	No	P0947	
		PT-948	1	10-200 psia	Yes	Yes	SR	1C	PI-948	No	P0948	
		PT-949	1	0-60 psig	Yes	Yes	SR	1B	PI-949	No	P0949	
		PT-950	1	10-200 psia	Yes	Yes	SR	MQ-483	PI-950	No	No	

7	**n.a.**	**Condensate Storage Tank (CST) Level**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	
	A	LT-2022A (tank A) LT-2022B (tank B)	1 1	0-24 ft 0-24 ft	Mild Mild	Yes Yes	SR SR	1A 1C	LI-2022A LI-2022B	No No	L2022A L2022B	The transmitters are not located in a Seismic Category I building. The tanks are connected by a locked open 10-in. line.
8	**n.a.**	**Pressurizer Pressure**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	
	A	PT-429 PT-430 PT-431 PT-449	1 1 1 1	1700-2500 psig 1700-2500 psig 1700-2500 psig 1700-2500 psig	Yes Yes Yes Yes	Yes Yes Yes Yes	SR SR SR SR	1A 1B 1C 1D	PI-429 PI-430 PI-431 PI-449	RK-8 RK-8 RK-8 RK-8	P0429 P0430 P0431 P0449	Although channel PT-449 is not powered from a safety-related supply, it is maintained as a Category 1 variable in all other aspects. Its protection signals are failsafe.
9	**n.a.**	**Pressurizer Level**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	
	A	LT-426 LT-427 LT-428	1 1 1	0-100% 0-100% 0-100%	Yes Yes Yes	Yes Yes Yes	SR SR SR	1A 1B 1C	LI-426 LI-427 LI-428	RK-9 RK-9 RK-9	L0426 L0427 L0428	Level instrumentation does not cover the hemispherical top and bottom of the pressurizer. Also satisfies item #60
10		**Deleted**										
11	**n.a.**	**RCS Cold Leg Temperature**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	
	A	TE-409B-1 (Loop A) TE-410B-1 (Loop B)	1 1	0-700°F 0-700°F	Yes Yes	Yes Yes	SR SR	1A 1C	TI-409B-1 TI-410B-1	RK-3 RK-3	T0409B T0410B	Also satisfies item #28
12		**Deleted**										
13	**n.a.**	**RCS Pressure**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	
	A	PT-420 PT-420A	1 1	0-3000 psig 0-3000 psig	Yes Yes	Yes Yes	SR SR	1A 1C	PI-420 PI-420A	No RK-8	P0420 P0420A	Also satisfies items #29,40
14	**n.a.**	**RHR Flow (Low Pressure Injection)**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	
	A	FT-626 FT-689 FT-931A (Loop A)* FT-931B (Loop B)*	1 1 1 1	0-4000 gpm 0-4000 gpm 0-2200 gpm 0-2200 gpm	Yes Yes Yes Yes	Yes Yes Yes Yes	SR SR SR SR	1C 1A 1B 1C	FI-626 FI-689 FI-931A FI-931B	No No No No	F0626 F0689 No No	*FT-931A and FT-931B monitor RHR flow to containment spray and SI pumps suction. Also satisfies items #49, 56

15	**n.a.**	**Reactor Vessel Level Indication System**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	
	A	LT-490A LT-490B	1 1	0-100% 0-100%	Yes Yes	Yes Yes	SR SR	1A 1C	LI-490A LI-490B	No No	L0496A L0496B	RVLIS receives 'correction' inputs from sensor line temperature, RCP status, RHR flow, SI flow, CETs, RCS pressure, and Tcold. Where both channels have common inputs the input signals to each channel are isolated. Also satisfies item #31
16	**n.a.**	**Refueling water storage tank (RWST) Level**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	
	A	LT-920 LT-921	1 1	0-100% 0-100%	Mild Mild	Yes Yes	SR SR	1C* 1A	LI-920 LI-921	No No	L0920 L0921	*Computer indication of this channel also requires power from 1A. Also satisfies item #57
17		**Deleted**										
18	**n.a.**	**Steam Generator Wide Range Level**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**		**Two Per Steam Generator Required for Two Loop Plants**
	A	LT-504 (SG A) LT-505 (SG A) LT-506 (SG B) LT-507 (SG B)	1 1 1 1	0-100% 0-100% 0-100% 0-100%	Yes Yes Yes Yes	Yes Yes Yes Yes	SR SR SR SR	1A 1C 1A 1C	LI-504 LI-505 LI-506 LI-507	RK-12A RK-12C RK-12A RK-12C	L0504 L0505 L0506 L0507	Two per steam generator provided. Also satisfies item #65
19	**n.a.**	**Steam Generator Narrow Range Level**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**		
	A	LT-461 (SG A) LT-462 (SG A) LT-463 (SG A) LT-471 (SG B) LT-472 (SG B) LT-473 (SG B)	1 1 1 1 1 1	0-100% 0-100% 0-100% 0-100% 0-100% 0-100%	Yes Yes Yes Yes Yes Yes	Yes Yes Yes Yes Yes Yes	SR SR SR SR SR SR	1A 1C 1D 1D 1A 1B	LI-461 LI-462 LI-463 LI-471 LI-472 LI-473	Yes* Yes* Yes* Yes* Yes* Yes*	L0461 L0462 L0463 L0471 L0472 L0473	*Median of three channels per generator is recorded on RK-12B. Although channels LT-463 and LT-471 are not powered from a safety-related supply, they are maintained as Category 1 variables in all other aspects. Also satisfies item #65
20	**n.a.**	**Steam Generator Pressure**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**		
	A	PT-468 (SG A) PT-469 (SG A) PT-478 (SG B) PT-479 (SG B) PT-482 (SG A) PT-483 (SG B)	1 1 1 1 1 1	0-1400 psig 0-1400 psig 0-1400 psig 0-1400 psig 0-1400 psig 0-1400 psig	Yes Yes Yes Yes Yes Yes	Yes Yes Yes Yes Yes Yes	SR SR SR SR SR SR	1A 1B 1C MQ-483 1C 1B	PI-468 PI-469 PI-478 PI-479 PI-482A PI-483A	No No No No No No	P0468 P0469 P0478 P0479 P0482 P0483	Also satisfies item #66
21		**Deleted**										

22	**n.a.**	**RCS Subcooling Monitor**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	
	A	TE-409A-1, PT-420 TE-410A-1 (or TE-410A-2, TE-404A-2, or TE-408A-2), PT-420A	1 1	0-100°F subcooled 0-100°F subcooled	Yes Yes	Yes Yes	SR SR	1A 1C	TI-409A TI-410A	No No	*TSUBA *TSUBB	*Ginna EOPs provide the means for determining subcooling based on CETs and RCS pressure. The SPDS/PPCS also calculates subcooling using these variables. Both capabilities exceed the range recommended in RG 1.97, Rev. 3. Also satisfies item #32.
23	**n.a.**	**Containment Sump Wide Range Level**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	
	A	LC-942 (A-E) LC-943 (A-E)	1 1	8, 78, 113, 180, 214 in. 8, 78, 113, 180, 214 in.	Yes Yes	Yes Yes	SR SR	1A 1C	Yes Yes	No No	Yes Yes	Five discrete level switches per channel, 214-in. indication corresponds to approximately 500,000 gal. Also satisfies items #34, 43
24	**B**	**Neutron Flux**	**1**	**1E-6-100% Power**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	
	B	N-31, N-32 (SR) N-35, N-36 (IR) N-41A, B; N-42A, B; N-43A, B; N-44A, B (PR)	3 3 3 3	1E-1 to 1E6 cps (SR) 1E-11 to 1E-3 amps (IR) 0 to 100% power (PR)	No No No No	Yes Yes Yes Yes	SR** SR** SR** SR**	1A/1C 1A/1B 1A/1B 1C/1D	NI-31, 32 NI-35, 36 NI-41, 42 NI-43, 44 (B suffix for MCB ind.)	RK-45 RK-45 RK-45 RK-45	Yes Yes Yes Yes	Neutron flux indication is considered a backup type B indication at Ginna and is therefore considered Category 3. **Protection portions of channels only.
25	**B**	**Control Rod Position**	**3**	**Full In or Not Full In**	**No**	**No**	**Comm.**	**n.p.**	**No**	**No**		
	B	Microprocessor rod position indication system (MRPI)	3	Rod position indicated in 12 step increments, as well as indication of rods full in or not full in	No	No	SS	*	Yes	No	Yes	*The MRPI system is powered from a dedicated transformer from safety-related 480-V MCCK/01MM.
26	**B**	**RCS Boron Concentration**	**3**	**0-6000 ppm**	**No**	**No**	**Comm.**	**n.p.**	**No**	**No**		
	B	AI-6053 [postaccident sampling system (PASS) boron analyzer]	3	50 ± 50 - 6000 ± 300 ppm	No	No	SS	*	No	No	No	*The PASS instrument panel is powered from 480-V bus 13 (non SR) via panel SB14. NRC SER dated 4/14/86, deferred the range and accuracy capabilities of postaccident sampling systems to NUREG-0737, item II.B.3. The Ginna PASS meets these criteria.
27	**B**	**RCS Hot Leg Water Temperature**	**1**	**50-700°F**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	
	B	TE-409A-1 (Loop A) TE-410A-1 (or TE-410A-2, TE-404A-2, or TE-408A-2) (Loop B)	1 1	0-700°F 0-700°F	Yes Yes	Yes Yes	SR SR	1A 1C	TI-409A-1 TI-410A-1	No No	T0409A T0410A	

28	**B**	**RCS Cold Leg Water Temperature**	**1**	**50-700°F**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**		
	A	*	*	*	*	*	*	*	*	*	*	*See item #11, RG&E type A variable
29	**B**	**RCS Pressure**	**1**	**0-3000 psig**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**		
	A	*	*	*	*	*	*	*	*	*	*	*See item #13, RG&E type A variable.
30	**B**	**Core Exit Temperature**	**3**	**200-2300°F**	**No**	**No**	**Comm.**	**n.p.**	**No**	**No**		
	A	*	*	*	*	*	*	*	*	*	*	*See item #3, RG&E type A variable.
31	**B**	**Coolant Inventory**	**1**	**Hot Leg Bot.-Flange**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**		
	A	*	*	*	*	*	*	*	*	*	*	*See item #15, RG&E type A variable.
32	**B**	**RCS Degrees of Subcooling**	**2**	**200°Fsub -35°Fsuper**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**		
	A	*	*	*	*	*	*	*	*	*	*	*See item #22, RG&E type A variable.
33	**B**	**Containment Sump Level Narrow Range**	**2**	**Plant Specific**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**		
	C	LT-2039 (Sump A) LT-2044 (Sump A)	3 3	0-30 ft 0-30 ft	No No	No No	SS SS	1A 1A	LI-2039 LI-2044	No No	L2039 L2044	NRC SER dated 12/4/90, found the instrumentation provided to be acceptable. Also satisfies item #42
34	**B**	**Containment Sump Level Wide Range**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**		
	A	*	*	*	*	*	*	*	*	*	*	*See item #23, RG&E type A variable.
35	**B**	**Containment Pressure**	**1**	**-5 psig to Design**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**		
	A	*	*	*	*	*	*	*	*	*	*	*See item #6, RG&E type A variable. Note: The Ginna containment pressure indication covers a range of 10 psia to 300% design pressure.

36	**B**	**Containment Isolation Valve Position**	**1**	**Closed/Not Closed**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	**One per redundant function reqd. Check valve position ind. is not reqd.**
	B	See UFSAR Table 6.2-29 for list of containment isolation valves.	3	Open/closed	No	Yes	SS	ADC, BDC	Yes	No / Yes	Isolation valves outside containment go closed prior to being exposed to a harsh environment and therefore environmental qualification is not required. RG&E has taken exception to the need to qualify indication for valves inside containment. Ref. letter RG&E-NRC 5/6/91.
37	**C**	**Core Exit Temperature**	**1**	**200-2300°F**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	
	A	*	*	*	*	*	*	*	*	* / *	*See item #3, RG&E type A variable.
38	**C**	**RCS Radiation Level**	**1**	**0.5 - 100X Tech Spec**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	
	n.a.	Postaccident sampling system (PASS), manual radiation isotopic spectroscopy after sample taken	3	0.01 mR-1.0E04 R/hr	n.a.	n.a.	SS	n.a.	No	No / No	NRC SER dated 4/14/86, found the instrumentation provided to be acceptable. See note at end of table.
39	**C**	**Gamma Analysis of Primary Coolant**	**3**	**1.0E-5-10 Ci/ml**	**No**	**No**	**Comm.**	**N.P.**	**No**	**No**	
	C	Postaccident sampling system (PASS), manual radiation isotopic spectroscopy after sample taken	3	1.0E-5-10 Ci/ml. Range can be extended by dilution techniques.	n.a.	n.a.	SS	n.a.	No	No / No	NRC SER dated 4/14/86, found the instrumentation provided to be acceptable.
40	**C**	**RCS Pressure**	**1**	**0-3000 psig**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	
	A	*	*	*	*	*	*	*	*	* / *	*See item #13, RG&E type A variable.
41	**C**	**Containment Pressure**	**1**	**-5 psig to design**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	
	A	*	*	*	*	*	*	*	*	* / *	*See item #6, RG&E type A variable. Note: The Ginna containment pressure indication covers a range of 10 psia to 300% design pressure.
42	**C**	**Containment Sump Level Narrow Range**	**2**	**Top to Bottom**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	C	*	*	*	*	*	*	*	*	* / *	*See item #33, RG&E type C variable. NRC SER dated 12/4/90, found the instrumentation provided to be acceptable.

43	**C**	**Containment Sump Level Wide Range**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	
	A	*	*	*	*	*	*	*	*	*	*See item #23, RG&E type A variable.
44	**C**	**Containment Area Radiation**	**3**	**1 to 1.0E4 R/hr**	**No**	**No**	**Comm.**	**n.p.**	**No**	**No**	
	E	R-2	3	0.01-1.0E5 R/hr	No	Yes	SS	1B	Yes	RK-77 R02	NRC SER dated 4/14/86 found the instrumentation provided to be acceptable.
45	**C**	**Condenser Air Exhaust Noble Gas Radioactivity**	**2**	**1E-6 to 1E5 μCi/cm^3**	**Yes**	**No**	**Part.**	**Rel.**	**No**	**No**	
	E	R-15	2	1E-6 to 1E-3 μCi/cm^3	Mild	No	SS	1D	Yes	RK-79 R15	
	C	R-47	3	3.5 E-7 to 5.3 E-2 μCi/cm^3	Mild	No	SS	TSC	No	No R47	
	E	R-48	2	1.3 E-2 to 1.0 E5μCi/cm^3	Mild	No	SS	TSC	No	No R48	
46		**Deleted**									
47	**C**	**Containment Effluent Noble Gas at Release**	**2**	**1E-6 to 1E-2 μCi/cm^3**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	C	R-12 (cont. purge vent) R-14 (plant exhaust vent) R-31 (SG steam line A) R-32 (SG steam line B)	2 2 2 2	1E-6 to 1E-2 μCi/cm^3 1E-6 to 1E-1 μCi/cm^3 1E-1 to 1E3 μCi/cm^3 1E-1 to 1E3 μCi/cm^3	Mild Mild Mild Mild	No No No No	SR SS SS SS	1A 1A * *	Yes Yes Yes Yes	RK-78 Yes RK-78 Yes No Yes No Yes	*SPING monitors are powered via a dedicated transformer from MCC D (safety related). SPING monitors R-12A (cont. purge vent) and R-14A (plant exhaust vent) are also available to monitor noble gas releases as well as particulates and iodine.
48	**C**	**Containment Effluent Noble Gas at Pen. etc.**	**2**	**1E-6 to 1E-2 μCi/cm^3**	**Yes**	**No**	**SS**	**Rel.**	**No**	**No**	
	C	*	*	*	*	*	*	*	*	*	*See item #47. These monitors are considered to provide adequate monitoring of all credible releases.
49	**D**	**RHR System Flow**	**2**	**0-110% Design**	**Yes**	**No**	**Partial**	**Ref.**	**No**	**No**	
	A	*	*	*	*	*	*	*	*	*	*See item #14, RG&E type A variable.

50	**D**	**RHR Heat Exchanger Outlet Temperature**	**2**	**40-350°F**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	n.a.	TE-627	3	50-400°F	No	No	SS	*	No	No	T0627	NRC SER dated 12/4/90 found the range provided acceptable. *Power to temperature loop from AC Dist. Panel CD03C/02
51	**D**	**Accumulator Tank Level**	**2**	**10-90%**	**Yes**	**No**	**Partial**	**n.p.**	**No**	**No**	
	n.a.	LT-934 (loop A) LT-935 (loop A) LT-938 (loop B) LT-939 (loop B)	3 3 3 3	±7 in. from nominal ±7 in. from nominal ±7 in. from nominal ±7 in. from nominal	No No No No	No No No No	SS SS SS SS	1C 1B 1C 1B	LI-934 LI-935 LI-938 LI-939	No No No No	No No No No	NRC SER dated 12/4/90 found the instrumentation provided acceptable. The Category 3 designation is consistent with RG&E's category determination philosophy.
52	**D**	**Accumulator Tank Pressure**	**2**	**0-750 psig**	**Yes**	**No**	**Partial**	**n.p**	**No**	**No**	
	n.a.	PT-936 (loop A) PT-937 (loop A) PT-940 (loop B) PT-941 (loop B)	3 3 3 3	0-800 psig 0-800 psig 0-800 psig 0-800 psig	No No No No	No No No No	SS SS SS SS	1C 1B 1C 1B	PI-936 PI-937 PI-940 PI-941	No No No No	No No No No	NRC SER dated 12/4/90 deferred resolution of these deviations to generic staff review of this issue. The Category 3 designation is consistent with RG&E's category determination philosophy.
53	**D**	**Accumulator Isolation Valve Position**	**2**	**Open/Closed**	**Yes**	**No**	**Partial**	**n.p.**	**No**	**No**	
	n.a.	MOV-841 (loop A) MOV-865 (loop B)	3 3	Open/closed Open/closed	No No	Yes Yes	SS SS	ADC BDC	Yes Yes	No No	No No	Valves are locked open and deenergized. NRC SER dated 12/4/90 found the instrumentation provided acceptable.
54	**D**	**Boric Acid Charging Flow**	**2**	**0-110% Design**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	n.a.	FT-128	2	0-75 gpm	Mild	No	SS	1D	FI-128B	No	F0128	NRC SER dated 4/14/86 found the instrumentation provided acceptable.
55	**D**	**High Pressure Injection (SI) Flow**	**2**	**0-110% design**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	D	FT-924 (SIP B) FT-925 (SIP A)	2 2	0-600 gpm 0600 gpm	Yes Yes	Yes Yes	SR SR	1A 1C	FI-924 FI-925	No No	F0924A F0925A	
56	**D**	**Low Pressure Injection (RHR) Flow**	**2**	**0-110% Design**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	A	*	*	*	*	*	*	*	*	*	*	*See item #14, RG&E type A variable.
57	**D**	**RWST Level**	**2**	**Top to Bottom**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	A	*	*	*	*	*	*	*	*	*	*	*See item #16, RG&E type A variable.

58	**D**	**RCP Status**	**3**	**Motor Current**	**No**	**No**	**Comm.**	**n.p.**	**No**	**No**	
	D	4.16-kV bus ammeters and RCP breaker status lights	3	0-1200A	No	No	SS	n.a.	Yes	No Yes	
59	**D**	**Pressurizer PORVs and Safeties Position**	**2**	**Closed/Not Closed**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	D	ZS-430 (PORV) ZS-431C (PORV) TE-438 (discharge temperature) ZT-434 (safety valve) ZT-435 (safety valve) TE-436, TE-437 (dis temp)	2 2 3* 2 2 3*	Open/close Open/close 0-300°F Open-close (in.) Open-close (in.) 0-400°F	Yes Yes No Yes Yes No	Yes Yes Yes Yes Yes Yes	SR SR SS SS SS SS	BDC BDC 1A 1A 1A 1A	Yes Yes TI-438 Yes Yes Yes, Yes	No V0430 No V0431 No No No No No No No No	*The RTDs downstream of these valves, TE-438 (PORVs) and TE-436 and TE-437 (safeties), are available in the control room and are considered backup indication of valve position.
60	**D**	**Pressurizer Level**	**1**	**Top to Bottom**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	
	A	*	*	*	*	*	*	*	*	* *	*See item #9, RG&E type A variable. Note: level indication does not cover the hemispherical top and bottom portions of the pressurizer.
61	**D**	**Pressurizer Heaters Status**	**2**	**Electric Current**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	D	Control bank breaker status lights Backup bank breaker status lights 480-V bus voltage and kW demand	2 2 2	Closed/auto/on Closed/auto/on 0-1500 kW	Mild Mild Mild	No No No	SS SS SS	ADC BDC n.a.	Yes Yes Yes	No No No No No Yes	NRC SER dated 12/4/90 found the instrumentation provided acceptable.
62	**D**	**Pressurizer Relief (Quench) Tank Level**	**3**	**Top to Bottom**	**No**	**No**	**Comm.**	**n.p.**	**No**	**No**	
	D	LT-442	3	0-100%	No	No	SS	1B	LI-442	No L0442	
63	**D**	**Pressurizer Relief (Quench) Tank Tamp.**	**3**	**50°F-750°F**	**No**	**No**	**Comm.**	**n.p.**	**No**	**No**	
	D	TE-439	3	(50-400°F)	No	No	SS	1A	TI-439	No T0439	NRC SER dated 12/4/90 found the instrument range acceptable.
64	**D**	**Pressurizer Relief (Quench) Tank Pressure**	**3**	**0 psig to design**	**No**	**No**	**Comm.**	**n.p.**	**No**	**No**	
	D	PT-440	3	0-150 psig	No	No	SS	1B	PI-440A PI-440B	No P0440	Rupture disk setpoint is 100 psig.
65	**D**	**Steam Generator Wide Range Level**	**1**	**Tubesheet - Separators**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**	**Two per generator required for two loop plants**
	A	*	*	*	*	*	*	*	*	* *	*See item #18, RG&E type A variable.
66	**D**	**Steam Generator Pressure**	**2**	**Atm. - 20% > Safety**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	A	*	*	*	*	*	*	*	*	* *	*See item #20, RG&E type A variable.

67	**D**	**Main Steam Flow (or SG Safety Valve Pos.)**	**2**	**0-110% Design**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	D	FT-464 (SG A) FT-465 (SG A) FT-474 (SG B) FT-475 (SG B) FT-498 (SG A) FT-499 (SG B)	2 2 2 2 3 3	0-4.6E6 pph 0-4.6E6 pph 0-4.6E6 pph 0-4.6E6 pph 0-4.6E6 pph 0-4.6E6 pph	Yes Yes Yes Yes No No	Yes Yes Yes Yes Yes Yes	SR SR SR SR SS SS	1A 1B 1C 1D 1C/TSC* 1C/TSC*	FI-464 FI-465 FI-474 FI-475 FI-498 FI-499	Yes** Yes** Yes** Yes** Yes** Yes**	F0464 F0465 F0474 F0475 F0498 F0499	*Denotes auctioneered power supply from the advanced digital feedwater control system (ADFCS). Power for the system is auctioneered from bus 1C and the TSC Inverter. **Median of three channels per SG is recorded RK-11(SGA), RK-13(SGB).
68	**D**	**Main Feedwater Flow**	**3**	**0-110% Design**	**No**	**No**	**Comm.**	**N.P.**	**No**	**No**	
	D	FT-466 (SG A) FT-467 (SG A) FT-476 (SG B) FT-477 (SG B) FT-500 (SG A) FT-503 (SG B)	3 3 3 3 3 3	0-4.6E6 pph 0-4.6E6 pph 0-4.6E6 pph 0-4.6E6 pph 0-4.6E6 pph 0-4.6E6 pph	No No No No No No	No No No No No No	SS SS SS SS SS SS	1C/TSC** 1C/TSC** 1C/TSC** 1C/TSC** 1C/TSC** 1C/TSC**	FI-466 FI-467 FI-476 FI-477 FI-500 FI-503	Yes* Yes* Yes* Yes* Yes* Yes*	F0466 F0467 F0476 F0477 F0500 F0503	*Recorders RK-11 (SGA) and RK-13 (SGB) record median flow of the three channels. **Main feedwater flow transmitters receive power from the digital feedwater control system (ADFCS). Power for the system is auctioneered from bus 1C and the TSC Inverter.
69	**D**	**Auxiliary Feedwater Flow**	**2**	**0-110% Design**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	A D D	* FT-4084 (Standby**) FT-4085 (Standby**)	* 2 2	* 0-300 gpm (0-128%) 0-300 gpm (0-128%)	* Mild Mild	* Yes Yes	* SR SR	* 1A 1C	* FI-4084B FI-4085B	* No No	* F4084 F4085	***See item #1, RG&E type A variable.** ****Ginna Station has a manual standby auxiliary feedwater system, (SAFW) which duplicates the capacity of the motor-driven Preferred auxiliary feedwater** system (AFW).
70	**D**	**Condensate Storage Tank (CST) Level**	**1**	**Plant Specific**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**		
	A	*	*	*	*	*	*	*	*	*	*	*See item #7, RG&E type A variable.
71	**D**	**Containment Spray Flow**	**2**	**0-110% Design**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**		
	n.a.	None	*	*	*	*	*	*	*	*	*	*Indirect indication of containment spray flow is available using SI flow and RHR flow. NRC SER dated 12/4/90 found this acceptable.

72	**D**	**Containment Fan Heat Removal**	**2**	**Plant Specific**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	n.a.	None	*	*	*	*	*	*	*	*	*Indirect indication of containment fan heat removal is available using containment air temperature, sump temperature, and containment pressure. NRC SER dated 12/4/90 found this acceptable.
73	**D**	**Containment Air Temperature**	**2**	**40-400°F**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	D	TE-6031 (elev. 245 ft 0 in.) TE-6035 (elev. 261 ft 9 in.) TE-6036 (elev. 261 ft 9 in.) TE-6037 (elev. 261 ft 9 in.) TE-6038 (elev. 261 ft 9 in.) TE-6045 (elev. 286 ft 4 in.)	2 2 2 2 2 2	0-300°F 0-300°F 0-300°F 0-300°F 0-300°F 0-300°F	Yes Yes Yes Yes Yes Yes	(Yes) (Yes) (Yes) (Yes) (Yes) (Yes)	SS SS SS SS SS SS	* * * * * *	No No No No No No	No No No No No No	Yes Yes Yes Yes Yes Yes	NRC SER dated 12/4/90 found the range deviation to be acceptable. *1E supply from MCC 1D (B train)
74	**D**	**Containment Sump Temperature**	**2**	**50-250°F**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	n.a.	TE-490 A/B (sump A) TE-491 A/B (≈4.3 ft above basement floor)	2 2	0-360°F 0-360°F	Yes Yes	Yes Yes	SR SR	1A/1C 1A/1C	No No	No No	Yes Yes	TE-490A/B and TE-491A/B are dual element RTDs. The 'A' elements are powered from bus 1A and the 'B' elements are powered from bus 1C. Each element is available on the PPCS as a separate point.
75	**D**	**Reactor Water Makeup Flow (CVCS)**	**2**	**0-110% Design**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	n.a.	FT-111	2	5-75 gpm (0-100%)	Mild	No	SS	1A	No	RK-10	No	NRC SER dated 12/4/90 found the instrument range acceptable.
76	**D**	**Letdown Flow (CVCS)**	**2**	**0-110% Design**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	n.a.	FT-134	2	0-100 gpm (0-167%)	Mild	No	SS	1D	FI-134	No	F0134	
77	**D**	**Volume Control Tank Level**	**2**	**Top to Bottom**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	n.a.	LT-112	2	0-100%	Mild	No	SS	1B	LI-112	No	L0112	
78	**D**	**CCW Temperature to ESF System**	**2**	**40-200°F**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	n.a.	TE-621 (component cooling water (CCW) heat exchanger temperature)	2	0-225°F	Mild	No	SS	1B	TI-621	No	T0621	NRC SER dated 12/4/90 found the instrumentation provided to be acceptable.

79	**D**	**CCW Flow to ESF System**	**2**	**0-110% Design**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	n.a.	FT-619 (component cooling water (CCW) system flow)	2	0-7000 gpm	Mild	No	SS	1C	No	No F0619	The CCW system is prealigned with flows to various ESF components manually adjusted using local flow indicating switches. RG 1.97 states that the purpose of this variable is to monitor operation. The instrumentation provided meets this intent.
80	**D**	**Hi Level Radioactive Liquid Tank Level**	**3**	**Top to Bottom**	**No**	**No**	**Comm.**	**n.p.**	**No**	**No**	
	D	LT-1001 (waste holdup tank) LT-1003 (reactor coolant drain tank)	3 3	≈0-100% ≈0-100%	No No	No No	SS SS	** *	No No	No No No L1003	Indication of both tank levels are available at the radwaste panel *Normally fed from 480-V safeguards bus 14 (train A) with a manual backup to 480-V safeguards bus 16 (train B) ** Pneumatic
81	**D**	**Radioactive Gas Holdup Tank pressure**	**3**	**0-150% Design**	**No**	**No**	**Comm.**	**n.p.**	**No**	**No**	
	n.a.	PT-1036 (Tank 1) PT-1037 (Tank 2) PT-1038 (Tank 3) PT-1039 (Tank 4)	3 3 3 3	0-150 psig (0-100%) 0-150 psig (0-100%) 0-150 psig (0-100%) 0-150 psig (0-100%)	No No No No	No No No No	SS SS SS SS	** ** ** **	No No No No	No No No No No No No No	Design of each tank and its safety valve setpoint is 150 psig. Normal radgas pump operating pressure is <100 psig. NRC SER dated 12/4/90 found this range deviation acceptable. ** Pneumatic
82	**D**	**Emergency Ventilation Damper Position**	**2**	**Open/Closed**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	D	7970 (mini-purge) 7971 (mini-purge) 7445 (mini-purge) 7478 (mini-purge)	3 3 3 3	Open/closed Open/closed Open/closed Open/closed	No No No No	Yes Yes Yes Yes	SS SS SS SS	ADC ADC ADC ADC	Yes Yes Yes Yes	No No No No No No No No	Mini-purge valves are locked closed and only opened for containment pressure control. These valves are in their safety-related position prior to any adverse conditions and do not change position throughout any accident. Therefore EQ is not deemed necessary.
83	**D**	**Standby Power/Energy Imp. to Safety Status**	**2**	**Plant Specific**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**	
	D	EDG A, B: V, 1W, A 125-V dc A, B, V, A PT-2023 (instrument air) PT-455 (PORV, SI acc) PT-456 (PORV, SI acc)	3 3 3 2 2	0-500 V, 0-3000 A, 0-2 MW 0-150 V, 0-50 A 0-160 psig 0-1000 psig 0-1000 psig	Mild Mild Mild Mild Mild	No No No No No	SS SS NS SS SS	n.a n.a 1C 1B 1A	Yes Yes PI-2086 PI-455 PI-456	No Yes No Yes No No No No No No	

84	**E**	**Containment High Radiation Monitor**	**1**	**1-1E7 R/hr**	**Yes**	**Yes**	**Full**	**1E**	**Yes**	**Plant Specific**		
	E	R-29 R-30	1 1	1 R/hr-1E7 R/hr 1 R/hr-1E7 R/hr	Yes Yes	Yes Yes	SR SR	1A 1C	RM-29 RM-30	RK-78 RK-79	R-29 R-30	
85	**E**	**Radiation Exposure Rate-Access Required Areas**	**3**	**1E-1-1E4 R/hr**	**No**	**No**	**Comm.**	**n.p.**	**No**	**No**		
	D	Various microprocessor based monitors located and qualified to satisfy NUREG 0654	3	0.1-1E7 mR/hr	No	No	SS	Various	Yes	Yes	Yes	
86	**D**	**Airborne Radiation Release Noble Gas and Flow**	**2**	**1E-6-1E5 µCi/cm^3**	**Yes**	**No**	**Partial**	**Rel.**	**No**	**No**		
	C	*	*	*	*	*	*	*	*	*	*	*See item #47, RG&E type C variable
87	**E**	**Airborne Radiation Release Particulate and Halogens**	**3**	**1E3-1E2 µCi/cm^3**	**No**	**No**	**Comm.**	**n.p.**	**No**	**No**		
	E	RM-12A (containment vent) RM-14A (plant exhaust vent)	3 3	1E-5-10 µCi/cm^3 halogens, 1E-6-1 µCi/cm^3 particulate 5E-5-50 µCi/cm^3 halogens, 2.5E-5-25 µCi/cm^3 part.	No No	No No	SS SS	* *	Yes Yes	No No	R-12A R-14A	*SPING radiation monitors are powered from a dedicated supply from MCC D (safety related).
88	**E**	**Airborne Radioactivity and Part. (Portable Samplers)**	**3**	**1E-9-1E-3 µCi/cm^3**	**No**	**No**	**Comm.**	**n.p.**	**No**	**No**		
	E	Various fixed and portable samplers	3	1E-12-1E-3 µCi/cm^3 (Aliquot or diluted sample)	No	No	SS	n.a.	No	No	No	
89	**E**	**Plant and Environ. Radiation (Portable)**	**3**	**1E-3-1E4 R(rad)/hr**	**No**	**No**	**Comm.**	**n.p.**	**No**	**No**		**Beta Radiations and Photons**
	E	Various portable instrumentation	3	1E-6-1E3 R/hr gamma 1E-3-1E3 R/hr beta	No	No	SS	n.a.	No	No	No	
90	**E**	**Plant and Environ. Radioactivity (Portable)**	**3**	**Isotopic Analysis**	**No**	**No**	**Comm.**	**n.p.**	**No**	**No**		
	E	Multichannel gamma ray spectrometer	3	1E-8-10 µCi	No	No	SS	n.a.	No	No	No	
91	**E**	**Wind Direction**	**3**	**0-360°**	**No**	**No**	**Comm.**	**n.p.**	**No**	**No**		
	E	Wind direction at 33 ft Wind direction at 150 ft Wind direction at 250 ft (elevations at met tower)	3 3 3	0-360° 0-360° 0-360°	No No No	No No No	SS SS SS	* * *	No No No	RK-32 No No	WD033 WD150 WD250	*The weather tower currently receives power directly via an offsite supply.

92	**E**	**Wind Speed**	**3**	**0-50 mph**	**No**	**No**	**Comm.**	**n.p.**	**No**	**No**		
	E	Wind speed at 33 ft Wind speed at 150 ft Wind speed at 250 ft (elevations at met tower)	3 3 3	0-50 mph 0-100 mph 0-100 mph	No No No	No No No	SS SS SS	* * *	No No No	RK-32 No No	WS033 WS150 WS250	*The weather tower currently receives power directly via an offsite supply.
93	**E**	**Estimation of Atmospheric Stab.**	**3**	**Based on Vert. ΔT**	**No**	**No**	**Comm.**	**n.p.**	**No**	**No**		
	E	RTDs at 33, 150, 250 ft elevations (met tower)	3	-8-20°F between each elevation	No	No	SS	*	Yes**	No	WDT1 WDT2	*The weather tower currently receives power directly via an offsite supply. **Temperatures at each elevation are displayed in the control room.
94		**Deleted**										
95		**Deleted**										

a. Recorder

Chart

Yes — A control room recorder is provided. The equipment identification number is provided if appropriate.

No — No recorder is provided.

Comp

Yes — The variable is available on the plant process computer. (The point identification is given if appropriate).

No — The instrument does not input to the computer.

b. Classification

Postaccident instrumentation at Ginna Station is classified according to the following criteria:

Type A: Indication required by the operator during performance of an emergency operating procedure (EOP), in response to a design basis accident, to determine if manual actions are required in order to accomplish required safety functions for which no automatic action is provided.

Type B: Indication used by the operator during performance of an emergency operating procedure (EOP), in response to a design basis accident, to verify that required automatic or manual safety functions have been accomplished.

Type C: Indication used by the operator during performance of an emergency operating procedure (EOP), in response to a design basis accident, to determine if any of the barriers to fission product release have been or may be breached.

Type D: Indication used by the operator during performance of an emergency operating procedure (EOP), in response to a design basis accident, to determine that a safety system or system important to safety has actuated.

Type E: Indication used by the operator to determine the magnitude of a radioactive release and to continually assess the release.

n.a. is entered for variables that although listed in Regulatory Guide 1.97, Revision 3, are not considered postaccident variables at Ginna Station.

c. Categorization

Category 1: Type A variables and key (primary) types B and C variables make up Category 1.

Category 2: Key (primary) types D and E variables make up Category 2.

Category 3: Backup types B, C, D, and E variables make up Category 3.

If the channel is not considered postaccident instrumentation at Ginna Station (n.a. under TYPE) then this entry represents the current level of qualification of the channel.

d. Equipment Qualification

Environment: Those portions of Category 1 or 2 postaccident instrumentation channels located in harsh environments are qualified for their design basis accident environments in accordance with the Ginna Station 10 CFR 50.49 Environmental Qualification Program. Design basis accident environments are specified in Table 3.11-1. Those portions of postaccident instrumentation channels located in mild environments do not require environmental qualification.

- Yes — Signifies environmental qualification in accordance with the Ginna Station 10 CFR 50.49 compliance program (Section 3.11) is provided.
- No — Signifies environmental qualification is not provided.
- Mild — Signifies the primary device is located in a mild environment during its postaccident function and therefore environmental qualification is not provided.
- (Yes) — Signifies environmental qualification in accordance with the Ginna Station 10 CFR 50.49 compliance program is planned but not yet complete.

Seismic: Category 1 postaccident instrumentation is seismically qualified in accordance with the Ginna Seismic Qualification Program (Section 3.10) with the following clarifications:

1. Seismic qualification for analog indicators was generally not provided for those indicators in place before 1983 regardless of category. Only those portions of the channel that performed a safety function (i.e., RPS or ESF actuation) were qualified.
2. Seismic qualification is not considered necessary for recorders unless they provide the sole indication for a Category 1 variable.
3. Seismic qualification for inputs to the plant process computer is provided only up to the isolating device feeding the computer input. The SAS/PPCS is not seismically qualified.
4. Only the mounting of status light housings is considered seismically qualified. Light bulbs are considered "commercially rugged" and can be reasonably expected to survive an earthquake.

- Yes — Signifies seismic qualification in accordance with the Ginna Seismic Qualification Program is provided. Seismic qualification at Ginna is currently being resolved under USI-46.
- No — Signifies seismic qualification is not provided.
- (Yes) — Signifies seismic qualification is proposed but not yet provided.

Seismic qualification only applies to the primary variable indication and those portions of the instrument loop necessary for this indication to function. Recorders are not seismically qualified unless they are the primary indicator. The plant process computer is not seismically qualified.

e. Quality Assurance

Regulatory Guide 1.97 Quality Assurance Category

full — Quality assurance in accordance with Regulatory Guides 1.28, 1.30, 1.38, 1.58, 1.64, 1.74, 1.88, 1.123, 1.144, and 1.146 is recommended.

partial — Quality assurance commensurate with the importance to safety of the instrument should be provided.

comm — Quality assurance through high quality commercial practices should be provided.

Ginna maintains an approved 10 CFR 50 Appendix B Quality Assurance Program which is based on the ANSI/ANS 51.1 Standard. Three quality categories exist:

1. Safety-related class (SR)
2. Safety-significant class (SS)
3. Non-safety class (NS)

The safety-related class (SR) provides for full program control and is considered suitable for any category of postaccident instrumentation. The safety-significant class (SS) provides augmented quality control based on the importance to safety of the device or activity and is considered suitable for Categories 2 or 3 variables, and certain portions of Category 1 channels (recorders, secondary indicators). The non-safety class (NS) provides normal commercial-grade quality control which may be suitable for some Category 3 variables.

Procurement of postaccident instrumentation equipment currently installed was in accordance with the Quality Assurance Program in effect at the time of the procurement for the classification of the equipment at that time. Future procurement, maintenance, calibration, and design controls will be in accordance with the program as described above.

f. Power Supply

Regulatory Guide 1.97

1E — Power provided in accordance with Regulatory Guide 1.32 with battery backup if momentary loss cannot be tolerated should be provided.

rel — A high reliability power source with battery backup if momentary loss cannot be tolerated should be provided.

n.p. — No provision made in Regulatory Guide 1.97, Revision 3.

Ginna Station

1A — A safety-related power supply (1E) provided from instrument bus 1A. Safety-related battery A supply precludes momentary loss of power.

1B — A safety-related power supply (1E) provided from instrument bus 1B. No battery backup is provided. Emergency onsite power is provided by emergency diesel generator A.

1C — A safety-related power supply (1E) provided from instrument bus 1C. Safety-related battery B supply precludes momentary loss of power.

MQ-483 — A safety-related power supply from inverter MQ-483. Safety-related battery A supply precludes momentary loss of power.

1D — A non-safety-related power supply from instrument bus 1D. No battery backup is provided nor emergency onsite source.

TSC — A highly reliable onsite power source with battery backup to preclude momentary loss of power.

ADC — Safety-related battery bus A.

BDC — Safety-related battery bus B.

g. Control Room Indication

Yes — Control room indication separate from a recorder is provided.

No — Control room indicator (other than plant process computer or recorder) is not provided.

Note: the equipment identification number is provided if appropriate.

7.6 OTHER INSTRUMENTATION SYSTEMS REQUIRED FOR SAFETY

7.6.1 OVERPRESSURE PROTECTION DURING LOW POWER OPERATION

The actuation circuitry of the pressurizer power operated relief valves (PORVs) has been modified to provide a low-pressure lift setpoint within the limit specified in the Pressure and Temperature Limits Report (PTLR) during startup and shutdown conditions (see Section 5.2.2.2).

The Low Temperature Overpressure Protection (LTOP) circuitry for low pressure power operated relief valve (PORV) actuation circuitry uses multiple pressure sensors, power supplies and logic trains to improve system reliability. Each of the two pressurizer power operated relief valves (PORVs) is manually enabled using two key lock switches, one to line up the nitrogen supply and the other to enable the low-pressure setpoint.

When the reactor vessel is at low temperature with the Low Temperature Overpressure Protection (LTOP) system enabled, a pressure transient is terminated below the 10 CFR 50, Appendix G limit by automatic opening of the pressurizer power operated relief valves (PORVs). An enabling alarm monitors the reactor coolant system temperature, the position of the key lock switches, and the upstream isolation valve position.

The Low Temperature Overpressure Protection (LTOP) system is required to be in operation during plant cooldown prior to decreasing temperature below the limit specified in the PTLR or on initiation of the residual heat removal system, and it is disabled prior to exceeding 350°F during plant heatup. The enabling alarm alerts the operator in the event the reactor coolant system temperature is below the limit specified in the PTLR and the Low Temperature Overpressure Protection (LTOP) system valve or switch alignment has not been completed.

The pressurizer power operated relief valves (PORVs) are spring closed and air or nitrogen opened. Each of the two pressurizer power operated relief valves (PORVs) receives actuating gas from either the plant instrument air system or a backup nitrogen accumulator; however, only nitrogen is used during LTOP conditions. Low-pressure alarms are installed in the control room to alert the operator to a low nitrogen accumulator pressure condition.

In addition to narrow-range pressurizer pressure indication, a reactor coolant system wide-range pressure indication and recording (0-3000 psig) and a low-pressure indication (0-700 psig) are provided on the main control board.

An overpressure alarm that incorporates two setpoints is also provided. One setpoint is variable and follows the PTLR limit. The other alarms at a preprogrammed differential pressure. Both setpoints alarm and light on the plant process computer system.

7.6.2 AUXILIARY FEEDWATER SYSTEM AUTOMATIC INITIATION AND FLOW INDICATION

Redundant flow indication is provided for each motor-driven auxiliary feedwater pump (MDAFW) and the common discharge of the turbine-driven auxiliary feedwater pump (TDAFW). Each redundant channel of flow indication consists of the following:

- Qualified transmitter.
- Transmitter power supply.
- Square root extractor.
- Output isolation amplifier.
- Main control board analog indicator.

Continuous indication is provided to the operator by means of a dual movement vertical scale indicator. Each movement receives the analog signal from its respective channel of flow indication for a particular auxiliary feedwater flow path. Hence, the operator can quickly ascertain if there is any discrepancy between channels.

7.6.3 SUBCOOLING METER

As a result of NUREG 0578, Item 2.1.3.b, Instrumentation for Detection of Inadequate Core Cooling, two separate analog subcooling meters were installed to provide a continuous display of reactor coolant temperature margin to saturation. There is one resistance temperature detector input from each hot leg, one going to each meter. The range is 0°-700°F. The dual-element resistance temperature detectors are seismically and environmentally qualified.
There is one pressurizer pressure input for each meter with a range of 0-3000 psig. Resistance temperature detectors and pressure transmitters are seismically and environmentally qualified.

Redundancy is provided by the plant process computer system and safety parameter display system whose inputs are independent of the subcooling meter. Computer temperature input comes from five in-core thermocouples with a range of 300-700°F and pressure input comes from the reactor coolant system with a range of 0-3000 psig.

Indication of the subcooling margin is provided in the control room. An alarm is provided to indicate that one of the channels has computed a subcooling margin of 35 °F or less. Subcooling margin is input to the plant process computer system for MODES 1 and 2 and safety assessment.

Emergency operating procedures (EOPs) utilize core exit thermocouples, reactor coolant system pressure and EOP subcooling attachments to determine subcooling values for EOP usage.

7.6.4 DIRECT CURRENT POWER SYSTEM BUS VOLTAGE MONITORING AND ANNUNCIATION

A dc monitoring system has been added to the three dc systems. The system provides a separate group alarm for each battery consisting of a high voltage alarm (greater than 140 V), a low voltage alarm (less than 132 V), low charging rate alarm, or negative (discharging) rate

alarm. The system along with existing alarms (Section 8.3.2.2) provides complete indication of abnormal DC system conditions.

7.6.5 REACTOR VESSEL LEVEL INDICATION SYSTEM

The reactor vessel level indication system is used to trend coolant inventory within the reactor vessel during all phases of plant operation, including postaccident conditions with quasi-steady-state conditions and during slowly developing transients. The reactor vessel level indication system is a Class 1E system and all components are designated Seismic Category I. The reactor vessel level indication system consists of two redundant differential pressure transmitters. One process connection of the transmitters is connected to tubing from the reactor vessel head and the other is connected to tubing associated with an in-core neutron flux mapping guide tube. The output from these transmitters is processed by redundant Foxboro signal processing racks. The Foxboro signal processing rack produces an analog signal that is proportional to the reactor coolant inventory in the reactor vessel.

Other parameters introduced to the Foxboro signal processing racks are core exit temperatures, cold leg temperature, reactor coolant system wide-range pressure, reactor coolant pump status, safety injection status, and residual heat removal status. The introduction of these inputs is necessary for an accurate reactor vessel inventory output. The differential pressure signals are processed to compensate for reference leg temperature differences, primary coolant flow and temperature, safety injection, and residual heat removal operation.

The reactor vessel level indication system displays reactor vessel level and vessel fluid fraction locally at each reactor vessel level indication system instrument rack and in the main control room. Signals are also input to the plant process computer system for an independent indication of reactor vessel level.

An evaluation of the Westinghouse Owners Group Emergency Response Guidelines was performed to establish a minimum accuracy design objective for the reactor vessel level indication system. This evaluation is presented in *Reference 1*. For worst-case conditions an uncertainty of approximately 10% was determined to be an acceptable design objective. The worst-case uncertainty for the system is 10%, which meets the design objective.

Failure of the upper sensing line to drain under voiding conditions is addressed in *Reference 2*. If this line does not drain, the reactor vessel level indication system will read higher than the actual reactor vessel level, which is non-conservative. A correction factor will address this issue. This correction factor of 4% fluid fraction (with reactor coolant pumps on) or 9% reactor vessel level (with reactor coolant pumps off) has been added to the setpoints for the reactor vessel level indication system used in emergency operating procedures.

The instrumentation ranges from the top of the reactor vessel to the top of the core exit thermocouples. Because of flow instabilities with vessel inventory below the hot leg and the reactor coolant pumps on, the instrumentation will only provide accurate trending information from the top of the vessel to the hot leg. With the reactor coolant pumps off, the instrumentation is accurate from the top of the vessel to the top of the core exit thermocouples.
Inventory trending below the top of the core is calculated based upon assumed saturated conditions within the core corresponding to system pressure. Instrument indication below the

top of the core should give reasonable results for collapsed inventory; however, it is considered only an approximation of the inventory trend because of the many phenomena that may affect system response. The reactor vessel level indication system was installed to meet the requirements of NUREG 0737, Item II.F.2. Its purpose is to provide the plant operator additional information on reactor vessel water level, particularly during transient events.

REFERENCES FOR SECTION 7.6

1. Letter from R. W. Kober, RG&E, to C. Stahle, NRC, Subject: Inadequate Core Cooling Instrumentation, NUREG 0737, Item II.F.2, dated September 18, 1987.

2. Rochester Gas and Electric Corporation Design Analysis, DA-EE-97-055, Reactor Vessel Level Indication System (RVLIS) Correction, dated June 23, 1997.

7.7 CONTROL SYSTEMS NOT REQUIRED FOR SAFETY

7.7.1 DESCRIPTION

7.7.1.1 General

7.7.1.1.1 Reactor Control System

The reactor control system is designed to limit nuclear plant transients for prescribed design load perturbations, under automatic control, within prescribed limits to preclude the possibility of a reactor trip in the course of these transients.

The following is a general description of the reactor control system employed by Westinghouse for control of pressurized water reactors (PWRs):

During steady-state operation, the primary function of the reactor control is to maintain a programmed average reactor coolant temperature that rises in proportion to load. The control system also limits nuclear plant system transients to prescribed limits about this programmed temperature for specified load perturbations. (See Figure 7.7-1.)

In 1997 and 1999, components in channels I, II, III, and IV were replaced such that the function being performed by the electrical bridge circuit in the temperature channels were modified to be accomplished mathematically in the time domain module (see Figure 7.2-14).

The controller compares the average of these temperatures with the programmed temperature. A signal, proportional to plant load, sets the programmed temperature.

The controller directs fixed groups of control rod clusters (the control groups) to decrease reactor power as required to maintain the desired average temperature. The automatic control rod withdrawal function has been disabled; therefore, rod withdrawal is performed manually by the operator to increase the average temperature. Within each control group, a proportional speed control sequentially actuates the rods. The sequential mode of operation provides fine temperature control for steady-state operation, including those periods when boron concentration is adjusted to account for long-term reactivity effects such as core burnup.

For rapid reactivity requirements to accommodate relatively large changes in load, the control groups are driven at a higher rate through the proportional speed control so that each group is effectively moving as a unit. A neutron flux signal and a turbine load signal are used in addition to the average temperature signal to improve the controller response for large and rapid load variations.

7.7.1.1.2 Steam Dump Control System

A steam dump control system removes sensible heat stored in the reactor coolant system for a large step load decrease or a reactor trip. With the average reactor coolant temperature programmed, the full load average temperature is significantly greater than the saturation pressure corresponding to the Main Steam Safety Valve (MSSV) set pressure. Steam is dumped in order to remove the stored heat in the primary system at a rate fast enough to prevent lifting of the Main Steam Safety Valve (MSSV) for a large step load decrease, or a

reactor trip. The average reactor coolant temperature and steam pressure activate the dump system, which is interlocked with plant output to improve overall control reliability.

7.7.1.1.3 Reactivity Control

The shutdown groups of control rods are capable of shutting the reactor down by a sufficiently safe margin. They are used in conjunction with the adjustment of chemical shim and the control group to maintain proper shutdown margins for all operating conditions.

The automatic control group is interlocked with measurements of turbine output to prevent automatic control below a predetermined percentage of full power. The manual automatic controls are further interlocked with measurements of coolant temperatures, nuclear flux, and rod drop indication to prevent approach to an overpower condition.

Overall reactivity control is achieved by the combination of chemical shim and control rod clusters. Long-term regulation of core reactivity is accomplished by adjusting the concentration of boric acid in the reactor coolant. Short-term reactivity control for power changes or reactor trip is provided by movement of control rod clusters.

The primary function of the reactor control system is to provide automatic control of the rod clusters during power operation of the reactor. The system uses input signals including neutron flux, coolant temperature, and plant turbine load. The chemical and volume control system serves as a secondary reactor control system by the addition and removal of varying amounts of boric acid solution.

A block diagram of the reactor control system is shown in Figure 7.7-2.
There is no provision for a direct continuous visual display of primary coolant boron concentration. When the reactor is critical, the best indication of reactivity status in the core is the position of the control group in relation to plant power and average coolant temperature.

There is a direct, predictable, and reproducible relationship between rod position and power and it is this relationship that establishes the lower insertion limit calculated by the rod insertion limit monitor. There are two alarm setpoints to alert the operator to take corrective action in the event a control group approaches or reaches its lower limit.

Any unexpected change in the position of the control group under automatic control or a change in coolant temperature under manual control provides a direct and immediate indication of a change in the reactivity status of the reactor. In addition, periodic samples of coolant boron concentration are taken. The variation in concentration during core life provides a further check on the reactivity status of the reactor including core depletion.

7.7.1.1.4 Reactor Control System Operation

The reactor control system is designed to enable the reactor to follow load changes automatically when the plant output is above 12.8% of nominal power. Control rod positioning may be performed automatically when plant output is above this value and manually at any time. Automatic control allows for control rod insertion to decrease the average temperature or account for load decreases. For load increases, the control rods are withdrawn manually by the operator.

The operator is able to select any single bank of rods for manual operation. This is accomplished with a single switch so that the operator may not select more than one bank. The operator may also select automatic or manual reactor control, in which case the control banks can be moved only in their normal sequence with some overlap as one bank reaches its full withdrawal position and the next bank begins to withdraw. Relay interlocks, designed to meet the single-failure criterion, are provided to preclude simultaneous withdrawal of more than one group of control and shutdown rods except in overlap regions.

The system enables the nuclear plant to accept a generation step load increase of 10% and a ramp increase of 5% per minute within the load range of 12.8% to 100% without reactor trip subject to possible xenon limitations. The reactor control system no longer has the ability to withdraw the control rods on plant load increase transients. These transients can still be accommodated without a reactor trip; however, the operator will withdraw the rods to return the average temperature to the programmed value. Similar step and ramp load reductions are possible within the range of 100% to 12.8% of nominal power.

The control system is capable of restoring coolant average temperature to within the programmed temperature deadband, following a scheduled or transient decrease in load.

The reactor plant can be placed under automatic control in the power range between 12.8% load and full load for the following design transients:

A. ±10% step change in load without steam dump.

B. ±5% per minute loading and unloading.

C. 50% load rejection from full power.

D. Turbine trip from 50% power without a reactor trip.

The control system is designed to operate as a stable system over the full range of automatic control throughout core life without requiring operator adjustment of setpoints other than normal calibration procedures.

7.7.1.1.5 Pressurizer Pressure and Water Level Control System

A programmed pressurizer water level as a function of reactor coolant average temperature minimizes the requirements of the chemical and volume control and waste disposal systems resulting from coolant density changes during loading and unloading from full power to zero power.

The pressurizer water level control system establishes, maintains, and restores pressurizer water level within specified limits as a function of the average coolant temperature.

The pressurizer pressure control system maintains plant pressure within an acceptable operating band during steady-state and/or transient conditions.

7.7.1.1.6 Steam Dump System

Following a reactor and turbine trip, sensible heat stored in the reactor coolant is removed without actuation of Main Steam Safety Valves (MSSV) by means of controlled steam dump

to the condenser and by injection of feedwater to the steam generators. Reactor coolant system temperature is reduced to the no-load condition. This no-load coolant temperature is maintained by steam bypass to the condensers to remove residual heat.

The advanced digital feedwater control system (ADFCS) measures, indicates, and controls the water level in the two steam generators. The steam dump system is used to minimize the stresses on the primary system induced by disturbances in the secondary plant steam loads. In conjunction with the rod control system, the steam dump system allows the plant to accommodate a 50% load rejection without inducing a reactor trip.

7.7.1.2 Rod Control System

7.7.1.2.1 Control Group Control

7.7.1.2.1.1 General

The rod control system is a solid-state electronic control system that moves and holds the control rods according to system input orders. The rod drive mechanism is an electromagnetic stepping type mechanism with three actuating coils for holding and movement. To hold a control rod, the system keeps a gripper coil energized. To move a rod, the system sequentially energizes and deenergizes the three coils causing the rod to move in discrete steps.

In automatic control the rod control system maintains a programmed reactor coolant average temperature with adjustments of control rod position for equilibrium plant conditions. The reactor control system is capable of restoring programmed average temperature following a scheduled or transient change in load. The coolant average temperature increases linearly from zero power to the full power conditions.

In manual control the operator maintains control of the reactor through bypassing the reactor control unit. By using the bank selector and the IN-HOLD-OUT switches the operator can move the rods either by individual banks or in manual with bank overlap.

The control system will also compensate initially for reactivity changes caused by fuel depletion and/or xenon transients. The automatic control rod withdrawal function has been disabled and the rod control system will no longer compensate for fuel depletion. The initial compensation for fuel depletion is performed manually by the operator. Final compensation for these two effects is periodically made with adjustments of boron concentration. The control system then readjusts the control rod in response to changes in coolant average temperature resulting from changes in boron concentration.

7.7.1.2.1.2 Rod Control Input Signals

The coolant average temperatures are measured from the hot leg and the cold leg twice in each reactor coolant loop. The average of the four measured average temperatures is the main control signal. This signal is sent to the control rod programmer through a proportional plus rate compensation unit. The control rod programmer commands the direction and speed of control rod motion. A power-load mismatch signal is also employed as a control signal to improve the plant performance. The power-load mismatch channel takes the difference between nuclear power (average of all four power range channels) and a signal of turbine load

(first-stage turbine pressure) and passes it through a high-pass filter such that only a rapid change in flux or power causes rod motion. The power-load mismatch compensation serves to speed up system response and to reduce transient peaks.

7.7.1.2.1.3 Rod Control Program

The control group is divided into four banks to follow load changes over the full range of power operation. Each control bank is driven by a sequencing, variable speed rod drive control unit. The rods in each control bank are divided into two subgroups; the subgroups are moved sequentially one step at a time. The sequence of motion is reversible, that is, a withdrawal sequence is the reverse of the insertion sequence. The variable speed sequential rod control affords the ability to insert a small amount of reactivity at low speed to accomplish fine control of reactor coolant average temperature about a small temperature deadband.

Manual control is provided to manually move a control bank in or out at a preselected fixed speed.

Proper sequencing of the control rod assemblies is ensured first, by automatic programming equipment in the rod control system and second, through administrative control by the reactor plant operator. Startup of the plant is accomplished by first manually withdrawing the shut-down rods to the full OUT position. This action requires the operator to select the SHUT-DOWN BANK position on a control board mounted selector switch and then to position the IN-HOLD-OUT lever (which has a spring return to the HOLD position) to the OUT position.

Control rod assemblies are then withdrawn under manual control of the operator by first selecting the MANUAL position on the control board mounted selector switch and then positioning the IN-HOLD-OUT lever to the OUT position. In the MANUAL selector switch position, the rods are withdrawn (or inserted) in a predetermined programmed sequence by the automatic programming equipment.

When the reactor power reaches approximately 12.8%, the operator may select the AUTOMATIC position, where the IN-HOLD-OUT lever is out of service and rod motion is controlled by the reactor control and protection systems. Automatic control rod withdrawal has been disabled. For plant startup, the control rods are manually withdrawn by the operator. A permissive interlock limits automatic control to reactor power levels above 12.8%. In the AUTOMATIC position, the rods are again inserted in a predetermined programmed sequence by the automatic programming equipment.

Programming is set so that as the first bank out (control bank A) reaches a preset position near the top of the core, the second bank out (control bank B) begins to move out simultaneously with the first bank. When control bank A reaches the top of the core, it stops, and control bank B continues until it reaches a preset position near the top of the core where control bank C motion begins. This withdrawal sequence continues until the plant reaches the desired power level. The programmed insertion sequence is the opposite of the withdrawal sequence, i.e., the last control bank out is the first control bank in.

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

Twenty-one of 29 control rods are used for reactivity control to maintain the programmed average coolant temperature as power level changes. The remainder are reserved for reactor shutdown.

7.7.1.2.2 Shutdown Group Control

The shutdown groups of control rods together with the control group are capable of shutting the reactor down. They are used in conjunction with the adjustment of chemical shim and the control group to maintain an adequate shutdown margin of at least 1% with a stuck control rod for all normal operating conditions. These shutdown groups are manually controlled, except for automatic trip signals, and are moved at a constant speed. They are fully withdrawn during power operation and are withdrawn first during startup. Criticality is always approached with the control group after withdrawal of the shutdown groups.

7.7.1.2.3 Control Rod Drive Performance

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

The sequence of motion is reversible, that is, withdrawal sequence is the reverse of the insertion sequence. The sequencing speed is proportional to the control signal from the reactor control system. This provides control group speed control proportional to the demand signal from the control system. (See Figure 7.7-3.)

A rod drive mechanism control center is provided to receive sequenced signals from the programmer and to actuate contactors in series with the coils of the rod drive mechanisms. Two reactor trip breakers are placed in series with the supply for these coils. To permit on-line testing, one bypass breaker position is provided across each of the two trip breakers.

7.7.1.2.4 Control Rod Power Supply System

7.7.1.2.4.1 General

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

The solid-state rod control system is operated from two parallel connected 438-kVA generators (Figure 7.7-4) which provide a 260-V, line-to-line, three-phase, four-wire AC power to the rod control circuits through two series connected reactor trip breakers. This AC power is distributed from the trip breakers to a lineup of identical solid-state power cabinets using a single overhead run of enclosed bus duct which is bolted to and therefore comprises part of

the power cabinet arrangement. The alternating current from the motor-generator sets is converted to a profiled direct current by the power cabinet and is then distributed to the mechanism coils. Each complete rod control system includes a single 70-V DC power supply that is used for holding the mechanisms in position during maintenance of normal power supply.

This 70-V supply, which receives its input from the ac power source downstream of the reactor trip breakers, is distributed to each power cabinet and permits holding mechanisms in groups of four manual positioning switches located in the power cabinets. The output capacity of this 70-V DC supply is 50 amp. The system configuration limits the holding capability to eight rods assuming that the DC holding function is used in only one power cabinet at a time.

Current to the mechanisms is interrupted by opening either of the reactor trip breakers. The 70-V DC maintenance supply will also be interrupted since this supply receives its input power through the reactor trip breakers.

The trip breakers are arranged in the reactor trip switchgear in individual metal-enclosed compartments. The 1000-amp bus work, making up the connections between scram breakers, will be separated by metal barriers to prevent the possibility that any conducting object could short circuit or bypass scram breaker contacts. Figure 7.7-4 indicates the arrangement of this equipment.

The 70-V DC holding supply and associated switches have been provided to avoid the need for bringing a separate DC power source to the rod control system during maintenance on the power cabinet circuits. This source is adequate for holding a maximum of eight mechanisms and satisfies all maintenance holding requirements.

7.7.1.2.4.2 Control Rod Power Supply Connections

The control rods are divided into banks that are further divided into two groups each. The banks are moved such that the groups of a bank are always within one step of each other. Groups of rods consist of two or more rods that are electrically parallel to step simultaneously.

The banks and groups are distributed among four solid-state power cabinets as shown below:

Control Bank A - Group 1	Control Bank A - Group 2
Control Bank C - Group 1	Control Bank C - Group 2
Shutdown Bank A - Group 1	Shutdown Bank A - Group 2
Control Bank B - Group 1	Control Bank B - Group 2
Control Bank D - Group 1	Control Bank D - Group 2
Not Used	Not Used

Each power cabinet is designed to operate three groups of mechanisms such that only one group can be moved at a time while the other two groups are held in position. Therefore, the distribution permits no more than two banks to move at a time.

7.7.1.2.5 Control Rod Power Supply Evaluation

The rod control system equipment is assembled in enclosed steel cabinets. Three-phase power is distributed to the equipment through a steel-enclosed bus duct, bolted to the cabinets. Direct current power connections to the individual mechanisms are routed to the reactor head area from the solid-state cabinets through insulated cables, enclosed junction boxes, enclosed reactor containment penetrations, and sealed connectors. In view of this type of construction, any accidental connection of either an AC or DC power source, either internal or external to the cabinets, is not considered credible.

7.7.1.2.5.1 Alternating Current Power Connections

The three-phase four-wire supply voltage required to energize the equipment is 260 V line to line, 58.3 Hz, 400-kVA capacity, zigzag connected. It is unlikely that any power supply, and in particular one as unusual as this four-wire power source could be accidently connected in phase in the required configuration. Also it should be noted that this requires multiple connections, not single connections. The closest outside sources available in the plants are 480-V auxiliary power sources and 208-V lighting sources.

Connections of either a 480-V or 208-V, 60-Hz source to the single ac bus supplying the rod control system causes currents to flow between the sources due to an out-of-phase condition. These currents flow until the generator accelerates to a speed synchronous with the 60-Hz outside source, a time sufficient to trip the generator breakers. The out-of-phase currents for an unlimited capacity outside source, an outside source with a capacity equivalent to the normal generator kVA, and for either one or two motor-generator sets in service are tabulated in Table 7.7-1.

All of the currents in Table 7.7-1 are sufficiently high to trip out the generator breakers on overcurrent. This trip-out is detectable by annunciation in the control room. If the outside power source trips, the connection is of no concern.

Each solid-state power cabinet is tied to the main ac bus through three fused disconnect switches: one each for the stationary gripper coil circuits, the movable gripper coil circuits, and the lift coil circuits. Reference voltages to operate the control circuits for all three coil circuits must be in phase with the supply to all coil circuits for proper operation of the system. If the outside power source were brought into an individual cabinet, nine normal source connections would have to be disconnected and the outside source would have to be tied in phase to the proper nine points plus one neutral point to allow movement of the rods. This is not considered credible.

Connection of a single-phase ac source (i.e., one line to neutral) is also considered improbable. This would again require a high capacity source which would have to be

connected in phase with the nonsynchronous motor-generator set supply. Again more than one connection is needed to achieve this condition. Each power cabinet contains three alarm circuits (stationary, movable, and lift) that would annunciate the condition to the operator. In addition, calculations show that a single-phase source of 208 V, 260 V, or 480 V would not supply enough current to hold the rods. Therefore, a jumper across two trip circuit breaker contacts in series that results in a single phase remaining closed would not provide sufficient current to hold up the rods.

The normal source generators are connected in a zigzag winding configuration to eliminate the effects of direct current saturation of the machines resulting from the direct currents that flow in the half wave bridge rectifier circuits. If this connection were not used, the generator core would saturate and loss of generating action would occur. This condition would also occur in a transformer. An outside source not having the zigzag configuration would have to have a large capacity (>400 kVA) to avoid the loss of transformer action from saturation.

Most of the components in the equipment are applied with a 100% safety factor. Therefore, the possibility exists that the system will operate at 480 V with a source of sufficient capacity. The system will definitely operate at 208 V with a source of sufficient capacity.

The connection of an outside source of ac power to one rod control system would first require a need for this source. No such need exists since two power sources (motor-generator sets) are already provided to supply the system. If the source were connected in spite of the need, extreme measures would have to be taken to complete the connection. The outside source would have to be a large capacity (400-kVA) one. The currents that flow would require the routing of large conductors or bus bars, not the usual clip leads. Then, the disassembly of switchgear or enclosed bus duct would be required to expose the single ac bus. Large bolted cable or bus bar terminations would have to be completed. A total of four conductors would have to be connected in phase with a nonsynchronous source. To expect that a connection could be completed with the equipment either energized or deenergized, in view of the obstacles which would prevent such a connection, is incredible. However, even if the connection were completed, the outside source connection would be detectable by the operator through the tripping of the generator breakers.

7.7.1.2.5.2 Direct Current Power Connections

An external DC source could, if connected inside the power cabinet, hold the rods in position. This would require a minimum supply voltage of 50 V. Since the holding current for each mechanism coil is 4.4 amp, the DC current capacity would have to be approximately 128 amp to hold all rods. Achieving this situation would require several acts: bringing in a power source which is not required for any type of operation in the rod control system, preferentially connecting it into the system at the correct points, and actuating specific holding switches so as to interconnect all rods. Closure of 12 switches in four separate cabinets would be required to hold all rods. One switch could hold as many as four rods.

Should an external DC source be connected to the system, the system is provided with features to permit its detection.

Each solid-state power cabinet contains circuitry which compares the actual currents in the stationary and movable gripper coils with the reference signals from the step sequencing unit (slave cycler). In taking a single step, the current to the stationary gripper coil will be profiled from the holding value to the maximum, to zero, and return to holding level. Correspondingly, the movable gripper coil must change from zero to maximum and return to zero. The pressure of an external DC source on either the stationary or movable coils would prevent the related currents from returning to zero.

This situation would be instantaneously annunciated by way of the comparison circuit. Therefore, any rod motion would actuate an alarm indicating the presence of an external dc source. In addition, an external dc source would prevent rods from stepping. Thus, an external source could be detected by the rod position indication system indicating failure of the rod(s) to move.

Connection of an external dc power source to the output lines of the 70-V dc power supply can be detected by opening the three-phase primary input of the supply and checking the output with a voltmeter.

7.7.1.2.5.3 Evaluation Summary

In view of the preceding discussion, the postulated connection of an external power source (either ac or dc) or short circuits that could prevent dropping of the rods is not considered credible. Specifically,

a. The need for an outside power source has been eliminated by incorporating built-in holding sources as part of the rod control system and by providing two motor-generator sets.
b. The equipment is contained within enclosed steel cabinets precluding the possibility of an accidental connection of either ac or dc power in the cabinets.
c. Alternating current power distribution is accomplished using steel-enclosed bus duct. The high capacity (400-kVA) ac power source is unique and not readily available. Multiple connections are required.
d. Direct current power is distributed to the individual mechanisms through insulated cables and enclosed electrical connections precluding the accidental connection of an outside dc source external to the cabinets. The high capacity dc source required to hold rods is not readily available in the rod control system, would require multiple connections, and would require deliberate positioning of switches within the enclosed cabinets.
e. Provisions are made in the system to permit detection of an external dc source that could preclude a rod release.

The total capacity of the system including the overload capability of each motor-generator set is such that a single set out of service does not cause limitations in rod motion during MODES 1 and 2. In order to minimize reactor trip as a result of a unit malfunction, the power system is normally operated with both units in service.

There is no possible failure in the power cabinet that can cause more than one group of four mechanisms to be moved at one time. First, to allow motion of mechanisms in a second group while one group is moving, the circuits for the stationary, movable, and lift coils must

all fail simultaneously. However, should this occur, the circuit arrangement for the movable and lift coils will cause the current available to the mechanism's coils to divide equally between coils in the two groups. It has been shown by test that the L-106 mechanism will not operate on half current. Finally, a multiplexing failure detection circuit is included in each power cabinet which stops rod withdrawal or insertion should such a failure occur.

7.7.1.2.6 Rod Position Indication System

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

7.7.1.2.6.1 Microprocessor System

The microprocessor rod position indication (MRPI) system consists of a digital detector assembly for each rod, a data cabinet located inside containment, and display racks located in the relay room. Rod position data is displayed on a color cathode ray tube (CRT) in the control room and also transmitted to the plant process computer system. The data cabinet inside containment contains two multiplexers (MUX), which take rod position information from each of the rods and transmit it to the processors, which are in the display racks located in the relay room. One processor supplies information to the CRT located on the control board, the other processor supplies information to the plant process computer system. Both processors are required to produce a block rod withdrawal[a] signal. The plant process computer system backup can be used if the CRT in the MRPI system becomes inoperable.

The MRPI system directly senses rod position in intervals of 12 steps for each rod. The digital detector assemblies consist of 20 discrete coil pairs spaced at 12-step intervals as shown in Figure 7.7-4a. The MRPI system will normally indicate zero rod position until the rod goes from zero steps to the first step. At that time the indication will normally switch from zero to 12. When the rod goes from >one to two steps, the indication will normally switch from 0 to The rod will normally be within +7 to –5 steps of the MRPI indication; however, if the transition uncertainty of +2 steps is considered, the rod will always be within +9 steps of the MRPI indication.

The safety concerns associated with the MRPI system are associated with generation of a block rod withdrawal signal and the ability to comply with the rod misalignment requirement.

The MRPI system consists of one digital detector assembly per rod. All the detector assemblies are multiplexed and become input to two redundant MRPI signal processors. Each signal processor independently monitors all rods and senses a rod bottom for any rod. A rod bottom signal from both signal processors is required to generate a block rod withdrawal[a] signal. The two-out-of-two coincident signal requirement reduces inadvertent block rod withdrawal but does not affect the accident analysis assumptions.

The MRPI system is designed to satisfy the rod misalignment requirement. The MRPI system determines rod position in 12-step intervals. The true rod position is always within ±9

a. The automatic rod withdrawal function of the reactor control system has been disabled. The block automatic rod withdrawal function from MRPI on a rod drop is no longer used.

to −7 steps of the indicated position (±7 to −5 steps due to the 12-step interval and ±2 steps transition uncertainty due to processing and coil sensitivity). Assume a rod becomes stuck at zero steps. The MRPI indication for that rod could be 8. Since the step counter does not know the rod is stuck, it would continue to count. The rod deviation alarm will be generated by the plant process computer system. The alarm would be generated when the step counter reaches 20 steps (20 steps--MRPI indication of 8 steps = ± setpoint of 12 steps). Therefore, the maximum deviation possible is 20 minus 0 or 20 steps. This is bounded by the accident analysis, which assumes 25-step rod misalignment. Another possible situation is the rod to rod misalignment within a group or a bank. Assume the inoperable rod is at step 0. The MRPI indication for this rod could be 8 steps. If the others within the group or bank are aligned so that their MRPI indicated position is also 8 steps, the highest actual position for any of these rods would be 14 steps. Therefore, if the rods are required to have the same indicated position, the maximum actual position difference would be 14 minus 0 or 14 steps. This is bounded by the accident analysis, which assumes 25-step rod misalignment.

The MRPI system is not Class 1E. The system is not required for safe shutdown of the plant and is not required to operate during or after a seismic event.

7.7.1.2.6.2 Digital System

The digital system counts pulses generated in the rod drive control system. One counter is associated with each group of rods within a bank, making a total of 10 for the four control banks and one shutdown bank. Readout of the digital system is in the form of digital add-subtract counters reading the number of steps of rod withdrawal with one display for each. These readouts are mounted on the control panel.

The digital and MRPI systems are separate systems; each serves as backup for the other. Operating procedures require the reactor operator to compare the system readings upon recognition of any apparent malfunction. Therefore, a single failure in rod position indication does not in itself lead the operator to take erroneous action in the operation of the reactor.

7.7.1.2.6.3 Actual Position Indication

This system derives the position signal directly from measurements of the driven rod position using the MRPI system described in Section 7.7.1.2.6.1, Item 1.

7.7.1.2.6.4 Demand Position Indication

The bank demand position signal is derived from the programmer and is displayed on an add-subtract pulse counter mounted in the control console.

7.7.1.2.6.5 Rod Deviation Alarm

Both the demand and actual rod position signals are monitored by a rod deviation monitoring system that provides an alarm whenever the individual rod position signal deviates from the bank demand signal by a preset limit.

7.7.1.2.7 Pulse-to-Analog Converter

A pulse-to-analog converter is furnished for each control bank. The converter and the plant process computer receive the control bank demand position pulses from the rod control system. The pulse to analog converter converts the count signal to an equivalent dc analog signal proportional to bank demand. This signal is fed to the bank insertion limit monitor and plant process computer system. The pulse-to-analog converter has a digital display inside the rod position indication cabinet with provisions for manually pulsing the counter up or down.

7.7.1.2.8 Interlocks and Rod Stops

The control group used for automatic control is interlocked with measurements of turbine generator load and reactor power to prevent automatic control rod withdrawal below 12.8% of nominal power. Automatic control rod withdrawal has been disabled for all power levels. The manual and automatic controls are further interlocked with measurements of nuclear flux, delta T, and rod drop indication to prevent approach to an overpower condition. The logic diagram of these interlocks is shown in Drawing 33013-1353, Sheet 15.

The following permissives (rod stops) are provided in the rod control system and are listed in Table 7.7-2.

A. Overpower rod stops (for withdrawal).

1. Power range nuclear instrumentation system high flux, setpoint 103% power with a one-of-four coincidence; operates in the manual and automatic modes.
2. Intermediate-range nuclear instrumentation system high flux, setpoint is current equivalent to 20% power with a one-of-two coincidence; operates in the manual and automatic modes; the rod stop is blocked when the intermediate-range nuclear instrumentation system trip is blocked.
3. Overtemperature delta T, setpoint is 3% of rated ΔT below the trip setpoint with a two-of-four coincidence; operates in the manual and automatic modes.
4. Overpower delta T, setpoint is 3% of rated ΔT below the trip setpoint with a two-of-four coincidence; operates in the manual and automatic modes.

B. Low power rod stop.

Low power rod stop prevents outward rod motion in automatic when turbine impulse pressure is less than 12.8% power. This prevents unstable low power operation. Automatic control rod withdrawal has been disabled for all power levels. The low power rod stop is no longer applicable.

C. Auto rod stop on dropped rod.

Dropped rod automatic rod stop has two setpoints or detected conditions: first, if a 5% power decrease occurs in 5 sec on one-of-four power range nuclear instrumentation system, and second, if any of the following conditions exists, outward rod motion will be prohibited. The automatic control rod withdrawal function has been disabled. The auto rod stop on dropped rod is no longer applicable.

D.

- any rod in the shutdown bank A or control bank A at 0 steps
- any rod in control bank B at 0 steps with bank B, C, or D ≥ 32 steps
- any rod in control bank C at 0 steps with bank C or D ≥ 32 steps
- any rod in control bank D at 0 steps with bank D ≥ 32 steps

E. T_{AVG} - average T_{AVG} channel deviation rod stop.

A temperature difference of ±4°F between any one of the four T_{AVG} channels and average T_{AVG} will actuate a control room alarm and stop automatic rod movement.

7.7.1.2.9 Rod Insertion Limit Circuit

The rod insertion limit circuit is designed to provide a continuously calculated insertion limit for each of the control banks that is variable with power. It provides alarms to ensure that the operator keeps the control rods located within the limits. The rod insertion limit circuit performs its function by receiving control bank position data from the rod control system. It compares this data to the calculated limit that is determined by reactor power as measured from the coolant loop average differential temperature (delta T).

The rod insertion limits ensure that adequate shutdown margin exists to shut down the reactor at any time and condition in the life of the core. In addition, it guarantees protection from core damage due to a postulated rod ejection accident, as well as possible core damage due to uneven core power distribution from misaligned control rods at high power (e.g., provides for acceptable core peaking factors).

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

Z_{LL} = A (average delta T) + B (average T_{AVG}) + C

where A, B are preset manually adjustable gains and C is a preset manually adjustable bias. Average delta T and average T_{AVG} are discussed in Section 7.7.5.

One insertion limit monitor is provided for each control bank. The Low alarm Bank D only alerts the operator of an approach to a reduced shutdown reactivity situation requiring boron addition by following normal procedures with the chemical and volume control system. Actuation of the Low-Low alarm (Banks A, B, C, and D) requires the operator to take immediate action to add boron to the system by any one of several alternative methods.

7.7.1.2.10 Rod Drop Protection

Two independent systems are provided to sense a dropped rod, (1) a rod bottom position detection system and (2) a system that senses sudden reduction in out-of-core neutron flux. Both protection systems initiate protective action in the form of blocking of automatic rod withdrawal. The automatic rod withdrawal function has been disabled. The rod drop protection function is not applicable. This action compensates for possible adverse core power distributions and permits an orderly retrieval of the dropped rod cluster control assembly.

The primary protection for the dropped rod cluster control assembly accident is the rod bottom signal derived for each rod from its individual position indication system. With this system, initiation of protection is not dependent on location, reactivity worth, or power distribution changes.

Backup protection is provided by use of the out-of-core power range nuclear detectors and is particularly effective for larger nuclear flux reductions occurring in the region of the core adjacent to the detectors.

The rod drop detection circuit from nuclear flux consists basically of a comparison of each ion chamber signal with the same signal taken through a first-order lag network. Since a dropped rod cluster control assembly will rapidly depress the local neutron flux, the decrease in flux will be detected by one or more of these four sensors. Such a sudden decrease in ion chamber current will be seen as a difference signal. A negative signal output greater than a preset value (approximately 5%) from any one of the four power range channels will actuate the rod drop protection.

Figure 7.7-6 indicates schematically the dropped rod alarm and the nuclear protection system in general. The potential consequences of any dropped rod cluster control assembly without protective action are limited to localized fuel failure, and the integrity of the reactor coolant system is maintained.

7.7.1.2.11 **Asymmetric Rod Cluster Control Assembly Withdrawal**

In a generic letter to licensees, Generic Letter 93-04, on June 21, 1993, the NRC staff identified actions to be taken by licensees related to the Salem rod control system failure event.
Rochester Gas and Electric Corporation responded (*References 2* and *3*) to the generic letter with detailed information on additional surveillance, troubleshooting, and monitoring that had been conducted; procedural changes and administrative controls that had been put into place; training on the Salem event that had been instituted; and a Westinghouse Owners Group initiative, which had demonstrated that for all Westinghouse plants there was no safety significance for an asymmetric rod cluster control assembly withdrawal related to the generic letter. Based on the results of the Westinghouse Owners Group initiative, RG&E concluded that the licensing basis for Ginna Station is still satisfied with regard to General Design Criterion 25 (or equivalent) for system response to a single failure in the rod control system.

The basis for this determination was enhanced by implementation of the following option as recommended by the Westinghouse Owners Group: (1) modification of the current order timing scheme to preclude asymmetric rod withdrawal in the presence of a rod control system failure and (2) implementation of a new current order surveillance test performed on a refueling outage basis that verifies that control rod drive mechanism current orders are not corrupted. Ginna Station successfully performed the lead plant testing on the timing change on April 14, 1994. Existing rod control system logic cabinet slave cycler decoder cards for lift coils, stationary coils, and movable coils were replaced with modified cards. Diodes were repositioned to implement a revised Westinghouse standard timing scheme. A fault similar to those experienced at Salem would now result in either conservative or no rod motion. This change does not affect normal rod movement and is transparent to operators.

A generic assessment of asymmetric rod cluster control assembly withdrawal was performed by Westinghouse and reported in WCAP 13803. A rod control system evaluation program performed on behalf of all Westinghouse plants was developed (WCAP 13864) to determine the type of motion that could occur when control rod drive mechanisms are subjected to corrupted current orders under varying conditions.

Test results from the Ginna Station lead plant tests were reviewed by the NRC and the as-tested modified timing sequence found acceptable (*Reference 4*). The Westinghouse Owners Group closure of this generic issue was provided to the NRC in *Reference 5* and was approved by the NRC in *Reference 6*. In *Reference 7*, the NRC stated that RG&E's responses to Generic Letter 93-04 were found to be acceptable and that the generic letter for Ginna Station was closed.

7.7.1.2.12 Rod Control Cabinet Cooling

The control rod drive logic cabinet and power cabinets located in the basement of the Intermediate Building (clean side) have been provided with packaged air conditioning units (door mounted). These air conditioning units are designed to maintain the internal cabinet temperatures within the normal intermediate building temperature limits. A high internal cabinet temperature alarm has also been provided (see Drawing 33013-1872).

7.7.1.3 Pressurizer Pressure and Level Control

7.7.1.3.1 Pressure Control

The reactor coolant system pressure is maintained at constant value by using heaters in the water region and spray in the steam region of the pressurizer. Electrical immersion heaters are located near the bottom of the pressurizer. A portion of the heater groups are proportional heaters and are used for small pressure variation control and to compensate for heat losses. The remaining backup heaters are turned on either when the pressurizer pressure controller signal is below a preset value or when pressurizer level is above a preset level setpoint.

Spray valves are located at the top of the pressurizer. Spray is initiated when the pressure controller signal is above a preset setpoint. Spray rate increases proportionally with increasing pressure until it reaches the maximum spray capacity. Steam condensed by spray reduces the pressurizer pressure. A small continuous spray is normally maintained to reduce thermal stresses and thermal shock when the spray valves open and to maintain uniform water chemistry and temperature in the pressurizer.

Two Pressurizer Power-Operated Relief Valves (PORV) limit system pressure below 2350 psia for large load reduction transients.

One relief valve is operated on the pressurizer pressure controller signals; the other one is operated on the actual pressure signal. An interlock is provided so that if a second pressure channel indicates low at the time the relief valve operation is called for by the control channel, the valve activation is blocked.

Two spring-loaded pressurizer safety valves limit system pressure below 2750 psia following a complete loss of load without direct reactor trip or turbine bypass. Under locked-rotor conditions, the pressurizer safety valves would maintain reactor coolant system pressure at a level below 2836 psia, which is acceptable.

The pressurizer has four pressure transmitters which provide signals used for indication, control, and protection. Each of the four channels may be displayed on a recorder by selecting the desired channel with the pressurizer pressure recorder selector switch. Pressurizer pressure is displayed on the main control board by four meters, with a range of 1700-2500 psig.

A pressure transmitter has also been installed on the pressurizer that is fully qualified to IEEE 323 and IEEE 344. This transmitter, which is powered from a Class 1E source, has its output continuously recorded to provide reactor coolant system wide-range pressure indication in the event of loss of offsite power.

To provide the control signal to the various pieces of equipment the actual system pressure is compared with the setpoint pressure. The output of the comparison is supplied to a proportional integral derivative (PID) circuit. The proportional part of the PID output is proportional to the actual pressure minus the reference pressure. Added to this is the integral component which accounts for the length of time a difference exists between actual and reference signals. Also added is a correction for rate-of-change of deviation signal to help speed up system response. This rate function is set to zero at Ginna Station.

7.7.1.3.2 Level Control

The pressurizer level control system maintains the pressurizer level within a programmed band consistent with T_{AVG}. The programmed level is a sufficient margin above the low level alarm where the heaters turn off. Letdown isolation is then initiated. The programmed level is sufficiently low to ensure that there is enough steam volume. A programmed level is used to limit charging pump speed change demands on a transient where T_{AVG} is changing, in contrast with a constant pressurizer level.

7.7.1.4 Turbine Bypass

A turbine bypass system is provided to accommodate a reactor trip with turbine trip, loss of 50% of rated load without reactor and turbine trip, or a turbine trip without reactor trip below 50% of rated load. The turbine bypass system removes steam to reduce the transient imposed upon the reactor coolant system so that the control rods can reduce the reactor power to a new equilibrium value without causing overtemperature-overpressure conditions in the reactor coolant system.

A turbine bypass is actuated by the coincidence of compensated coolant average temperature higher than the programmed value by a preset value and electrical load decrease greater than a preset value. All the turbine bypass valves stroke to full open immediately upon receiving the bypass signal. The bypass valves are modulated by the compensated coolant average temperature signal after they are full open. The turbine bypass reduces proportionately as the control rods act to reduce the coolant average temperature. The artificial load is therefore removed as the coolant average temperature is restored to its programmed equilibrium value.

The turbine bypass capacity is discussed in UFSAR Section 10.7.1. Analyses have shown that the capacity is adequate for the design basis transients described at the beginning of this section. The bypass flows to the main condenser.

7.7.1.5 Steam Generator Level Control

The steam generator water level is controlled by a digital microprocessor controlled steam generator feedwater control system termed the advanced digital feedwater control system (ADFCS). The ADFCS provides automatic control of the programmed level in the steam generators without the need for operator intervention over the range of power operation. This range of operation extends from the point at which the transition is made from feeding via the preferred auxiliary feedwater system to feeding via the main feedwater system on the Main Feedwater bypass valve (approximately 2-3% power) up to full power. One control system operates on both the Main Feedwater Regulating Valve (MFRV) and Main Feedwater bypass valves without the need for manual action to switch operating modes or switch between valves.

The basic control system functional design is similar to the original analog feedwater control system; however, a number of features have been added to improve the performance of the system. Functional block diagrams of the system are shown in Figures 7.7-14, 7.7-15, and 7.7-16. A feedwater temperature-dependent gain has been added to the narrow-range level regulator as shown in Figures 7.7-14 and 7.7-15. The response of steam generator water level to changes in feedwater flow is a function of feedwater temperature. At low feedwater temperatures and low power levels the level response exhibits more of the classical shrink/ swell effect. This non-minimum-phase response is a destabilizing influence on the feedback control system. Therefore the control system lowers the gain at low feedwater temperature to preserve stability and increases the gain at high feedwater temperature to improve the response of the system. Derivative action has also been added to the level controller to provide some anticipatory action based on the rate of change of level.

The flow regulator has a high-power mode and a low-power mode which is shown in Figure 7.7-15. This is necessary because the feedwater flow and steam flow signals are not usable at low power levels. The switching between these two modes is done automatically within the system and is performed in a bumpless manner without the need for operator action. At low power levels a load index is used as a feed forward signal to anticipate the need for changes in feedwater flow in advance of an actual change in level. The wide-range steam generator water level measurement is used for this purpose. This signal changes with plant load and also leads the response of the narrow-range measurement.

The high-power load regulator uses the standard steam-flow-feed flow mismatch input. However, the loop steam flow signal is compensated with high-pass filtered loop average steam flow to improve the response of the system to steam-flow-induced transients, such as a large load change. Initially, during a large load change, there is a rapid decrease in steam flow. If the compensation on steam flow were not present, this would cause the control system to close the feedwater control valve, which is opposite to the desired response. As was the case with the low power mode load index, the feed flow and steam flow signals will automatically be switched in and out of the system. This mode switching is performed

independently of which valve (Main Feedwater Regulating Valve (MFRV) or Main Feedwater bypass valve) is being used for control.

An additional unique feature of the control system design is the valve lift calculator or the "linearization circuit." The block diagram of this part of the system is shown in Figures 7.7-15 and 7.7-16. The output of the flow regulator is a demanded feedwater flow. The relationship between changes in valve position and changes in feedwater flow is highly nonlinear. It depends on the valve flow characteristic, pressure drop across the system, and system hydraulic characteristics. The linearization circuit calculates the amount that the control valve(s) must be moved to accomplish the change in flow demanded by the control system. The valve lift calculator operates on both the Main Feedwater Regulating Valve (MFRV) and Main Feedwater bypass valves and is independent of the control mode. The Main Feedwater bypass and Main Feedwater Regulating Valves (MFRV) are stroked open sequentially with some overlap. Either of the valves may be operated in manual while leaving the other valve in auto as shown in Figure 7.7-16. The valves are closely coupled through the algorithms in the valve demand portion of the system in order to minimize disturbances on the process (flow and level).

As the plant is taken from low power to high power, the Main Feedwater bypass and Main Feedwater Regulating Valves (MFRV) are opened sequentially. Before the Main Feedwater bypass valve reaches its nominal full-open condition, the control system logic begins to open the Main Feedwater Regulating Valve (MFRV) from its full-closed position. At full power, the valves normally operate in a "split-range" fashion with both valves open as controlled by the system's valve sequencing logic. Therefore, there is no valve "switchover" at a particular power level. The normal sequence can be altered by placing either or both of the valves in manual control. Also, at full power operation, the system can be operated with only the Main Feedwater Regulating Valve (MFRV) valve open by taking manual control of the Main Feedwater bypass valve and closing it.

The feedwater control system includes signal validation for input signals to reduce the probability of a failed sensor causing an upset condition in the plant. The input channel signal validation configuration is shown in Figure 7.7-14. When three channels of a variable are available, the median signal select method is used. In this method, the middle value of the three input values is used as the input to the control algorithms. This will prevent high or low failures of a single input from affecting the control system. When two input channels of a variable are available, an arbitration method is used. In this method, the two inputs are compared, and if they agree to within a certain criterion, they are averaged and the result is sent to the control algorithms. If the two channels disagree significantly, they are compared to an estimate of the variable, which is calculated using other process measurements. The primary input that is closest to the estimate is used in the control system.

The signal validation feature of the feedwater control system allowed elimination of the low feedwater flow reactor trip that was incorporated into the original design of the plant. WCAP 12347 provides justification for elimination of the trip (*Reference 1*).

A summary of the signals input to the advanced digital feedwater control system is as follows:

Process Variable	Channels
Narrow-range steam generator water level	6, 3/loop
Wide-range steam generator water level	6, 3/loop
Steam flow	6, 3/loop
Feedwater flow	6, 3/loop
Feedwater temperature	2, 1/loop
Steam generator pressure	6, 3/loop
Turbine first stage pressure	2
Feedwater header pressure	2
Valve position	4, 1/valve

Controls for the two Atmospheric Relief Valves (ARV) have also been incorporated into the advanced digital feedwater control system. Each Atmospheric Relief Valves (ARV) is now controlled by a validated, median signal-selected steam generator pressure signal (Section 10.3.2.5).

7.7.1.6 Steam Generator Overfill Protection

In a generic letter to licensees, Generic Letter 89-19, on September 20, 1989, the NRC staff identified actions to be taken by licensees related to automatic steam generator overfill protection. Rochester Gas and Electric Corporation's initial response to the generic letter provided overfill protection information as it related to the then existing analog feedwater control system. Upon installation of the new advanced digital feedwater control system (ADFCS) in 1991 (see Section 7.7.1.5), the NRC requested that the original response to the generic letter be updated with regard to the ADFCS. Rochester Gas and Electric Corporation's updated response (*Reference 8*) was accepted by the NRC (*Reference 9*) as confirmation that a satisfactory design for steam generator overfill protection was provided, closing out Generic Letter 89-19 for Ginna Station.

7.7.2 CONTROL SYSTEM EVALUATION

7.7.2.1 Plant Stability

The rod control system is designed to limit the amplitude and the frequency of continuous oscillation of coolant average temperature about the control system setpoint within acceptable values. Continuous oscillation can be induced by the introduction of a feedback control loop with an effective loop gain that is either too large or too small with respect to the process transient response, i.e., instability induced by the control system itself. Because stability is more difficult to maintain at low power under automatic control, no provision is made to provide automatic control below 12.8% of full power.

The control system is designed to operate as a stable system over the full range of automatic control throughout core life. The automatic control rod withdrawal feature of the rod control system has been disabled. The disabled rod withdrawal function will not adversely impact the plant stability.

7.7.2.2 Step Load Changes Without Turbine Bypass

A typical power control requirement is to restore equilibrium conditions, without a plant trip, following a plus or minus 10% change in load demand, over the 12.8% to 100% power range for automatic control. The design must necessarily be based on conservative conditions and a greater transient capability is expected for actual operating conditions. A load demand greater than full power is prohibited by the turbine control load limit devices.

The function of the control system is to minimize the reactor coolant average temperature deviation during the transient within an acceptable value and to restore average temperature to the programmed setpoint within an acceptable time. The automatic control rod withdrawal function of the rod control system has been disabled. The operator may need to manually return the reactor coolant average temperature to the programmed value for step increases in load. Excessive pressurizer pressure variations are prevented by using spray and heaters in the pressurizer.

The margin to overtemperature high delta T reactor trip is of primary concern for the step load changes. This margin is influenced by nuclear flux, pressurizer pressure, and reactor coolant average temperature and temperature rise across the core.

7.7.2.3 Loading and Unloading

Ramp loading and unloading is provided over the 12.8% to 100% power range under automatic control. The automatic control rod withdrawal function of the rod control system has been disabled. The operator will manually withdraw the rods during plant loading. The function of the control system is to maintain the coolant average temperature and the secondary steam pressure as functions of turbine-generator load within acceptable deviation from the programmed values. The minimum control rod speed provides a sufficient reactivity rate to compensate the reactivity changes resulting from the moderator temperature coefficient and the power coefficient.

The coolant average temperature is increasing during loading and there is a continuous in-surge to the pressurizer resulting from coolant expansion. The sprays limit the resulting pressure increase. Conversely, as the coolant average temperature is decreasing during unloading, there is a continuous out-surge from the pressurizer resulting from coolant contraction. The heaters limit the resulting system pressure decrease. The pressurizer level is programmed such that the water level has an acceptable margin above the low level heater cutout setpoint during the loading and unloading transients.

The primary concern for the loading is to limit the overshoot in coolant average temperature to provide sufficient margin to overtemperature high delta T trip.

The automatic load controls are designed to safely adjust the unit generation to match load requirements within the limits of the unit capability and licensed rating.

7.7.2.4 Loss of Load With Turbine Bypass

The reactor control system is designed to accept a turbine trip from 50% power or 50% loss of load. No reactor trip or turbine trip will be actuated. The automatic bypass system is able to accommodate this abnormal load rejection and to reduce the transient imposed upon the reactor coolant system. The reactor power is reduced at a rate consistent with the capability of the rod control system. Manual control is used when the power is below this value. The bypass is removed as fast as the control rods are capable of inserting negative reactivity.

The pressurizer safety valves might be actuated for the most adverse conditions, e.g., the most negative doppler coefficient and the minimum incremental rod worth. The relief capacity of the Pressurizer Power Operated Relief Valves (PORV) is sized large enough to limit the system pressure to prevent actuation of high-pressure reactor trip for the most adverse conditions.

7.7.2.5 Turbine Trip With Reactor Trip

A turbine-generator unit trip above 50% power is accompanied by reactor trip. With a secondary system design pressure of 1100 psia, the plant is operated with a programmed average temperature as a function of load, with the full load average temperature significantly greater than the saturation temperature corresponding to the Main Steam Safety Valve (MSSV) setpoint. This, together with the fact that the thermal capacity in the reactor coolant system is greater than that of the secondary system, requires a heat sink to remove heat stored in the reactor coolant to prevent actuation of Main Steam Safety Valves (MSSV) for turbine and reactor trip from full power.

This heat sink is provided by the combination of controlled release of steam to the condenser and by makeup of cold feedwater to the steam generators. The turbine bypass system is controlled from the reactor coolant average temperature signal whose reference setpoint is reset upon trip to the no-load value. Turbine bypass actuation must be rapid to prevent Main Steam Safety Valve (MSSV) actuation. With the bypass valves open the coolant average temperature starts to reduce quickly to the no-load setpoint. A direct feedback of reactor coolant average temperature acts to proportionately close the valves to minimize the total amount of steam bypassed.

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

Additional feedwater makeup is then controlled manually to restore and maintain steam-generator level while maintaining the reactor coolant at the no-load temperature. Residual heat removal (manually selected) is maintained by the steam-generator pressure controller which controls the amount of steam dump to the condensers. This controller operates the same bypass valves to the condensers which are controlled by coolant average temperature during the initial transient following turbine and reactor trip.

The pressurizer pressure and level fall very fast during the transient resulting from the coolant contraction. If heaters become uncovered following a reactor trip by the automatic low level shutoff, the chemical and volume control system will provide full charging flow to restore water level in the pressurizer. Heaters are then turned on after the pressurizer level has been restored to heat up pressurizer water and restore pressurizer pressure to normal.

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

7.7.2.6 Control Rod Misalignment

7.7.2.6.1 General

Ginna Station does not have fixed in-core instrumentation. Measurements of core power distribution necessary to provide information to the operator for the control of axial power distribution will be performed by the out-of-core power range nuclear instrumentation. In addition, protection of the core from abnormal axial power distributions is achieved by this same out-of-core nuclear instrumentation. The protection system functions that achieve this protection have been described in Section 7.2. The analytical justification for the use of out-of-core nuclear instrumentation in the control system and the protection system together with supporting experimental data has been reported in WCAP 7208, October 1968.

Abnormal power distribution can also be caused by rods out of position with respect to other bank positions for rods in the same group. The operation of control rods is supervised by the operator who is provided with continuous indication of all control rods. The operator is assisted in this supervision by a rod deviation monitoring program in the computer that will alarm whenever a rod deviates from the bank position by more than a preset amount. In the event the signal for the position of any control rod is lost or suspected of a malfunction, the operator can monitor the core power distribution by signals from the out-of-core nuclear instrumentation, primary coolant system temperature instrumentation, in-core thermocouples, and the in-core flux monitoring system. The checks and periodic tests the operator performs under this condition of plant operation, together with experimental data which demonstrates the sensitivity of the various instrumentation systems to rod misalignment, are presented below.

7.7.2.6.2 Consequences of Rod Misalignment

As discussed below, the immediate consequences of control rod misalignment are tolerable, i.e., in no case would the core safety limits be exceeded. The operator would be made aware of rod misalignment by the direct rod position indication system and associated deviation alarms and would take corrective action as necessary. If the rod position indicator is out of service, the effects of rod misalignment can be noted by checking for normal indications in other variables as discussed in Section 7.7.2.6.5. An emergency procedure has been prepared for the case of a rod position indicator being out of service.

7.7.2.6.3 Analysis of Control Rod Misalignment

Rod cluster misalignment is defined as one cluster being lower than its bank or one cluster being higher than its bank.

If one control rod cluster is below its bank, the hot-channel factors F_Q and $F_{\Delta H}$ remain within design limits. If one control rod cluster is above its bank the design hot-channel factor limits may, in extreme cases, be exceeded. However, even complete rod misalignment (control rod 12 ft out of alignment with its bank) does not result in exceeding core safety limits in steady-state operation at rated power.

7.7.2.6.4 Redundant Checks for Control Rod Malfunction

Analysis has shown that malpositioning of a control rod will not result in exceeding the core safety limits during MODES 1 and 2. In extreme cases, however, core design margins are not maintained, i.e., design hot-channel factors are exceeded. Plant Technical Specifications are therefore placed on control rod positioning. Allowable hot-channel factors are also prescribed in the Technical Specifications.

Monitoring long-term trends in hot-channel factors with core burnup is the responsibility of the reactor engineering staff. The shift operators are responsible at all times for monitoring control rod position and taking corrective action as necessary in the event that a malfunction of the rod control system occurs.

7.7.2.6.4.1 Operator Checks

In order for the operator to fulfill the responsibility for verifying proper rod positioning, several independent and redundant instrumentation systems are provided. The usage of these systems is outlined below, along with appropriate operator action in the event of alarms or abnormal indications.

a. **Rod position indication system.** Each control rod position is continuously indicated on a color cathode ray tube in the control room on the main control board. The cathode ray tube is a component of the microprocessor rod position indication system, which provides input to the cathode ray tube display by a digital detector assembly for each rod (see Section 7.7.1.2.6).

   The plant computer also monitors each position signal and alarms if deviation from the bank demand signal occurs.

b. **Nuclear instrumentation system.** The total signal (top plus bottom detector) for each of the four sets of power range excore nuclear detectors is automatically compared to the average of all channels and an alarm is generated if channel deviation occurs. This alarm alerts the operator to short-term trends which would be indicative of a power tilt.

   Additional symmetric checks and alarms are performed by the plant computer.

   Technical Specifications provide the required actions for rod position indication or step counter inoperability.

c. **Core outlet thermocouples.** Two core outlet thermocouple temperatures can be readily compared, one in the immediate vicinity of the non-indicated rod, and the other in a symmetric location far away from the control rod. Excessive differences between the two temperatures would be indicative of control rod malfunction. In the core there are at least two pairs of symmetric thermocouples suitable for monitoring any suspect control rod.

   In addition to this operator check, during normal operation the plant computer also monitors all thermocouples and alarms abnormal conditions.

d. **In-core movable detector system.** Axial movable detector traces can easily be taken by the shift operators and require no data analysis or evaluation. Just as for the thermocouple check above, axial traces in two symmetric locations would be compared. One trace would be near the suspect rod, and the other in a symmetric location further away. If the deviation between the two traces is excessive, control rod malfunction is indicated.

   At least two pairs of symmetric movable detector locations are available for each suspect control rod in the core.

7.7.2.6.4.2 Additional Periodic Tests

In addition to routine operator surveillance and the checks described above, normal plant instructions and procedures include the following tests to be performed on a periodic basis. These also constitute independent checks of correct control rod operation.

a. **Rod exercise test.** As required by the Technical Specifications, any rod not fully inserted is exercised periodically to verify correct operation. In the event a rod position indicator is out of service, positive verification that the rod has moved can be accomplished by monitoring the neighborhood of the non-indicated rod by in-core detectors.

b. **In-core power distribution maps.** Approximately once a month in MODES 1 and 2, the Technical Specifications require that a complete core power distribution map be made by use of the in-core movable detectors. Additional complete or partial maps may be made whenever desired. Any misaligned rod that has a significant effect on hot-channel factors or burnup would be noticeable from the results of these maps.

7.7.2.6.4.3 Details of Instrumentation System

Pertinent details of the power range nuclear instrumentation and in-core movable detectors are discussed in the following sections.

7.7.2.6.4.4 Power Range Nuclear Instrumentation

The power range nuclear instrumentation system is described in Section 7.7.3.

There are four channels, each consisting of two long ion chambers (top and bottom detectors). These channels are on the 45 degree and 135 degree axis with respect to the core. Detector position and analog circuitry is shown in Figures 7.7-7, 7.7-8, and 7.7-9.

Two types of signals are provided from each channel: a calibrated power signal, and a calibrated current signal from each of the two detectors.

The calibrated current signal represents the normalized signal from each detector. At rated full power, with nominal full power conditions and a flat power distribution, each calibrated current signal is set equal to 100%. In this way, detector sensitivity and geometry effects are cancelled. This calibration is done by instrument technicians on the basis of the plant startup tests and results of subsequent in-core power distribution studies. The total power signal is calibrated by the operators each day (or more frequently if necessary) such that all channels indicate the total reactor power as determined by calorimetric measurements.

The delta-current indicators provide information to the operator on axial power distribution. The calibrated current signals are also used in the Reactor Trip System (RTS) for reduction of the delta T reactor trips if adverse axial power distribution exists.

The total power signal is used for the nuclear overpower reactor trip. A comparator and deviation alarm alerts the operator to channel deviations. In MODES 1 and 2, errors caused by power distribution variations would affect all channels by the same amount. Therefore, this alarm indicates an abnormality, either a power tilt or a channel failure, and alerts the operator to check for abnormalities in other instrumentation.

The design specification for the power range channels calls for ±1% reproducibility. Somewhat better reproducibility is expected for day-to-day operation. Including readout error and normal symmetric variations, the calibrated signals from symmetric locations are expected to follow one another to within 2%.

7.7.2.6.4.5 Thermocouples

Thirty-nine chromel-alumel thermocouples are threaded into guide tubes that penetrate the reactor vessel head through seal assemblies (36 terminate at the exit flow end of the fuel assemblies and three are located in the upper head). The thermocouples are enclosed in stainless steel sheaths within the above tubes to allow replacement if necessary.

Thermocouple readings are indicated in the control room on scanning digital display units, and selected core exit thermocouples may be removed from scan if they are inoperable or malfunctioning. If removed from scan, the thermocouple readings are not displayed on the local digital display units or on the plant process computer system (PPCS). The location of the thermocouples is shown in Figure 7.7-8.

Thermocouple data is continually archived by the plant process computer system (PPCS).

Based on operational experience with similar thermocouple systems, the thermocouple reproducibility is expected to be within ±1/2°F. Including allowance for flow mixing and normal variations in temperature profiles, the normal variation between symmetric thermocouples is expected to be within 3°F.

7.7.2.6.4.6 In-Core Movable Detectors

The movable detector flux monitoring system is described in Section 7.7.4. These miniature neutron flux detectors are remotely positioned in the core and provide remote readout for flux mapping. Retractable thimbles are provided into which the miniature detectors are driven. The 36 thimble locations are shown in Figure 7.7-8.

Three movable detectors are provided, with separate drives and a common readout at the flux map system console. This allows three locations to be monitored simultaneously. The three detectors are cross-calibrated to give the same readout in the same thimble. This cross-calibration is done during each flux map.

The control room flux map system console contains the necessary equipment for control and position indication. A "flux-map" consists, briefly, of selecting flux thimbles in given fuel assemblies at various core locations. The detectors are driven or inserted to the top of the core and stopped automatically. A plot of position versus flux level is initiated with the slow withdrawal of the detectors through the core from the top to a point below the bottom. In a similar manner other core locations are selected and plotted.

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

Experience has shown that flux traces in symmetric locations are virtually identical in MODES 1 and 2 and deviate markedly when a control rod is withdrawn or inserted near one location.

7.7.2.6.4.7 Summary

Routine operator surveillance of the rod position indicators and nuclear instrumentation system, supplemented by operational alarms on rod position deviation and nuclear power range channel deviation, provide redundant checks of control rod position. These checks are sufficient to ensure, by two independent means, that a malpositioned control rod would be quickly noticed and corrective action taken as required for control rod malfunction.

In the event that this routine monitoring cannot be performed because of instrument malfunction, backup checks can be readily carried out by the shift operators using in-core movable detectors and/or thermocouples. Prescribed limits, based on operating history, can be specified for the allowable deviation between detectors at symmetric locations. Thus, there is no requirement for data analysis and evaluation on the part of the operator.

The expected maximum variations between symmetrically located detectors is summarized in Table 7.7-3 for MODES 1 and 2. Similar values for complete misalignment between a control rod and its bank are listed for comparison.

7.7.2.6.5 Expected Instrument Response to Control Rod Misalignment Ginna Station

The placement of in-core and ex-core instrumentation relative to the control rod placement is shown in Figure 7.7-8. For all control rod clusters, at least one core outlet thermocouple and one movable detector channel are located in adjacent fuel assemblies.

Instrument response to misaligned control rods were determined during the plant initial startup tests. As shown by operating plant data, asymmetric variations in thermocouple temperatures of only a few degrees can be used as a reliable indication of abnormal radial power tilts.

7.7.2.6.6 Plant Startup Tests

Extensive core physics tests were conducted as part of the plant initial startup tests to determine the effects of misaligned rods (see Section 14.6.1). These included rod insertion tests, in which each rod or its symmetric equivalent was fully inserted with other rods essentially fully withdrawn. Rod withdrawal tests were also made for selected rods in which the rod was fully withdrawn while its bank was deeply inserted. This included all rods in control banks C and D.

Test measurements included rod worths and hot-channel factors based on in-core and thermocouple maps, and the response of out-of-core nuclear instrumentation. The hot-channel factor measurements were to verify that core limits would not be exceeded in steady-state operation as an immediate result of any malpositioned rod. The measured response of core thermocouples and nuclear instrumentation was recorded and attached to the operating instructions as a guide for checking rod alignment if a rod position indicator was out of service.

7.7.3 NUCLEAR INSTRUMENTATION SYSTEM

7.7.3.1 Design Basis

The following design criterion was used during the licensing of Ginna Station. It was included in the Atomic Industrial Forum (AIF) version of proposed criteria issued by the AEC for comment on July 10, 1967 (see Section 3.1.1). Conformance with 1972 General Design Criteria of 10 CFR 50, Appendix A, is discussed in Section 3.1.2. The criteria discussed in Section 3.1.2 as they apply to the nuclear instrumentation system includes GDC 13 and GDC 19. Conformance to IEEE 279-1971 Standard is discussed in Section 7.1.2.2.

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

The nuclear instrumentation system is provided to monitor the reactor power from source range through the intermediate range and power range up to 120% full power. The system provides indication, control, and alarm signals for reactor operation and protection.

The operational status of the reactor is monitored from the control room. When the reactor is sub-critical and during approach to criticality (i.e., during MODE 6, "Refueling" through MODE 3 "Hot Shutdown", and during MODE 2 "Startup"), the relative reactivity status (neutron source multiplication) is continuously monitored by two source range proportional counter detectors located in instrument wells within the primary shield and adjacent to the reactor vessel. Two source range detector channels are provided to supply neutron source multiplication information during the above mentioned plant modes. A reactor trip is actuated from either channel if the neutron flux level becomes excessive.

The source range channels are checked prior to operations in which criticality may be approached. A source of neutrons is necessary to provide at least the minimum count rate (> 5 cps) required for startup operations. The discrete (Sb-Be) secondary sources initially installed were removed from the core during the EOC 20 refueling outage. The neutron emissions which

occur naturally in burnt fuel are now utilized as the neutron source. These neutron emissions are produced primarily by spontaneous fission of Cm-242 and Cm-244.

Any appreciable increase in the neutron source multiplication, including that caused by the maximum physical boron dilution rate, is slow enough to give ample time to start corrective action (boron dilution stop and/or emergency boron injection) to prevent the core from becoming critical.

When the reactor is critical, means for showing the relative reactivity status of the reactor is provided by control bank positions displayed in the control room. The position of the control banks is directly related to the reactivity status of the reactor when at power and any unexpected change in the position of the control banks under automatic control or change in the coolant temperature under manual control provides a direct and immediate indication of a change in the reactivity status of the reactor. Periodic samples of the coolant boron concentration are taken. The variation in concentration during core life provides a further check on the reactivity status of the reactor including core depletion.

High-nuclear-flux protection is provided both in the power and intermediate ranges by reactor trips actuated from either range if the neutron flux level exceeds trip setpoints. When the reactor is critical, the best indications of the reactivity status in the core (in relation to the power level and average coolant temperature) is the control room display of the rod control group position.

7.7.3.2 System Design

The nuclear instrumentation system provides the detectors and electronic circuitry necessary to monitor flux levels from outside the reactor vessel. Indication is provided over the range of 10^{-1} to 10^{11} n/cm^2-sec. The lowest range (source range) covers six decades of neutron flux. The next range (intermediate range) covers eight decades of flux and overlaps both the source range and power range. The highest level of indication (power range) covers approximately three decades of neutron flux. The three instrumentation ranges are provided with overlap between adjacent ranges so that continuous readings will be available during transition from one range to another, as indicated in Figure 7.7-10.

Triaxial cable is used for all interconnections from the detector assemblies to the instrumentation in the control room. The electronic equipment for each of the source, intermediate, and power range channels is contained in a drawout panel mounted adjacent to the main control board. The detector assemblies are located in instrument wells around the reactor as shown in the (plan view) lower right hand corner of Figure 7.7-6.

The neutron detectors are positioned in detector assembly containers by means of a linear, high-density moderator insulator. The detector and insulator units are packaged in a housing that is inserted into the guide thimbles.

The detector assembly is electrically isolated from the guide thimble by means of insulated standoff rings.

7.7.3.2.1 Source Range Description

The source range is composed of two independent channels, N-31 and N-32. The neutron detectors are proportional counters that are filled with boron trifluoride (BF_3) gas.

Neutron flux, as measured in the primary shield area, produces current pulses in the detectors. These preamplified pulses are applied to transistor amplifiers and discriminators located in the control room. The preamplifiers are located outside the reactor containment.

The channels indicate the source range neutron flux and provide high flux level reactor trip and alarm signals to the reactor control and protection system. The reactor trip signal is manually blocked when a permissive signal from the intermediate range is available. They are also used at shutdown to provide an audible alarm in the control room of any inadvertent increase in reactivity. An audible count rate signal is used during initial phases of startup and is audible in both the reactor containment and control room. The range of the source range channels is 10^0 to 10^6 cps.

The pulse integrator derives an analog signal, proportional to the logarithm of the number of pulses per unit time, as received from the output of the preamplifier. This unit amplifies the neutron pulse, provides gamma and noise discrimination, shapes the output pulse, performs log integration of the pulse rate to determine the count rate, and amplifies the log integrator output for indication, recording, control, and automatic data logging.

Each source range contains two bistable trip units. Both units trip on high flux level but one is used during shutdown to alarm reactivity changes and the other provides overpower protection during shutdown and startup. The shutdown alarm unit is blocked manually approximately two decades above shutdown. When the input to either unit is below its setpoint, the bistable is in its normal position and assumes a FULLY ON status. When an input from the log amplifier reaches or exceeds the setpoint, the unit reverses its condition and goes FULLY OFF. The output of the reactor trip unit controls a relay in the Reactor Trip System (RTS).

Power supplies furnish the positive and negative voltages for the transistor circuits and alarm lights and the adjustable high voltage for the neutron detector.

A test calibration unit can insert selected test or calibration signals into the preamplifier channel input or the log amplifier input. A set of precalibrated level signals is provided to perform channel tests and calibrations. An alarm is registered on the main control board annunciator whenever a channel is being tested or calibrated. A trip bypass switch is also provided to prevent a reactor trip during channel test under certain reactor conditions.

The neutron detector high-voltage cutoff assembly receives a trip signal when a one-of-two matrix controlled by intermediate range channel flux level bistables and manual block condition are present and disconnects the voltage from the source range channel high voltage power supply to prevent operation of the BF_3 counter outside its design range. High voltage and reactor trip circuits are reactivated automatically when two of the intermediate range signals are below the permissive trip setting.

Mounted on the front panel of the source range channel is a neutron flux level indicator (1 to 10^6 cps). Mounted on the control board is a neutron count rate level indicator (1 to 10^6 cps). Isolated neutron flux signals are available for recording by the nuclear instrumentation system recorder, by the data logger, and for startup rate computation. The startup rate for each channel is indicated at the main control board in terms of decades per minute over the range of -0.5 to 5.0 decades/min. The isolation network for these signals prevents any electrical malfunction in the external circuitry from affecting the signal being supplied to the flux level bistables. The signals for channel test, high neutron flux at shutdown, and source range reactor trip are alarmed on the main control board annunciator. In addition, there are annunciators for the following source range conditions: manual block of high-flux level at shutdown, loss of high voltage, and individual nuclear instrumentation system trip bypass.

7.7.3.2.2 Intermediate Range Description

The intermediate range is composed of two independent channels. The lowest level of intermediate range indication corresponds to ~10^3 cps on the source range and the highest level corresponds to full power operation. The intermediate range channels measure neutron flux in the range of 10^{-11} to 10^{-3} amp. The intermediate range has control and protective functions.

The intermediate range neutron detectors are compensated ionization chambers that sense thermal neutrons in the range from 2.5 x 10^2 to 5 x 10^{10} neutrons/cm^2-sec and have a nominal sensitivity of 7.6 x 10^{-14} amp per neutron/cm^2-sec. They produce a corresponding direct current of 10^{-11} to 10^{-3} amp. These detectors are located in the same detector assemblies as the proportional counters for the source range channels.

Direct current from the ion chambers is transmitted through triaxial cables to transistor logarithmic current amplifiers in the nuclear instrumentation equipment.

The logarithmic amplifier derives a signal proportional to the logarithm of the current as received from the output of the compensated ion chamber. The output of the logarithmic amplifier provides an input to the level bistables for reactor protection purposes and source range cutoff. The bistable trip units are similar to those in the source range. The trip outputs can be manually blocked after receiving a permissive signal from the power range channels. On decreasing power, the intermediate range trips for reactor protection are automatically inserted when the power range permissive signal is not present.

Low voltage power supplies contained in each drawer furnish the necessary positive and negative voltages for the channel electronic equipment. Two medium voltage power supplies, one in each channel, furnish compensating voltage to the two compensated ion chambers.

The high voltage for the compensated ion chambers is supplied by separate power supplies also located in the intermediate range drawers.

On the front panel of the intermediate range channel cabinet and on the control board are mounted a neutron (log N) flux level indicator (10^{-11} to 10^{-3} amp).

Isolated neutron flux level signals are available for recording, automatic data logging, and startup rate computation. The startup rate for each channel is indicated at the main control board in terms of decades per minute over the range -0.5 to 5.0 decades/min.

Channel test and reactor trip signals are alarms on the main control board annunciator. The latter signal is sent to the Reactor Trip System (RTS).

7.7.3.2.3 Power Range Description

The power range portion of the nuclear instrumentation system consists of four channels. The power range instrumentation covers approximately three decades and overlaps the intermediate range. The power range utilizes linear instead of log indicators. Each channel and individual detector is continually compared with the others to alert the operator to a possible flux imbalance.

Four detector assemblies are used in the power range. They are long ionization chambers approximately equal to the core height, in which the inner electrodes are divided into two equal sections to supply in effect a total of eight separate ionization chambers approximately one-half the core height. The eight uncompensated (guard-ring) ionization chambers sense thermal neutrons in the range from 5×10^{2} to 1×10^{11} neutrons/cm^{2}-sec.

Each has a nominal sensitivity of 3.1×10^{-13} amp per neutron/cm^{2}-sec. The four long ionization chamber assemblies are located in vertical instrument wells adjacent to the four "corners" of the core. The assembly is manually positioned in the assembly holders and is electrically isolated from the holder by means of insulated standoff rings.

There are three sets of power range measurements. Each set utilizes four individual currents as follows:

A. Four currents directly from the lower sections of the long ionization chambers.

B. Four currents directly from the upper sections.

C. Four total currents of A. and B. above, equivalent to the average of each section.

For each of the four currents in A. and B., the current measurement is indicated directly by a microammeter and isolated signals are available for data logging and control console indication and recording. Analog signals proportional to individual currents are transmitted through buffer amplifiers to the overtemperature and overpower delta T channels and provide automatic reset of the trip point for these protection functions. The total current, equivalent to the average, is then applied through a linear amplifier to the bistable trip circuits. The amplifiers are equipped with gain and bias controls for adjustment to the actual output corresponding to 100% rated reactor power.

Each of the four amplifiers also provides amplified isolated signals to the main control board for indication and for use in the reactor control system. Each set of bistable trip outputs is operated as a two-out-of-four coincidence to initiate a reactor trip. Bistable trip outputs are provided at low and high power setpoints depending on the operating power. To provide more protection during startup operation, the low power setpoint is used. The trip is manually

blocked after a permissive condition is obtained by two-of-four power range channels. The high power trip bistable is always active. Power Range trip functions may be bypassed during surveillance testing for an individual channel.

The four amplifier signals corresponding to C. above are supplied to circuits that compare a referenced channel output with the corresponding signal from the other channels. Alarms are provided to present deviations that might be indicative of quadrant flux asymmetries.

The overpower trip will be set so that, for operating limit reactor conditions concurrent with the maximum instrumentation and bistable setpoint error, the maximum reactor overpower condition will be limited to 115%. This limit is accomplished by the use of solid-state instrumentation and long ionization chambers that permit an integration of flux external to the core over the total length of the core, thereby reducing the influence of axial flux distribution changes due to control rod motion.

The ion chamber current of each detector is measured by sensitive meters with an accuracy of 0.5%. A shunt assembly and switch in parallel with each meter allows selection of one of four meter ranges. The available ranges are 0.1, 0.5, 1, and 5 mA. The shunt assemblies are designed in such a manner that they will not disconnect the detector current to the summing assembly upon meter failure or during switching. An isolation amplifier provides an analog signal proportional to ion chamber current for data logging and delta flux indication. A test calibration unit provides necessary switches and signals for checking and calibrating the power range channels.

7.7.3.2.4 Dropped Rod Protection

As backup to the primary protection for the dropped control rod accident, the rod bottom signal, an independent detection means is provided using the out-of-core power range nuclear channels that is effective even if one of the channels is out of service. The dropped-rod sensing unit contains a difference amplifier that compares the instantaneous nuclear power signal with an adjustable power lag signal and responds with a trip signal to the bistable amplifier when the difference exceeds a preset adjustable amount. The signal initiates protective action in the form of blocking of rod withdrawal[a].

7.7.3.2.5 Audio Count Rate Channel

The audio count rate channel provides audible source range information during MODE 6 (Refueling) operations in both the control room and the reactor containment. In addition, this channel signal is fed to a scaler-timer assembly that produces a visual display of the count rate for an adjustable sampling period.

7.7.3.2.6 Recorders

One multi-channel paperless recorder is mounted on the main control board for recording the complete range of the source, intermediate, and power channels. All 8 NIS channels are connected to the recorder for continuous monitoring.

---

a. The automatic rod withdrawal function of the reactor control system has been disabled. The block automatic rod withdrawal function from the microprocessor rod position indication (MRPI) on a rod drop is no longer used.

7.7.3.2.7 Power Supply

The nuclear instrumentation system is powered by four independent vital bus circuits (see Section 8.3).

7.7.3.2.8 Equipment Locations

The plant locations of the detectors are shown in the (plan view) lower right-hand corner of Figure 7.7-6. The view also indicates the position of the detectors relative to the core center plane.

7.7.3.3 System Evaluation

The sensitivity of the reactor neutron detectors is illustrated in Figure 7.7-10.

The nuclear instrumentation draws its primary power from battery-backed vital instrument buses whose reliability is discussed in Section 8.3.

Loss of nuclear instrumentation power would result in the initiation of all reactor trips that were operational prior to the power loss. In addition, all trips that were blocked prior to loss would be unblocked and initiated also. Single bus failures do not result in reactor trips since only one channel is powered from each bus.

The requirements established for the Reactor Trip System (RTS) apply to the nuclear instrumentation. All channel functions are independent of every other channel.

7.7.4 IN-CORE INSTRUMENTATION

7.7.4.1 Design Basis

The in-core instrumentation is designed to yield information on the neutron flux distribution and fuel assembly outlet temperatures at selected core locations. Using the information obtained from the in-core instrumentation system, it is possible to confirm the reactor core design parameters and calculated hot-channel factors. The system provides means for acquiring data and performs no operational plant control.

7.7.4.2 System Design

7.7.4.2.1 General

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

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

maximum core capability.

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

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

7.7.4.2.2 Thermocouples

Chromel-alumel thermocouples are threaded into guide tubes that penetrate the reactor vessel head through seal assemblies (36 terminate at the exit flow end of the fuel assemblies and three are located in the upper head). A simplified sketch of a typical thermocouple is shown in Figure 7.7-12 (Sheet 2). The thermocouples are enclosed in stainless-steel sheaths within the above tubes to allow replacement if necessary. Thermocouples are split into two trains outside of containment and run to separate digital scanning displays in the control room. The displays provide isolated outputs to the plant process computer system (PPCS) as required for MODES 1, 2, and 3. The displays, cable, containment penetrations, and connectors at the reactor head are seismically and environmentally qualified. Operating range of the thermocouple system, including displays, is 0-2300°F. The support of the thermocouple grid tubes in the upper core support assembly is described in Section 3.9.5.1.3.

7.7.4.2.3 Movable Miniature Neutron Flux Detectors

Three detector cable assemblies are used in the system, one for each drive. Each cable includes a miniature fission chamber detector, mineral insulated coaxial cable, and hollow helix wrapped drive cable. The coaxial cable is threaded through the hollow drive cable and terminated at the drive unit with a subminax coaxial connector. The stainless steel detector shell is welded to the end of the drive cable and coaxial cable. Three fission chamber detectors (employing $U_3 0_8$ which is approximately 90 to 93% enriched in Uranium-235) can be remotely positioned in retractable guide thimbles to provide flux mapping of the core. The stainless-steel detector shell is welded to the leading end of the helical-wrap drive cable and the stainless steel sheathed coaxial cable. Each detector is designed to have a minimum thermal neutron sensitivity of 1.0×10^{-17} amp/nv and a maximum gamma sensitivity of 3×10^{-14} amp/R-hr. Operating thermal neutron flux range for these probes is 1×10^{11} to 5×10^{13} nv. A simplified sketch of a typical basic system for the insertion of these detectors is shown in Figures 7.7-11 and 7.7-13. Retractable thimbles into which the miniature detectors are driven are pushed into the reactor core through conduits that extend from the bottom of the reactor vessel down through the concrete shield area and then up to a thimble seal zone.

The thimbles are closed at the leading ends, are dry inside, and serve as the pressure barrier between the reactor water pressure and the atmosphere.

Mechanical seals between the retractable thimbles and the conduits are provided at the seal table.

During reactor operation, the retractable thimbles are stationary. They are extracted downward from the core during MODE 6 (Refueling) to avoid interference within the core. A space above the seal table is provided for the retraction operation.

The Detector Drive System consists of three drive units, three 6-path transfer devices, three 15-path transfer devices, and the associated limit and Transfer Insertion Switches (TIS).

The drive units are mounted on separate raised platforms in Containment (Intermediate Level). The 6-path transfer devices are mounted on a support beam in front of the drive units. The Safety Limit switches and Withdraw Limit switches are mounted in the tubing run between the drive unit output and the 6-path transfer device input. The 15-path transfer devices are mounted on a movable assembly in front of and below the 6-path transfer devices.

For refueling, the three tubing connections between the 6-path devices and the 15-path devices are disconnected, and the 36 tubing runs between the output of the 15-path transfer devices and the manual isolation valves are removed.

The assembly holding the three transfer devices is rolled out of the way and stored in the refueling position. This opens access to the seal table. The manual isolation valves are removed and the thimble tables are pulled out of the seal table far enough to allow removal of the fuel assemblies without interference from the thimble tubes (typical simplified sketch of the arrangement shown in Figure 7.7-13). The drive system pushes hollow helical-wrap drive cables into the core with the miniature detectors attached to the leading ends of the cables and small diameter sheathed coaxial cables threaded through the hollow centers back to the trailing ends of the drive cables. Each drive assembly generally consists of a gear motor that pushes a helical-wrap drive cable and detector through a selective thimble path by means of a special drive box and includes a storage device that accommodates that total drive cable length. Further information on mechanical design and support is described in Section 3.9.5.1.3 .

7.7.4.2.4 **Control and Readout System**

The Flux Mapping Console (FMC) located in the Main control room provides the means for inserting the miniature neutron detectors into the reactor core and withdrawing the detectors at a selected speed while displaying induced flux level versus detector position and collecting and storing data. The FMC is the heart of the Flux Mapping System (FMS) equipment. This console is installed in three cabinet bays in the main control room that contain the electronic circuits required to obtain a flux map. The first bay of the cabinet contains a DIN rail assembly with a power distribution assembly, power supply and the input/output (I/O) terminal blocks for drive A. The second bay of the cabinet contains the Human Machine Interface (HMI) subsystem equipment, the Keithley Sourcemeters, and the Real Time Controller (RTC) subsystem equipment. The third bay of the cabinet contains a DIN rail assembly with I/O terminal blocks and a power supply for drives B and C. The 6-path and 15-path transfer devices are used to route a detector into any one of up to 36 selectable paths. A total of 36 manually operated isolation valves allows free passage of the detector and drive wire when open and prevents steam leakage from the core in case of a thimble rupture

when closed. A path common to each group of flux thimbles is provided to permit cross calibration of the detectors.

A flux map consists, briefly, of selecting flux thimbles in given fuel assemblies at various core quadrant locations. The detectors are driven or inserted to the top of the core and stopped automatically. An x-y plot (position versus flux level) is initiated with the slow withdrawal of the detectors through the core from the top to a point below the bottom. In a similar manner other core locations are selected and plotted.

Each detector provides axial flux distribution data along the center portion of a fuel assembly. This data is then processed to obtain a core flux map.

7.7.5 REACTOR COOLANT TEMPERATURE INDICATION

The reactor coolant system temperature provides indication of the system heat content, power, and core reactivity balance. Temperature is measured by resistance temperature detectors and is used to control the Atmospheric Relief Valves (ARV), control rods, and pressurizer level. The T_{AVG} and delta T signals generated by the temperature instruments are used by the Reactor Trip System (RTS) to generate reactor trips. Alarms are generated to alert the operator to possible problem conditions.

There are 11 resistance temperature detector locations utilized in each reactor coolant system loop. Four (T_{cold}) are direct immersion 510°F to 590°F detectors; Four (T_{hot}) are direct immersion 540°F to 650°F detectors; The T_{cold} and T_{hot} detectors provide input to the narrow range (540°F to 620°F) T_{avg} temperature channels and 0-85°F ΔT temperature channels. Two are direct immersion, wide-range (0°F to0 700°F), dual-element detectors; and one is a wide-range (50°F to 650°F) detector installed in a thermowell.

The narrow-range temperature indication system for the reactor coolant system loops provides high accuracy, fast responding indication of loop average temperature (T_{AVG}) and hot-leg minus cold-leg temperature difference (delta T) necessary for various reactor control and protection functions.

The narrow-range temperature is measured by four resistance temperature detectors in each loop hot leg and four resistance temperature detectors in each loop cold leg (16 total). The need for faster responding temperature signals dictated the need for direct immersion or wet-bulb type resistance temperature detectors. An immersion type resistance temperature detector results in a higher probability for coolant system leaks and the system must be depressurized and drained to allow replacement.

Plant average T_{AVG} is computed from the average of the four T_{AVG} channel values, displayed on a recorder, and used to generate alarms. Plant average T_{AVG} also sends a control signal to the automatic rod control system, pressurizer level program, steam dump control system, rod insertion limit computer, and the Main Feedwater Regulating Valves (MFRV).

Plant average delta T is computed from the average of the four delta T channel values, and provides a deviation alarm and an input to the rod insertion limit computer.

Wide-range reactor coolant system temperature is measured by one direct immersion, dual-element detector (0°F to 700°F) in each hot leg and cold leg and by one thermowell mounted detector (50°F to 650°F) in each cold leg (six total). The wide-range reactor coolant loop temperature measurement system provides hot leg and cold leg temperature signals, which are input to redundant hot and cold leg temperature displays, the subcooling monitor, the Low Temperature Overpressure Protection (LTOP) System, and the reactor vessel level indication system.

The wide-range temperature indication range (0°F to 700°F) is adequate to monitor transients and heatup and cooldown operations. The temperature is displayed on a 3-pen recorder located on the main control board left section, on indicators in the main control board and the intermediate building emergency local instrument panel, and on the plant process computer system.

7.7.6 PLANT PROCESS COMPUTER SYSTEM AND SAFETY ASSESSMENT SYSTEM

7.7.6.1 General

The plant process computer system (PPCS)/safety parameter display system (SPDS) is an integrated data acquisition and display system. The PPCS has hardcopy output devices. The PPCS/SPDS satisfies the performance requirements of NUREG 0696, as modified by NUREG 0737.

The PPCS/SPDS computer system is not designed to perform any control functions. The system is capable of operation during all plant conditions except a seismic event. During a seismic event, the main control board will provide critical parameter display in the event of loss of nonseismic equipment. MUX cabinets 1-4 are powered from the technical support center uninterruptible power supply. Breakers and fuses are provided to protect the multiplexers (MUX) in the event of electrical faults.

In 2001, the plant process computer system (PPCS) and safety assessment system (SAS) were replaced with an integrated advanced technology system (*Reference 11*). The SAS, now referred to as the safety parameter display system (SPDS), is part of the plant process computer system (PPCS). Redundancy is maintained, since there are two independent PPCS systems, and the SPDS processing and display functions can be accessed from any of the several PPCS monitors in the control room. There are two major differences between the former SAS and the new SPDS. The diagnostic "AIDS" bars were removed. These bars were not required by regulation, and could provide misleading information for some accident scenarios. Also, the continuous monitoring function of the SPDS is accomplished by an audible and visual alarm on the PPCS monitor. These alarms alert the operator that a parameter on the top-level display of the SPDS has reached a predetermined value. The operator is administratively directed to display the appropriate SPDS screen. In addition, the top-level display automatically displays on the terminal located on the desk of the head control operator when a reactor trip occurs. Manual action by the head control operator is required to remove this display.

There are six multiplexer (MUX) cabinets. When redundant field inputs for a parameter are available, they are assigned to different MUX cabinets. This minimizes the effect of a MUX failure on the parameter.

The three MUX cabinets in the relay room are seismically qualified and use input cards, which provide electrical isolation sufficient to prevent any credible voltage excursion from propagating to the Reactor Trip System (RTS) and Engineered Safety Features Actuation System (ESFAS) circuits from other inputs via the multiplexer. The remaining three MUX cabinets are located in the Turbine and Intermediate (cleanside) Buildings, and Station 13A. These new remote MUX cabinets allow for additional plant parameters to be displayed on the PPCS.

All PPCS/SPDS alarms and displays will be viewable on CRTs in the control room, technical support center, emergency operations facility, and engineering support center.

The systems are capable of displaying and printing the set of Type A, B, C, D, and E variables specified in Regulatory Guide 1.97 when sensor outputs are available for those parameters.

Data storage and recall capability are provided. At least 2 hours of pre-event and 12 hours of post-event data will be recorded for selected parameters. Capacity to record at least 2 weeks of additional post-event data for selected parameters with reduced time resolution are provided. The capability to transfer data between active memory and archival data storage without interrupting data acquisition and displays are provided.

7.7.6.2 Plant Process Computer System

The purpose of the plant process computer system (PPCS) is to provide information to the plant operator to effectively assist in the operation of the nuclear steam supply system and to inform the operator of specific abnormal conditions by comparison with preset or calculated limits. Basic to the design of this computer system is the requirement that the conventional plant instrumentation systems and control room instrumentation and control functions permit operation of the plant with the computer out of service. The computer system reduces the burden to the plant operator in maintaining surveillance over the nuclear steam supply system to ensure that operating conditions are maintained within normal bounds.

The computer and instrumentation are used instead to alert plant operators that in-core parameters are deviating from values shown to be safe by prior analysis.

For the analysis of in-core thermocouple data, the core is divided into regions. Thermocouple readings (converted to enthalpy rise) are compared region-wise to check for possible peaking or asymmetry. The variation of this type of data over time is available to the operator so that trends can be identified at an early stage.

The plant process computer system (PPCS) supports in-core flux mapping by providing a convenient data collection platform. The plant process computer system is used for data acquisition during flux mapping activities. This data is available for trending.

Plant process computer system inputs are provided from the reactor coolant system, the secondary system, the effluent monitoring system, and auxiliary service systems throughout the

plant. These inputs are stored as discrete, addressable data points that are used to perform specific computations (e.g., compute subcooling margin), generate alarms, indicate digital and analog information, and to provide pre-trip and post-trip data.

7.7.6.3 Safety Parameter Display System

The safety parameter display system (SPDS) is designed to provide an integrated display of critical plant safety parameters and perform reference diagnostics during emergencies. The performance requirements of NUREG 0696, as modified by NUREG 0737, are satisfied by the SPDS. It also fully meets the requirements of NUREG 0737, Supplement 1 (*Reference 10*). See also Section 7.5.2. The SPDS provides the operators in the control room and personnel in the technical support center, the emergency operations facility, and the engineering support center with an indication of the safety status of the plant and postaccident monitoring. In the event of specific abnormal conditions (those for which computer programs were formulated) the computer system is designed to assist the operator by an orderly presentation of symptoms.

The control room reliability of the plant process computer system (PPCS)/safety parameter display system (SPDS) meets the NUREG-0696 specified unavailability goal of 0.01 when the reactor is above MODE 5 (Cold Shutdown) and 0.2 while the reactor is in cold-shutdown status.

Human factors have been considered in all aspects of the SPDS design. Function keyboards are provided that allow for rapid and error-free display requests. Color and pattern coding techniques have been extensively used to portray status in graphic form for rapid and unambiguous recognition. Color-coded bars, targets, and alphanumeric displays are employed to represent off-normal parameter values. The displays were designed to be readable at distances in accordance with the safety significance of particular data. The information on the top level or mode displays is sized to be readable at a distance of up to 15 ft, while alphanumeric text data are readable at a 28-in. viewing distance. The SPDS displays can be accessed from any PPCS terminal.

REFERENCES FOR SECTION 7.7

1. Westinghouse Electric Corporation, Advanced Digital Feedwater Control System, Median Signal Selector for Rochester Gas & Electric, Robert E. Ginna, WCAP 12347, September 1990.

2. Letter from R. C. Mecredy, RG&E, to A. R. Johnson, NRC, Subject: Response to Generic Letter 93-04, dated August 5, 1993.

3. Letter from R. C. Mecredy, RG&E, to A. R. Johnson, NRC, Subject: Transmittal of 90-day Response to Generic Letter 93-04, dated September 20, 1993.

4. Letter from M. Virgilio, NRC, to R. Newton, Westinghouse Owners Group, Subject: Generic Letter 93-04, Demonstration Plant Testing and Closure of Issuance, dated June 20, 1994.

5. Letter from R. A. Newton, Westinghouse Owners Group, to A. C. Thadani, NRC, Subject: Final Transmittal of Documentation Associated with Westinghouse Owners Group Rod Control System Enhancement Program Addressing Generic Letter 93-04, dated July 12, 1994 (OG-94-62).

6. Letter from G.M. Holahan, NRC, to R.A. Newton, Westinghouse Owners Group, Subject: WCAP-13864, “Rod Control System Evaluation,” Revision 1 and Related Documents (TAC No. M88305), dated November 10, 1994.

7. Letter from A.R. Johnson, NRC, to R.C. Mecredy, RG&E, Subject: Resolution of Generic Letter 93-04, “Rod Control System Failure and Withdrawal of Rod Cluster Control Assemblies, 10 CFR 50.54 (f),” (TAC No. M86848), dated June 27, 1995.

8. Letter from R. C. Mecredy, RG&E, to A. R. Johnson, NRC, Subject: Generic Letter 89-19, "Safety Implication of Control System in LWR Nuclear Power Plants" (USI A-47), dated October 27, 1993.

9. Letter from A. R. Johnson, NRC, to R. C. Mecredy, RG&E, Subject: Closeout of Generic Letter (GL) 89-19, "Request for Action Related to Resolution of Unresolved Safety Issue A-47, "Safety Implication of Control Systems in LWR Nuclear Power Plants" Pursuant to 10 CFR 50.54(f)" (TAC No. M74945), dated December 21, 1993.

10. Letter from A. R. Johnson, NRC, to R. C. Mecredy, RG&E, Subject: to NRC Generic Letter 89-06 on the Safety Parameter Display System [Post Accident Monitoring (PAM) Instrumentation] for Rochester Gas and Electric Corporation, dated June 29, 1980.

11. PCR 2000-0005, SAS/PPCS Replacement.

Table 7.7-1
OUT-OF-PHASE CURRENTS (AMPS)

	One Motor-Generator Set in Service	Two Motor-Generator Sets in Service
480-V		
Unlimited capacity	25,000	50,000
400-kVA capacity	12,000	24,000
208-V		
Unlimited capacity	16,000	32,000
400-kVA capacity	8,000	16,000

Table 7.7-2
ROD STOPS

Rod Stop	Actuation Signal	Rod Motion to be Blocked
Rod drop	1/4 rapid power range nuclear flux decrease or any rod bottom signal	Automatic withdrawal[a]
Nuclear overpower	1/4 high power range nuclear flux or 1/2 high intermediate range nuclear flux	Automatic and manual withdrawal[a]
High delta T	2/4 overpower delta T or 2/4 overtemperature delta T	Automatic and manual withdrawal[a]
(Actuation of rod stops [item 3] indicates a turbine load reduction)		
Low power	1/1 low MWe load signal	Automatic withdrawal[a]
T_{AVG} deviation	1/4 T_{AVG} channel deviation from average T_{AVG}	Automatic withdrawal and insertion[a]

a. The automatic rod withdrawal function of the reactor control system has been disabled for all conditions. The automatic rod stops are no longer relevant. The manual rod stops remain applicable.

Table 7.7-3
EXPECTED MAXIMUM VARIATIONS BETWEEN SYMMETRICALLY LOCATED DETECTORS

Parameter	Expected Normal Symmetric Variation	Expected Symmetric Variation With Rod Misalignment
Power range nuclear instrumentation	±2%	10% to 35%
Core outlet thermocouples	±3°F	15°F to 35°F
In-core movable detectors	±2%	10% to 50%