REGULATORY DOCKET FILE COPY

DISTRIBUTION
Docket
NRC PDR
Local PDR
ORB Reading
NRR Reading
DEisenhut
RVollmer
OELD
OI&E (3)
DLZiemann
HSmith
TWambach
BSIC
TERA
ACRS (16)
DCrutchfield
CHofmayer
WShapaker

Docket No. 50-244

Mr. Leon D. White, Jr.
Vice President
Electric and Steam Production
Rochester Gas & Electric Corporation
89 East Avenue
Rochester, New York 14649

Dear Mr. White:

RE: SEP TOPICS VI-10,A Testing of Reactor Trip System and Engineered Safety Features, Including Response Time Testing. VI-7.A.3 ECCS Actuation.

Enclosed is a copy of our evaluation of the above Systematic Evaluation Program Topics. This assessment compares your facility, as described in Docket No. 50-244, with the criteria currently used by the regulatory staff for licensing new facilities. Please inform us if your as-built facility differs from the licensing basis assumed in our assessment.

We have discussed this assessment with your staff and believe the facts concerning your plant are correct. In some areas, we do not have sufficient information to assess the conformance of the R. E. Ginna Plant with current criteria. These areas and our request for the additional information is identified in Section VI of the enclosed evaluation. To complete this assessment consistent with our present schedule, we request that you provide the requested information within 60 days of the date of this letter.

Sincerely,

Dennis L. Ziemann, Chief
Operating Reactors Branch #2
Division of Operating Reactors

Enclosure:
Complete SEP
Topics VI-10.A
and VI-7.A.3

8005270234

cc w/enclosure:
See next page

OFFICE	DOR: ORB #2	DOR: ORB #2	DOR: ORB #2			
SURNAME	HSmith:cc	TWambach	DLZiemann			
DATE	4/25/80	4/25/80	4/25/80			

NRC FORM 318 (9-76) NRCM 0240 ☆ U.S. GOVERNMENT PRINTING OFFICE: 1976 - 265 - 769

cc
Harry H. Voigt, Esquire
LeBoeuf, Lamb, Leiby & MacRae
1757 N Street, N. W.
Washington, D. C. 20036

Mr. Michael Slade
12 Trailwood Circle
Rochester, New York 14618

Rochester Committee for
Scientific Information
Robert E. Lee, Ph.D.
P. O. Box 5236 River Campus
Station
Rochester, New York 14627

Jeffrey Cohen
New York State Energy Office
Swan Street Building
Core 1, Second Floor
Empire State Plaza
Albany, New York 12223

Director, Technical Development Programs
State of New York Energy Office
Agency Building 2
Empire State Plaza
Albany, New York 12223

Rochester Public Library
115 South Avenue
Rochester, New York 14604

Supervisor of the Town
of Ontario
107 Ridge Road West
Ontario, New York 14519

Director, Technical Assessment
Division
Office of Radiation Programs
(AW-459)
U. S. Environmental Protection
Agency
Crystal Mall #2
Arlington, Virginia 20460

U. S. Environmental Protection
Agency
Region II Office
ATTN: EIS COORDINATOR
26 Federal Plaza
New York, New York 10007

Herbert Grossman, Esq., Chairman
Atomic Safety and Licensing Board
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Dr. Richard F. Cole
Atomic Safety and Licensing Board
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Dr. Emmeth A. Luebke
Atomic Safety and Licensing Board
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Mr. Thomas B. Cochran
Natural Resources Defense Council, Inc.
1725 I Street, N. W.
Suite 600
Washington, D. C. 20006

TECHNICAL ASSESSMENT OF SEP SAFETY TOPICS VI-10.A AND VI-7.A.3 FOR GINNA

TECHNICAL ASSESSMENT OF TWO SAFETY TOPICS FOR GINNA

1. VI-10.A: Testing of Reactor Trip System and Engineered Safety Features, Including Response Time Testing
2. VI-7.A.3: ECCS Actuation

TABLE OF CONTENTS

TECHNICAL ASSESSMENT OF TWO SAFETY TOPICS FOR GINNA

1. VI-10.A: Testing of Reactor Trip System and Engineered Safety Features, Including Response Time Testing

2. VI-7.A.3: ECCS Actuation

TABLE OF CONTENTS

TOPIC VI-10.A. TESTING OF REACTOR TRIP SYSTEM AND ENGINEERED SAFETY FEATURES, INCLUDING RESPONSE TIME TESTING

TOPIC VI-7.A.3 ECCS ACTUATION SYSTEM

I. Introduction

These two SEP safety topics deal with the testability and operability of the Reactor Protection System (RPS) and the Engineered Safety Features (ESF) Systems. Since the ECCS actuation is part of the Engineered Safety Features System, these two topics will be treated in one evaluation report.

The RPS and ESF test program should demonstrate a high degree of availability of the systems and the response times assumed in the accident analyses to be within the design specifications. This report will review the plant design to assure that all ECCS components, including the pumps and valves, are included in the component and system test, the frequency and scope of the periodic testing is adequate, and the test program meets the requirements of the General Design Criteria and the Regulatory Guides defined in Section II of this report.

This evaluation report is limited to a comparison of the RPS and ESF testing program with the review criteria and the review guidelines defined in Section II and IV.

Further detail of the test program for pumps and valves can be found in the "in-service valve test program and relief request" safety evaluation report.

II. Review Criteria

The following General Design Criteria govern the topic review:

GDC 21 - Protection system reliability and testability

GDC 37 - Testing of emergency core cooling system

The following Regulatory Guides and Branch Technical Positions provide acceptable basis for RPS and ESF testing program:

RG 1.22 - Periodic testing of protection system actuation functions.

RG 1.118 - Periodic testing of electric power and protection systems.

RG 1.105 - Instrument setpoint

Branch Technical Position ICSB 24 - Testing of Reactor Trip System and Engineered Safety Feature Actuation System Sensor response times.

Branch Technical Position ICSB 25 - Guidance for Interpretation of General Design Criterion 37 for testing and operability of the ECCS as a whole.

Standard Review Plan Section 7.2 and 7.3.

III. Related Safety Topics and Interfaces

VI-7.C - ECCS Single Failure Criteria and requirements for lockout power to valves.

VI-7.F - Accumulator isolation valves power and control system design.

III-12 - Environmental Qualification of Safety Related Equipment.

VI-4 - Containment isolation.

IV. Review Guidelines

1. GDC 21 states that the redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) the protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

2. GDC 37 requires that the ECCS be designed to permit appropriate periodic pressure and functional testing to verify the performance of the full operational sequence that brings the system into operation, including operation of applicable portions of the protection system, the transfer between normal and emergency power sources, and the operation of the associated cooling water system.

3. Regulatory Guide 1.22 provides the acceptable methods for testing actuation devices and actuated equipment.

4. Regulatory Guide 1.105 states that Instruments should be calibrated so as to ensure the required accuracy at the setpoint. The accuracy of all setpoints should be equal to or better than the accuracy assumed in the safety analysis.

5. Regulatory Guide 1.118 describes the method acceptable to the NRC staff of complying with the Commission's regulations with respect to the periodic testing of the protection system and electric power system for systems important to safety.

6. Systems important to safety as defined by R.G. 1.105 are as follows: Those systems that are necessary to ensure (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shut down the reactor, or (3) the capability to prevent or mitigate the consequences of accidents.

7. Branch Technical Position ICSB 24 states that periodic tests for verification of system response times of RTS and ESFAS should include the response time of the sensors whenever practical.

8. Branch Technical Position ICSB 22 states that all portions of the protection system should be designed in accordance with IEEE Std. 279-1971 and all actuated equipment that is not tested during reactor operation should be identified and justified to the provisions of position D.4 in R.G. 1.22.

9. Branch Technical Position ICSB 25 states that all ECCS pumps should be included in the system test.

10. Standard Review Plan Section 7.2 Appendix A, Items 9, 10, 11 and 13 provide more specific guidance to review Reactor Trip System Testing.

11. Standard Review Plan Section 7.3 Appendix A, Items 11, 12, 13 and 14 provide more specific guidance to review Engineered Safety feature system testing.

12. Verify the following:

    A. Test conditions come as close as possible to the actual performance required by RTS and ESF.

    B. Compliance with the single failure criterion during testing.

    C. The results of licensee response time testing data (if available) for the RTS and ESF are within the delay times used in the FSAR accident analysis.

    D. Test can be made to ensure the readiness or the operability of system components.

    E. The Auto Mode of actuation does not inhibit the Manual Mode of actuation, and vice versa, at any time.

    F. The power supplies satisfy the Single Failure Criterion.

    G. The overlapping tests indeed overlap from one test segment to another.

    H. Transducer calibrations are adequate.

    I. Comparator calibrations are adequate.

V. Testing of RPS and ESF at Ginna Plant

1. Reactor Protection System general description.

The RPS automatically trips the reactor to protect against reactor coolant system (RCS) damage caused by high system pressure and to protect the reactor core against fuel rod cladding damage caused by a departure from nucleate boiling (DNB) under the following conditions:

A. Reactor power reaches a preset limit.

B. Excessive temperature rise across the core.

C. Pressurizer pressure or level reaches an established minimum or maximum limit.

D. Loss of reactor coolant flow.

The basic reactor tripping philosophy is to define a region of power and coolant temperature and pressure conditions allowed by the primary tripping functions (overpower high ΔT trip, overtemperature high ΔT trip, and nuclear overpower trip). The allowable operating region within these trip settings is provided to prevent any combination of power, temperature, and pressure which would result in a DNB with all reactor coolant pumps in operation.

Additional tripping functions such as a high pressurizer pressure trip, low pressurizer pressure trip, high pressurizer water level trip, loss-of-flow trip, steam and feedwater flow mismatch 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 tripping functions for specific accident conditions and mechanical failures.

The Ginna reactor possesses high-speed Westinghouse magnetic-type control rod drive (CRD) mechanisms. The reactor internal components, fuel assemblies, rod cluster control (RCC) assemblies, and drive systems components are designed as Class I equipment.

Two reactor trip breakers are provided to interrupt power to the CRD mechanisms. The breaker main contacts are connected in series with the power supply to the mechanism coils. The trip breakers are opened by the undervoltage coils on both breakers (normally energized) which becomes deenergized by any one of the several trip signals. Each protection channel actuates two separate trip logic trains, one for each reactor trip breaker undervoltage trip coil. The electrical state of the devices providing signals to the circuit breaker undervoltage trip coils causes these coils to trip the breaker in the event of reactor trip or power loss. Opening either breaker interrupts power to the magnetic latch mechanisms on each CRD, causing them to release the rods and allowing the rod clusters to insert by gravity into the core.

The reactor shutdown function of the rods is completely independent of the normal control functions since 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 upon the loss of power to the control rods.

The RPS is designed on a channelized basis to achieve isolation and independence between redundant protection channels. The coincident trip philosophy is carried out to provide a safe and reliable system since a single failure will not defeat the function of the 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. The channelized design that applies to the analog as well as the logic portions of the protection system is discussed below.

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 the 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. This approach is used for pressurizer pressure and water level channels, steam generator water level, and ΔT channels, steam flow-feedwater flow and nuclear power range channels.

Physical separation is used to achieve isolation of redundant transmitters, Separation of field wiring is achieved using separate wireways, cable trays, conduit runs, and containment penetrations for each redundant channel. Analog equipment is separated by locating redundant components in different protection racks.

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 a-c 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, i.e., a two-out-of-three circuit becomes a one-out-of-a-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 subcritical operation, are bypassed at power operation to prevent spurious reactor trip signals and to improve reliability.

The reactor trip bistables are mounted in the protection racks and are the final operational components 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 d-c 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 are 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 d-c power feed No. 2 and the contacts from the D relays. Therefore, the two redundant reactor trip logic channels will be physically separated and electrically isolated from one another. Overall, the RPS is comprised of identifiable channels which are physically, electrically, and functionally separated and isolated from one another. A typical trip logic channel is shown in Figure 7.2-8 of the FSAR.

2. Reactor Protection Trip Function

A. 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 which could make the automatic circuitry inoperable.

B. High Nuclear Flux (Power Range) Trip

This circuit trips the reactor when two-of-the-four power range channels read above the trip setpoint. There are two setpoints associated with this trip. The low setting can be manually bypassed when two-of-the-four power range channels are above approximately 10% power. Three-of-the-four channels reading below 10% power automatically reinstates the trip. The high setting is always active.

C. High Nuclear Flux (Intermediate Range) Trip

This circuit trips the reactor when one-of-the-two intermediate range channels reads above the trip setpoint. This trip can be manually bypassed if two-of-the-four power range channels are above approximately 10% power. Three-of-the-four channels below this value automatically reinstates the trip. The intermediate channels (including detectors) are separate from the power range channels in this plant design.

D. High Nuclear Flux (Source Range) Trip

This circuit trips the reactor when one-of-the-two source range channels reads above the trip setpoint. It can be manually bypassed when one-of-the-two intermediate range channels reads above the source range cutoff value. Both intermediate range channels below this value automatically reinstate the trip.

This trip is also bypassed by two-of-the-four high power range signals. The trip point is set between the source range cutoff power level and the maximum source range power level.

E. Overtemperature ΔT Trip

This circuit trips the reactor on coincidence of two-of-the-four signals, with two channels per loop to protect the core against a DNB.

F. Overpower ΔT Trip

This circuit trips the reactor on coincidence of two-of-the-four signals, with two channels per loop to protect against excessive power (i.e., fuel rod rating protection).

G. Low Reactor Coolant Pressure Trip

This circuit trips the reactor on coincidence of two-of-the-four pressurizer pressure signals to protect against excessive voids and resultant high fuel temperature.

H. High Reactor Coolant Pressure Trip

This circuit trips the reactor on coincidence of two-of-the-three pressurizer pressure signals to limit the range of required protection from the overtemperature ΔT trip and to protect against overpressure.

I. High Pressure Water Level Trip

This circuit trips the reactor on coincidence of two-of-the-three high pressurizer water level signals to trip the reactor. It is provided as a backup to the high pressure trip.

J. Low Reactor Coolant Flow Trip

This circuit trip signal is actuated by the coincidence of two-of-the-three signals for each reactor coolant loop. The loss of flow in either loop causes a reactor trip. This trip protects the core from a DNB following a loss of coolant flow.

K. Safety Injection System Actuation Trip

This reactor trip occurs on the actuation of the safety injection system (SIS), i.e., when there is:

1) Low primary system pressure (two-of-the-three signals);

2) High containment pressure (two-of-the-three signals);

3) Coincidence of low pressure in either steam generator (two-of-the-three signals).

L. Turbine Trip

This trip is sensed by two-of-the-three signals from the autostop oil pressure. This is an anticipatory trip which protects the reactor from a sudden loss of heat sink.

M. Steam/Feedwater Flow Mismatch Trip

This trip is actuated by a steam/feedwater flow mismatch (one-of-the-two signals) in coincidence with low water level (one-of-the-two signals) in either steam generator. This trip protects the reactor from a sudden loss of heat sink.

N. Low-Low Steam Generator Water Level Trip

This trip is actuated on two-of-the-three low-low water level signals in either steam generator. This trip protects the reactor from a loss of heat sink.

3. Reactor Protection System Testing

A. Protective Systems Capability for Testing and Calibration

The bistable portions of the protective system (e.g., relays, bistables, etc.) provide trip signals only after signals from the analog portions of the system have reached a preset value.

The 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 of the analog portion of a protective channel during reactor operation:

1) Varying the monitored variable

2) Introducing and varying a substitute transmitter signal

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

This design permits administrative control of the:

1) Means for manually bypassing channels or protective functions.

2) Access to all trip settings, module calibration adjustments, test points, and signal injection points.

B. 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 the final element in a trip channel (required during power operation) to be 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.

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 allows testing and calibration of meters and bistables. Transmitters and sensors are checked against each other and against precision read-out equipment during normal power operation.

C. RPS Analog Channel Testing

The basic elements comprising an RPS analog protection channel are shown in Figure 7.2-7 of the FSAR, 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 the 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 of 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 the bistable in the channel under test be placed in the tripped mode prior to test. 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 controls prevent the nuclear instrumentation source range and intermediate range protection channels from being disabled during periodic testing. Power range over-power protection does not have administrative control provision because there are sufficient channels to satisfy single failure criterion during 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 will provide indication of an associated corrective actions for a dropped rod condition.

Actual channel calibration will consist of injecting a test signal from an external calibration signal into the signal injection jack. Where applicable, the channel power supply will serve as a power source for the calibration source and permit verification of 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.

D. RPS Logic Channel Testing

The general design features of the RPS logic system are described below. The trip logic channels for a typical two-out-of-four trip function are shown in Figure 7.2-8 of the FSAR. The analog portions of these channels are shown in Figure 7.2-9 of the FSAR. Each bistable drives two relays: The A and B relays for level, and the C and D relays 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. A series

configuration is used for the trip breakers since they are actuated (i.e., opened) by undervoltage coils. This approach is consistent with a deenergize-to-trip preferred failure mode.

The planned logic system testing includes exercising the individual reactor trip breakers to demonstrate system integrity. One bypass breaker is used in conjunction with testing of the reactor trip breakers. It is installed to allow opening the normal trip breaker. To test both reactor trip breakers, the bypass breaker must be used in one cell for reactor trip breaker A after which it is physically moved to the cell associated with reactor trip breaker B. One annunciator window on the main control board will indicate that the bypass breaker is closed in either cell. During normal operation, the bypass breaker is physically removed (racked out).

As shown in Figure 7.2-8 of the FSAR, 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. If a valid trip signal occurs while bypass breaker AB-1 is bypassing trip breaker No. 1, the trip breaker No. 2 will be opened through its associated logic train. The trip signal applied to trip breaker No. 2 is simultaneously applied to bypass breaker AB-1, thereby opening the bypass around trip breaker No. 1. Trip breaker No. 1 would either have been opened manually as part of the test or 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 signal through the logic network during testing. Lights are also provided on the main control board to indicate the status of the individual logic relays.

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 7.2-10 of the FSAR. The test switches used to deenergize the trip bistable relays operate through interposing relays as shown in Figures 7.2-7 and 7.2-9 of the FSAR. 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 the instrumentation protection system are provided by colored nameplates on the cabinets.

4. Engineered Safety Features General Description

Engineered safety features (ESF) are provided in the facility to mitigate the consequence of the design bases accidents. ESFs have been designed to cope with any size reactor coolant pipe breaks, up to and including the circumferential rupture of any pipe assuming unobstructed discharge from both ends. They are also designed to cope with any steam or feedwater line break, up to and including the main steam or feedwater headers.

ESFs in the Ginna plant are comprised of the following systems:

Safety Injection System (ECCS)

Containment Spray System

Containment Air Recirculation, Cooling and Filtration System

Containment Isolation System

A. Safety Injection System

Emergency core cooling is provided by the SIS which constitutes the ECCS. The SIS components operate in three modes delineated as passive accumulator injection, active safety injection, and residual heat removal (RHR) recirculation. The primary purpose of the SIS is to automatically deliver cooling water to the reactor core to limit the fuel clad temperature, and thereby ensure that the core will remain intact and in place with its heat transfer geometry preserved. This protection is prescribed for all breaks (up to and including a hypothetical instantaneous double ended rupture of the reactor coolant pipe), for a rod ejection accident, and for a steam generator tube rupture.

For any rupture of a steam pipe and the associated uncontrolled heat removal from the core, the SIS adds concentrated boron solution to provide negative reactivity to accommodate the reactivity increase due to the temperature drop and a possible stuck rod.

The principal SIS components that provide core cooling immediately following a LOCA are the two accumulators (one for each loop), the three 50%-capacity safety injection (high-head) pumps, and the two 100%-capacity RHR (low-head) pumps. For large breaks, the accumulators, which are passive components discharge into the cold legs of the reactor coolant piping, thus rapidly ensuring core cooling.

The safety injection pumps are actuated by two-of-the-three low pressurizer pressures, or by two-of-the-three low steamline pressures, or by two-of-the-three high containment pressures, or manually. The pressurizer pressure is monitored by pressure transmitters with bellow capsules.

The safety injection signal will open the SIS isolation valves and start the high-head safety injection pumps and low-head safety injection pumps. Suction for the safety injection pumps will be aligned initially to a tank containing boric acid. The suction for these pumps is transferred to the refueling water storage tank when the boric acid in the tank is nearly expended.

During normal plant operation, the two boric acid tanks are aligned to the suction of the high-head safety injection pumps. The piping from the boric acid tank to the suction of the high-head safety injection pump contains two independent parallel flow paths, each with two motor-operated valves (MOVs) in series. The safety injection signal is applied to the MOVs in the suction line to assure that the concentrated boric acid flow to the suction of the safety injection pumps.

When a low level is reached in the boric acid tanks, the suction valves from the refueling water storage tank open and the suction valves from the boric acid tanks close. The suction to the safety injection pump is then aligned from the refueling water storage tank. In the event that the suction valves from the boric acid tanks do not open within two seconds after receiving the safety injection actuation signal, the suction valves from the refueling water storage tank open.

Redundant level instrumentation to the boric acid tank are used to switch the safety injection pump suction flow from the boric acid tanks to the refueling water storage tank. The refueling water storage tank is equipped with two redundant level indicators. Each level indicator has two alarm setpoints such that each level channel has two alarms, i.e., the first low-level alarm and the second low-low-level alarms, respectively. During reactor operation, the RHR pumps are aligned to the refueling water storage tank.

Because the injection phase of the LOCA is terminated before the refueling water storage tank is emptied, all pipes are kept filled with water before recirculation is initiated. The level indicator and alarms on the refueling water storage tank warn the operator to terminate the injection phase. Two additional level indicators and alarms are provided in the containment sump which also indicate when injection can be terminated and recirculation initiated. After the injection operation, the coolant that spilled from the break and the water that was collected from the containment spray are cooled and recirculated to the RCS by the SIS.

When the break is large, depressurization occurs due to the high rate of mass and energy loss through the break to the containment. When the break is small, the depressurization of the RCS can be augmented by a steam dump and auxiliary feedwater addition.

If the necessary RCS depressurization occurs before the injection mode of the SIS is terminated, the RHR pumps take suction from the containment sump, circulate the spilled coolant through the residual heat exchangers, and return the coolant to the reactor. If depressurization of the RCS proceeds slowly, the safety injection pumps may be used to augment the head capacity of the RHR pumps in returning the spilled coolant to the reactor.

The recirculation sump lines comprise two independent lines which penetrate the containment. Each line has a remote MOV located inside and outside the containment. Each line is run independently to the suction of a RHR pump. The system permits long-term recirculation in the event of a passive or active component failure.

The remote-operated SIS valves which are under manual control (i.e., valves which normally are in their ready position and do not receive a safety injection signal) have their positions indicated on a common portion of the control board.

B. Containment Spray System

The containment spray system consists of two pumps, one spray additive tank, two spray headers, spray nozzles, and the necessary piping and valves. The system initially takes suction from the refueling water storage tank. When a low level is reached in the refueling water storage, the spray pump suction is fed from the discharge of the RHR pumps if continued spray is required. The system design conditions were selected to be compatible with the design conditions for the low pressure injection system since both of these systems share the same suction line.

During the period of time that the spray pumps draw from the refueling water storage tank, approximately 20 gpm of spray additive (sodium hydroxide) will be added to the refueling water by using a liquid eductor motivated by the spray pump discharge pressure. The fluid passing from the tank will then mix with the fluid entering the pump suction. The result will be a solution suitable for the removal of iodine.

The spray system will be actuated by the coincidence of two sets of two-out-of-three high containment pressure signals. This starting signal, entitled "Containment Hi-Hi-Pressure", will start the pumps and open the discharge valves to the spray header. The valves associated with the spray additive tank will be opened automatically two minutes after the containment spray signal is actuated. Sodium hydroxide will flow due to the suction of the spray pumps and mix with refueling water prior to being discharged through the spray nozzle into the containment.

After the containment spray signal is actuated, the operator has the capability to stop the timer if it has been determined that actuation of the sodium hydroxide addition is not warranted. The operator also has the capability to reinitiate the sodium hydroxide addition, if required. Emergency procedures set forth guidelines for this action.

C. Containment Air Recirculation, Cooling, and Filtration System

The containment air recirculation system consists of four air-handling systems, each including a motor, fan, cooling coils, moisture separators and high-efficiency particulate air (HEPA) filters, duct distribution system, instrumentation, and controls. The units are located on the intermediate floor between the containment wall and the primary compartment shield walls. Two-of-the-four air-handling systems are equipped with activated charcoal-filter units, which are normally isolated from the main air recirculation stream and through which the air-steam mixture is bypassed to remove volatile iodine following an accident.

Two of the air-handling assemblies are required during the post-accident period for depressurization of the containment vessel. Local flow and temperature indication of service water at each air-handling unit and the alarms indicating abnormal service water flow, temperature, and radioactivity are provided in the control room.

Upon receipt of either high containment pressure or automatic safety injection signal, the butterfly valves in the containment recirculation systems are tripped to the accident position. Accident position is also the "fail-safe" close position.

Butterfly valves are used to route the air flow through the charcoal filters; these valves have only two positions: full open or full closed. These valves are air operated and spring loaded. Upon loss of control signal or control air, the spring actuates the valve to the accident position.

Redundant electrically operated three-way solenoid valves are used at each butterfly valve to control the instrument air supply (control air). These valves are arranged so that failure of a single solenoid valve to respond to the accident signal will not prevent actuation of the butterfly valve to the accident position.

The containment pressure is sensed through six separate pressure transducers located outside the containment. Containment pressure is communicated to the transducers by three 3/8" stainless steel lines penetrating the containment vessel. The high containment

pressure signal from these sensors trip the containment isolation dampers and valves and sends a signal to start the fan motors - the remaining two motors not operating under normal conditions, or all four motors in the case of a loss of outside power.

The automatic safety injection signal is that resulting from two-out-of-three low pressure in the pressurizer, or from high containment pressure.

D. Containment Isolation System

Containment isolation is initiated automatically by a safety injection signal or manually by one of two switches on the main control board. Containment isolation trips the containment sump pumps and closes all containment isolation valves that are not required to be open during an accident condition, which includes containment sump pump discharge isolation valves; steam generator blowdown isolation valves, reactor coolant drain tank vent header and pump suction valve. The containment isolation signal also isolates four containment ventilation purge valves, two containment depressurization valves, containment air test supply valve, two containment air test vent valves, and trips the purge supply and exhaust fans. The containment ventilation valves also are isolated on high containment activity or on manual containment spray.

Remote operated containment isolation valves are either air or motor operated. When one air operated isolation valve is used, there are two relays in series to energize the solenoid. Each relay is operated from a separate control channel, each of which has an independent dc power source. When two air operated isolation valves in series are used, there is one solenoid for each valve, each of which has an independent dc power source. When a motor operated valve is used, the ac power is fed from one of two motor control centers, and each MCC is fed from a diesel powered bus. In the FSAR, Section 5.2.2, the licensee has stated that if, in an emergency, only one diesel starts, then both MCCs are automatically loaded onto the operating diesel. This design deviates from current licensing criteria because this design challenges the independence of the redundant emergency power sources.

The containment isolation system can be reset by a manual switch in the control room. Some equipment would return automatically to the position prior to the isolation signal. Presently, procedures require that the operator place containment isolation valve switches in the "closed" position prior to resetting containment isolation. This current design on reset capability does not satisfy the NRC Lessons Learned Task Force position, which requires that resetting of the containment isolation signal will not result in the automatic reopening of containment isolation valves. The licensee has committed to modify the control circuitry to preclude the reopening of isolation valves. The modified design will be reviewed in Topic VI-4, "Containment Isolation".

5. Engineered Safety Features Testing

A. Safety Injection System test is performed at each reactor refueling interval, with the reactor coolant system pressure less than or equal to 350 psig and temperature less than or equal to 350°F. A test signal is applied to initiate operation of the system. The safety injection and residual heat removal pump motors are prevented from starting during the test. The system is considered satisfactory if control board indication and visual observations indicate that all valves have received the Safety Injection Signal and have completed their travel.

Except during cold or refueling shutdowns, the safety injection pumps and residual heat removal pumps are started at intervals not to exceed one month. Acceptable levels of performance for the RHR pumps will be 200 gpm at the minimum discharge pressure of 140 psig. Acceptable level of performance for the SI pumps will be 50 gpm at the minimum discharge pressure of 1420 psig. The spray additive valves are tested at intervals not to exceed one month. With the pumps shut down and the valves upstream and downstream of the spray additive valves closed, each valve is opened and closed by operator action. The accumulator check valves are checked for operability at refueling shutdown.

B. Containment Spray System test is performend at each reactor refueling interval. The test is performed with the isolation valves, in the spray supply lines, at the containment blocked closed. Operation of the system is initiated by tripping the normal actuation instrumentation. The spray nozzles are checked for proper functioning at least every five years. The test is considered satisfactory if visual observations indicate all components have operated satisfactorily. Acceptable level of performance for containment spray pumps is 35 gpm at the minimum discharge pressure of 240 psig.

C. There is not sufficient information in the docket describing the testing of containment air recirculation, cooling, and filtration system. The technical speicification requires that the containment air filtration system be tested during the integrated containment leak rate tests. The charcoal filter isolation valve shall be tested at intervals not greater than one month to verify operability and proper orientation.

D. There is not sufficient information in the docket to describe the testing of containment isolation system. The technical specification requires that the containment isolation valves be tested during each reactor shutdown for refueling. Test interval shall not be greater than two years.

VI. Evaluation and Conclusion

Based on the information available on the docket, the Ginna plant testing program for the Reactor Trip System in general is in conformance with the reliability and testability criteria discussed in Section II of this report. However, there are several areas in the Engineered Safety Feature System which are not in conformance with the criteria discussed in Section II of this report. The following listed items summarize the major deviations based on the staff's audit review. The licensee is requested to provide additional information to address each of the following concerns:

1. Provide information which discusses the response time testing to verify Reactor Trip System and Engineered Safety Feature response time.

2. The surveillance test frequency information is incomplete. As shown on Tables 1 & 2, the test frequency on many items is not available. Provide test frequency information in areas where this information is lacking.

3. Provide descriptive information on how the following actuation systems are being tested:

   A. Auxiliary Feedwater Actuation System

   B. Main Steam and Feedwater Isolation Actuation System

4. RG 1.22 states that the protection system and the systems whose operation it initiates should be designed to permit testing of the actuation devices during reactor operation. The actuating equipment not tested during reactor operation should be identified and justified to the provisions of position D.4 in RG 1.22. Most Engineered Safety Feature Systems in Ginna are only tested during refueling shutdown. Identify and justify the actuation logic and the actuated devices in the ESF Systems that are not tested during reactor operation.

5. For the purpose of performing a test during reactor operation, each bypass condition should be individually and automatically indicated to the reactor operator in the main control room. Provide information on bypassed and inoperable status indications and describe their application during the RPS logic testing and ESF channel and logic testing.

D. There is not sufficient information in the docket to describe the testing of containment isolation system. The technical specification requires that the containment isolation valves be tested during each reactor shutdown for refueling. Test interval shall not be greater than two years.

VI. Evaluation and Conclusion

Based on the information available on the docket, the Ginna plant testing program for the Reactor Trip System in general is in conformance with the reliability and testability criteria discussed in Section II of this report. However, there are several areas in the Engineered Safety Feature System which are not in conformance with the criteria discussed in Section II of this report. The following listed items summarize the major deviations based on the staff's audit review. The licensee is requested to provide additional information to address each of the following concerns:

1. Provide information which discusses the response time testing to verify Reactor Trip System and Engineered Safety Feature response time.

2. The surveillance test frequency information is incomplete. As shown on Tables 1 & 2, the test frequency on many items is not available. Provide test frequency information in areas where this information is lacking.

3. Provide descriptive information on how the following actuation systems are being tested:

   A. Auxiliary Feedwater Actuation System

   B. Main Steam and Feedwater Isolation Actuation System

4. RG 1.22 states that the protection system and the systems whose operation it initiates should be designed to permit testing of the actuation devices during reactor operation. The actuating equipment not tested during reactor operation should be identified and justified to the provisions of position D.4 in RG 1.22. Most Engineered Safety Feature Systems in Ginna are only tested during refueling shutdown. Identify and justify the actuation logic and the actuated devices in the ESF Systems that are not tested during reactor operation.

5. For the purpose of performing a test during reactor operation, each bypass condition should be individually and automatically indicated to the reactor operator in the main control room. Provide information on bypassed and inoperable status indications and describe their application during the RPS logic testing and ESF channel and logic testing.

6. Provide information which discusses the testing of containment air recirculation, cooling, and filtration systems.

7. Provide information which discusses the testing of containment isolation systems.

VII. References

1. Code of Federal Regulations, Title 10, Part 50 (10 CFR 50) Appendix A, (General Design Criteria), 1978.

2. U. S. Nuclear Regulatory Commission, Regulatory Guides 1.22, 1.75, 1.89 and 1.118.

3. Rochester Gas and Electric Corporation, Ginna Final Safety Analysis Report (FSAR), dated April 23, 1975.

4. Westinghouse Standard Technical Specifications (NUREG-0452), dated June 15, 1978.

5. Institute of Electrical and Electronics Engineers, IEEE Std.-279-1971.

VIII. Topic Definition

Topic VI-10A: Testing of Reactor Trip System and Engineered Safety Features, Including Response Time Testing

NRC Task Definition

The task is to review the reactor trip system (RTS) and engineered safety features (ESFs) test program to verify RTS and ESF operability on a periodic basis and to verify RTS and ESF response time.

NRC Safety Objective

The safety objectives are to ensure, on a periodic basis, the operability of the RTS and ESFs and to verify sensor response times so that the RTS and ESF test program demonstrates a high degree of system availability and the response times assumed in the accident analysis are within the design specification.

Topic VI-7.A.3: ECCS Actuation System

NRC Task Definition

The task is to review the emergency core cooling system (ECCS) actuation system with respect to testability of the operability and performance of individual active components of the system and of the entire system under conditions as close as to the design condition as practical.

NRC Safety Objectives

The safety objectives are to ensure that all ECCS components (e.g., valves and pumps) are included in the component and system test, and that the frequency and scope of the periodic testing are adequate and meet the requirements of the General Design Criteria (GDC) 37.

TABLE 1: GINNA PLANT TECHNICAL SPECIFICATION INSTRUMENTATION

SURVEILLANCE REQUIREMENTS FOR REACTOR, TRIP SYSTEM

Reactor Trip Function	Channel Check	Channel Calibration	Channel Test	Remark
(1) Manual Trip	N/A	N/A	no information	
(2) High Nuclear Flux (Power Range) Trip	Each shift	Daily for Heat Balance Quarterly for Axial offset	Biweekly	
(3) High Nuclear Flux (Intermediate Rng) Trip	Each shift	None	Prior to startup	
(4) High Nuclear Flux (Source range) Trip	Each Shift	None	Prior to startup	
(5) Overtemperature ΔT Trip	Each shift	Each refueling	Monthly	
(6) Overpower ΔT Trip	Each shift	Each refueling	Monthly	
(7) Low RC Pressure Trip	Each shift	Each refueling	Monthly	
(8) High RC Pressure Trip	Each shift	Each refueling	Monthly	
(9) High Pressurizer Water Level Trip	Each shift	Each refueling	Monthly	
(10) Low Reactor Coolant Flow Trip	Each shift	Each refueling	Monthly	

Not applicable

Reactor Trip Function	Channel Check	Channel Calibration	Channel Test	Remark
(11) Safety Injection Actuation Trip	N/A	N/A	No information	
(12) Turbine Trip	N/A	Each refueling	Monthly	
(13) Steam/FW Flow Mismatch Trip	No information	No information	No information	
(14) Lo-Lo Steam Gen Level Trip	Each shift	Each refueling	Monthly	
(15) Reactor Trip Breaker	N/A	N/A	No information	
(16) Automatic Trip Logic	N/A	N/A	No information	

TABLE 2

GINNA PLANT TECHNICAL SPECIFICATION INSTRUMENTATION SURVEILLANCE REQUIREMENTS FOR ENGINEERED SAFETY FEATURE SYSTEM

ESF System Function	Channel Check	Channel Calibration	Channel Test	Remark
1. Safety Injection				
a. Manual	N/A	N/A	no information	
b. Containment Pressure Analog	each shift	each refueling	monthly	
c. Steam Generator Steam Pressure Analog	each shift	each refueling	monthly	
d. Pressurizer Low Pressure Analog	each shift	each refueling	monthly	
e. Automatic Initiate Logic	N/A	N/A	no information	
f. BAT & RWST Valve Controls	no information	no information	no information	
2. Containment Spray				
a. Manual	N/A	N/A	no information	
b. Containment Pressure Analog	no information	no information	no information	
c. Automatic Initiate Logic	N/A	N/A	no information	
d. Spray Additive Tank Valve Controls	no information	no information	no information	
3. Containment Isolation				
a. Manual	N/A	N/A	no information	
b. Safety Injection Actuation	N/A	N/A	no information	
c. Automatic Initiate Logic	N/A	N/A	no information	
d. Containment Activity Analog	each shift	each refueling	monthly	

TABLE 2

GINNA PLANT TECHNICAL SPECIFICATION INSTRUMENTATION SURVEILLANCE REQUIREMENTS FOR ENGINEERED SAFETY FEATURE SYSTEM

ESF System Function	Channel Check	Channel Calibration	Channel Test	Remark
4. Steam Line Isolation				
a. Manual	N/A	N/A	no information	
b. Containment Pressure Analog	each shift	each refueling	monthly	
c. Hi-Hi Steam Flow with S.I.	no information	no information	no information	
d. Hi Steam Flow 2/4 low T w/S.I.	no information	no information	no information	
5. Feedwater Line Isolation				
S.I. Automatic Actuation Logic	N/A	N/A	no information	
6. Auxiliary Feedwater				
a. Steam Generator Level Analog	each shift	each refueling	monthly	
b. Safety Injection	N/A	N/A	no information	
c. Station Blackout	N/A	N/A	no information	
d. Manual	N/A	N/A	no information	
7. Containment Air recirculation, cooling, and Filtration System				
a. Manual	N/A	N/A	no information	
b. Containment Pressure Analog	no information	no information	no information	
c. Safety Injection Actuation	N/A	N/A	no information	
d. Automatic Initiate Logic	N/A	N/A	no information	

TABLE 2

GINNA PLANT TECHNICAL SPECIFICATION INSTRUMENTATION SURVEILLANCE REQUIREMENTS FOR ENGINEERED SAFETY FEATURE SYSTEM

ESF System Function	Channel Check	Channel Calibration	Channel Test	Remark
8. Other ECCS-related Analog Instrument				
a. Boric Acid Tank Level	daily	each refueling	n/a	
b. Refueling Water Storage Tank Level	daily	each refueling	n/a	
c. Containment Sump Level	no information	each refueling	no information	
d. Accumulator Level & Pressure	each shift	each refueling	no information	
e. Volume Control Tank Level	no iformation	each refueling	no information	
f. Boric Acid Control	no information	each refueling	no information	
g. 4 Kv Bus Voltage	n/a	each refueling	monthly	
h. Pump Valve Interlock	each refueling	no information	no information	