EG&G
ENERGY MEASUREMENTS GROUP

EGG 1183-4147
SEPTEMBER 1980

SYSTEMATIC EVALUATION PROGRAM REVIEW OF NRC SAFETY TOPIC VII-3 ASSOCIATED WITH THE ELECTRICAL, INSTRUMENTATION, AND CONTROL PORTIONS OF THE SYSTEMS REQUIRED FOR SAFE SHUTDOWN FOR THE GINNA NUCLEAR POWER PLANT

SAN RAMON OPERATIONS
2601 OLD CROW CANYON ROAD
SAN RAMON, CALIFORNIA 94583

EG&G
Energy Measurements Group
San Ramon Operations

SYSTEMATIC EVALUATION PROGRAM REVIEW OF NRC SAFETY TOPIC VII-3 ASSOCIATED WITH THE ELECTRICAL, INSTRUMENTATION, AND CONTROL PORTIONS OF THE SYSTEMS REQUIRED FOR SAFE SHUTDOWN FOR THE GINNA NUCLEAR POWER PLANT

by

D. H. Laudenbach

Approved for Publication

J. R. Radosevic
Department Manager

This document is UNCLASSIFIED

Derivative Classifier:
Nicholas E. Broderick
Department Manager

Work Performed for Lawrence Livermore National Laboratory under U.S. Department of Energy Contract No. DE-AC08-76 NVO 1183.

ABSTRACT

This report documents the technical evaluation and review of NRC Safety Topic VII-3, associated with the electrical, instrumentation, and control portions of the systems required for safe shutdown of the Ginna Nuclear Power Plant, using current licensing criteria.

FOREWORD

This report is supplied as part of the Systematic Evaluation Program being conducted for the U.S. Nuclear Regulatory Commission by Lawrence Livermore National Laboratory. The work was performed by EG&G, Inc., Energy Measurements Group, San Ramon Operations for Lawrence Livermore National Laboratory under U.S. Department of Energy contract number DE-AC08-76NV01183.

TABLE OF CONTENTS

LIST OF TABLES

SYSTEMATIC EVALUATION PROGRAM REVIEW OF NRC SAFETY TOPIC VII-3 ASSOCIATED WITH THE ELECTRICAL, INSTRUMENTATION, AND CONTROL PORTIONS OF THE SYSTEMS REQUIRED FOR SAFE SHUTDOWN FOR THE GINNA NUCLEAR POWER PLANT

Donald H. Laudenbach

EG&G, Inc., Energy Measurements Group
San Ramon Operations

1. INTRODUCTION

Some SEP plants may not have the capability to achieve hot shutdown and subsequent cold shutdown of the reactor from outside of the control room. The "Safe Shutdown" report [Ref. 1] generated by the NRC/SEP staff identifies the systems required for safe shutdown. This report reviews the electrical, instrumentation, and control aspects of the identified Category I systems as they are utilized from inside and outside of the control room.

2. CURRENT LICENSING CRITERIA

GDC 17 [Ref. 2], entitled "Electric Power Systems," states in part that:

> An onsite electric power system and an offsite electric power system shall be provided to permit functioning of structures, systems, and components important to safety.

GDC 19 [Ref. 2], entitled "Control Room," states in part that:

> A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including LOCAs.
>
> Equipment at appropriate locations outside the control room shall be provided with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown and with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

GDC 21 [Ref. 2], entitled "Protection System Reliability and Testability," states in part that:

> Redundancy and independence designed into the protection system shall be sufficient to assure that:
>
> a. No single failure results loss of the protection function.
>
> b. Removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated.

Standard Review Plan (NUREG-75/087) [Ref. 3], Section 7.5, entitled "Safety-Related Display Instrumentation," states in paragraph II.2 and 3 that:

a. All monitoring channels should be redundant, to assure that wrong indication due to device malfunction will not cause false action or inaction on the part of the operator. Identification malfunctions can be identified by cross checking between redundant channels.

b. Redundant channels of safety-related display instrumentation should be isolated physically and electrically to assure that a single failure will not result in complete loss of information about a monitored variable.

3. REVIEW GUIDELINES

The following NRC guidelines were used for this review:

Identify the systems and equipment necessary to achieve safe shutdown of the plant.

Verify that the instrumentation and control systems necessary for safe shutdown possess sufficient redundancy (GDC 21).

Verify that the systems and equipment identified above are capable of receiving power from both normal and emergency sources (GDC 17).

Verify that the instrumentation and controls necessary for safe shutdown are available in the control room (GDC 19).

Identify the instrumentation and control equipment that is located outside the control room that is available to achieve and maintain hot and cold shutdown (GDC 19).

Verify that the safe shutdown display instrumentation in the control room meets the single failure criterion (SRP 7.5 II.2 and 3).

Compile a list of electrical structures, systems and components that are necessary for safe shutdown of the plant. Submit the compilation as a section of the report on NRC Safety Topic III-1 [Ref. 4].

Verify that no single power supply failure inhibits achieving safe shutdown of the plant and that the availability of power exists from both normal and emergency source.

Identify the related NRC safety topics as an appendix to the report.

4. SYSTEM DESCRIPTION

4.1 GENERAL

The SEP Review of Safe Shutdown Systems for the R.E. Ginna Nuclear Power Plant [Ref. 1] states that:

> The NRC staff and the licensee, Rochester Gas and Electric Corp. (RG&E) developed a list of the minimum systems necessary to take the reactor from operating conditions to 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 requirements of BTP RSB 5-1 [Ref. 5].
>
> (1) Reactor Protection System
> (2) Auxiliary Feedwater System
> (3) Main Steam System
> (4) Service Water System
> (5) Chemical and Volume Control System
> (6) Component Cooling Water 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 hot-shutdown, to cold-shutdown. These functions and their associated alternate methods are identified in Table 4.1.

Table 4.1. Functions for shutdown and cooldown.

Function	Method
1. Control of Reactor Power	a. Boration 1. CVCS 2. High Pressure Safety Injection
	b. Control Rods 1. Controlled Rod Insertion 2. Reactor Trip
2. Core Heat Removal	a. Forced Circulation (reactor coolant pumps) b. Natural Circulation (using steam generators) c. Residual Heat Removal d. CVCS Letdown Heat Exchangers (CCW) e. Pressurizer Reliefs and Safety Injection
3. Steam Generator Heat Removal	a. Main Condenser (circulating water system) b. Atmospheric Dumps (manual actuation) c. Safety Valves d. Auxiliary Feed System Turbine e. Steam Generator Blowdown f. Water-Solid Steam Generator
4. Feedwater	a. Main Feedwater Pumps b. Steam- and Motor-Driven Auxiliary Feedwater Pumps c. Standby Auxiliary Feedwater Pumps
5. Primary System Control	a. CVCS b. Pressurizer Relief Valves

4.1.1 Reactor Protection System

The reactor protection system (RPS) 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. RPS 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 a-c power feed. Each reactor trip circuit is designed so that a trip occurs when the circuit is de-energized. 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 de-energize 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.

4.1.2 Auxiliary Feedwater System

The auxiliary feedwater system (AFS) is divided into two independent channels or trains. One channel is supplied by a turbine-driven pump; the other channel is supplied by two motor-driven pumps powered from separate redundant 480V emergency buses which can receive power from either onsite or offsite sources. Each motor-driven pump can provide 100 percent of the AFS flow required for decay heat removal and can be cross-connected to provide flow to either steam generator.

A standby auxiliary feedwater system (SAFS) provides flow in case suction loss from the condensate storage tanks (CST) to the AFS pumps causes AFS pump burnup. The SAFS uses two motor-driven pumps which can be aligned to separate service water system (SWS) loops. The SAFS provides the same features as the AFS pumps with regard to functional capability and power supply diversity; it is manually actuated from the control room.

4.1.3 Main Steam System

The safety-grade shutdown components associated with the main steam system (MSS) are the main steam isolation valves (MSIV), the steam safety valves, and the steam atmospheric dump valves. Each of the two steam generators is equipped with an air-operated, solenoid-controlled MSIV, four steam safety valves, and one air-operated atmospheric dump valve. The MSIVs fail 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 sufficient for maintaining hot shutdown or for cooldown of the RCS below 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 cirulating 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.

4.1.4 Service Water System

The service water system (SWS) 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. Under accident conditions, one pump is sufficient to supply essential loads. The SWS piping is arranged so that there are at least two flow paths to each essential load; non-essential loads are automatically isolated on a safeguards actuation signal. Valving is provided to isolate any single failure and to permit continued operation of the system. The SWS valve lineup splits the system into two independent trains. Safety-related equipment (diesel generators, AFS supply, containment ventilation coolers, etc.) is split between the trains so that the loss of one SWS loop will affect only half of the redundant safety-related equipment capacity. Motor-operated valves which isolate non-essential SWS loads, as well as the system pumps, are operable from the control room. Power for the SWS pumps is provided by the 480V emergency buses which can be supplied by onsite (emergency diesels) or offsite power. One SWS pump per emergency diesel is automatically started during post-accident diesel load sequencing.

4.1.5 Chemical and Volume Control System

The chemical and volume control system (CVCS) provides borated water from the boric acid tanks (BAT) or from the refueling water storage tank (RWST) through three positive displacement charging pumps to the RCS. The capacity of one pump (46 gpm) is sufficient to compensate for contraction of the RCS coolant during normal cooldown. One charging pump alone, or with one boric acid transfer pump, can provide cold shutdown

boration requirements immediately 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 which renders the system susceptible to a single failure which could prevent charging for boration and coolant contraction during cooldown. Should this occur, a redundant method of charging and boration exists by means of the high pressure safety injection (HPSI) system. Any of the three HPSI pumps can be lined up from the control room to take a suction on the BATs or the RWST and to inject borated water into the RCS via the HPSI lines.

4.1.6 Component Cooling Water System

The component cooling water system (CCW) system consists of two pumps, two heat exchangers, a surge tank and connecting valves and piping. During normal full power operation, or for post-accident operation, one component cooling pump and one component cooling heat exchanger accommodate the heat removal loads. The standby pump and heat exchanger provide 100 percent 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 CCW pumps receive power from the redundant 480V emergency buses which can be supplied by onsite or offsite power. The CCW system is normally operated from the control room. The surge tank accommodates expansion, contraction and inleakage of water, and ensures a continuous component cooling water 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 pump inlet header 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.

4.1.7 Residual Heat Removal System

The residual heat removal system (RHR) system consists of a single drop line from the RCS hot leg through two redundant pumps and their associated heat exchangers and back to the RCS via a single header. Each pump can be manually cross-connected to the alternate heat exchanger for increased reliability. Normal cooldown of the RCS is accomplished by operating both pumps and heat exchangers; however, a lesser cooldown rate can be achieved with only one pump. One heat exchanger can effect cooldown approximately 30 hours after shutdown. Each RHR pump is supplied power from separate redundant 480V emergency buses which can receive power from either onsite or offsite sources. The system is normally operated from the control room.

4.1.8 Electrical Instrumentation and Power Systems

Table 4.2 provides a list of the instruments required 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 RCS pressure, RCS 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. The asterisk in the "instrument location" column of the table indicates which indicators are located outside the control room at local shutdown panels.

Table 4.2 List of safe shutdown instruments.

Component/ System	Instrument	Instrument Location	Reference
Main Steam	Steam generator level LT & LI 460, 461 and 470, 471	LT Inside Containment LI Control Room*	Dwg. 33013-519
Reactor Coolant	Pressurizer level LT & LI, 426, 427, 428, 433	LT Inside Containment Control Room*	Dwg. 33013-424
	Pressurizer pressure PT & PT 449, 429, 430, 431	PT Inside Containment PI Control Room*	Dwg. 33013-424
	RCS temperature TE & TI 409 A & B and 410 A & B	TE Inside Containment TI Control Room	Dwg. 33013-424
Auxiliary Feed	AFWS flow FT 2021, 2022, 2023, 2024 FI 2021, 2022, 2023, 2024	FT Intermed. Build. FI Control Room*	Dwg. 33013-519
	SAFS flow FT & FT 4084, 4085	FT Aux. Build. Addition FI Control Room*	Dwg. D-302-071-E
Service Water	Pump discharge press. PT 2160 & 2161 PI 2160 & 2161	PT Screen House PI Control Room	Dwg. 33013-529
Chemical and Volume Control	Charging flow FIT 128, FI 128	FIT Auxiliary Build. FI Control Room	Dwg. 33013-433
	RWST level LT 920, LI 920	LT Auxiliary Build. LI Control Room	Dwg. 33013-425

*Indicators are also available at local shutdown panels.

Table 4.2 List of safe shutdown instruments. (Continued)

Component/ System	Instrument	Instrument Location	Reference
Component Cooling Water	System flow FIT 619	FIT Auxiliary Build. Low flow alarm in control room	Dwg. 33013-436
	Surge tank level LIT 618	LIT Auxiliary Build. LI Control Room	Dwg. 33013-435
Residual Heat Removal	System flow FT 626, FI 626	FT Auxiliary Build. FI Control Room	Dwg. 33013-436
Diesel Generator	Generator output voltage and current	Control Room	
Emergency AC Power	480 V Busses 14, 16, 17, 18, voltage indication	Control Room	
Emergency DC Power	125 VDC Busses 1 and 2 voltage indication	Control Room	

Offsite emergency power is provided through a single 4.16 kV station auxiliary transformer. Therefore the BTP RSB 5-1 [Ref. 5] assumption on loss of onsite emergency power, i.e., loss of both diesel generators renders the offsite emergency power susceptible to single failure. The acceptability of this design was reviewed during the Provisional Operating License review, and it was concluded that, because of the demonstrated high reliability of the type of transformers involved, the absence of a redundant transformer does not significantly affect the reliability of offsite power. A secondary source of offsite power can be made available via the unit auxiliary transformer by manually disconnecting flexible connections at the main generator terminals. This design meets the current NRC requirements for offsite power supplies (GDC-17), providing that disconnection of the flexible connections at the main generator terminals can be accomplished within the time constraints imposed by coolant water inventory and battery life, even though it deviates from the guidelines of BTP RSB 5-1 [Ref. 5].

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-volt buses. Each diesel can also be started locally or from the control room.

Table 4.3 details the safe shutdown systems power source and location.

Table 4.3. Safe shutdown systems power source and location.

System	Power Source	Location
Reactor Protection Reactor Breakers Reactor Bistables	DC power, Instrument buses	Control Room (289')
Main Steam		
Safety Valves	- - - - -	Intermediate Build. (278')
Isolation Valves	Air (fail closed)	Intermediate Build. (278')
Atmos. Dump Valves	Air or manual	Intermediate Build. (278')
Auxiliary Feed		
Motor Driven Pumps A, B	A-bus 14, B-bus 16	Intermediate Build. (253')
Turbine Driven Pump	Steam driven	Intermediate Build. (253')
Standby Pumps C, D	C-bus 14, D-bus 16	Aux. Build. Addition (270')
Service Water Pumps A, B, C, D	A,C-bus 18 B,D-bus 17	Screen House (253') Screen House (253')
Chemical and Volume Control pumps A, B, C	A-bus 14 B, C-bus 16	Auxiliary Build. (235') east
Refueling Water Storage Tank	- - - - -	Auxiliary Build.
Component Cooling Water		
pumps A, B	A-bus 14, B-bus 16	Auxiliary Build. (271')
Heat Exchangers	- - - - -	Auxiliary Build. (271')
Residual Heat Removal		
pumps A, B	A-bus 14, B-bus 16	Auxiliary Build. (219') RHR pit
Heat Exchangers	- - - - -	Auxiliary Build. (219')
Diesel Generators	125VDC control power	Diesel Room N side of Turbine Build. (253')
1A		
1B	125VDC control power	Diesel Room N side of Turbine Build. (253')

Table 4.3. Safe shutdown systems power source and location (continued).

System	Power Source	Location
480 V, bus 14	Diesel 1A or Offsite Power	Auxiliary Build. (271')
480 V, bus 16	Diesel 1B or Offsite Power	Auxiliary Build. (263')
480 V, bus 17	Diesel 1B or Offsite Power	Screen House (253')
480 V, bus 18	Diesel 1A or Offsite Power	Screen House (253')
Instrument buses 1A, 1B, 1C, 1D	1A-Inverter 1, 1B-480V MCC 1C-Inverter 2, 1D-480V MCC	Control Room (289')
Battery and Inverter 1A	- - - - -	Battery Room (253')
Battery and Inverter 1B	- - - - -	Battery Room (253')

5. EVALUATION AND CONCLUSIONS

5.1 REACTOR PROTECTION SYSTEM

The reactor protection system (RPS) 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. RPS 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 a-c power feed. Each reactor trip circuit is designed so that a trip occurs when the circuit is de-energized. 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

de-energize 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.

Based on a review of the documentation listed in the Reference Section of this report, we conclude that the RPS complies to the current licensing criteria listed in Section 2 of this report.

5.2 AUXILIARY FEEDWATER SYSTEM

The primary source of water to the auxiliary feedwater system (AFS) is from the condensate storage tanks (CST) via nonseismic CST supply lines. The backup source of water to the AFS is from the seismic Class 1 service water system (SWS) via two separate paths; one path provides suction to the turbine-driven pump, the other path provides suction to two motor-driven pumps. Manual action is required to isolate the AFS pump suctions from the CST and to line up the pumps to the SWS. All other functions of the AFS can be initiated, controlled, and monitored from the control room. The manual valve alignment of the AFS to the SWS can be performed by an operator dispatched from the control room. The NRC staff has determined that the manual lineup of the AFS suction to the SWS is justified under the "limited operator action outside the control room" provision of BTP RSB 5-1 [Ref. 5]. The two motor-driven pumps are powered from separate redundant 480 V emergency buses which can receive power from either onsite or offsite sources. Each motor-driven pump can provide 100 percent of the AFS flow required for decay heat removal and can be cross-connected to provide flow to either steam generator.

A standby auxiliary feedwater system (SAFS) provides flow in case suction loss from the condensate storage tanks (CST) to the AFs pumps causes AFS pump burnup. The SAFS uses two motor-driven pumps which can be aligned to separate SWS loops. The SAFS provides the same features as the AFS pumps with regard to functional capability and power supply diversity;

it is manually actuated from the control room. The NRC staff evaluation of the SAFS is contained in reference 6.

Based on a review of the documentation listed in the Reference Section of this report, we conclude that AFS complies to the current licensing criteria listed in Section 2 of this report.

5.3 MAIN STEAM SYSTEM

The safety-grade shutdown components associated with the main steam system (MSS) are the main steam isolation valves (MSIV), the steam safety valves, and the steam atmospheric dump valves. Each of the two steam generators is equipped with an air-operated, solenoid-controlled MSIV, four steam safety valves, and one air-operated atmospheric dump valve. The MSIVs fail 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 sufficient for maintaining hot shutdown or for cooldown of the RCS below hot shutdown conditions.

Boiling of the 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.

The MSS-level instrumentation 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. Loop A steam generator level is monitored by level transmitters LT-460, LT-461, LT-462 and LT-463. Loop A steam generator level is indicated in the control room by level indicators LI-461, LI-462 AND LI-463. LI-460A provides loop A steam generator level indication at the auxiliary feedwater pump panel. LI-460B provides loop A steam generator level indication at the main feedwater control valves. Loop B steam generator level is monitored by level transmitters LT-470, LT-471, LT-472 and LT-473. Loop B steam generator level is indicated in the control room by level indicators LI-471, LI-472 and LI-473A. LI-470A provides loop B steam generator level indication at the auxiliary feedwater pump panel. LI-470B provides loop B steam generator level indication at the main feedwater control valves. [Ref. 7, drawings BD-8, BD-9, BD-18 and BD-19].

Based on a review of the documentation listed in the Reference Section of this report, we conclude that the MSS complies to the current licensing criteria listed in Section 2 of this report.

5.4 SERVICE WATER SYSTEM

The service water system (SWS) 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. Under accident conditions, one pump is sufficient to supply essential loads. The SWS piping is arranged so that there are at least two flow paths to each essential load; non-essential loads are automatically isolated on a safeguards actuation signal. Valving is provided to isolate any single failure and to permit continued operation of the system. The SWS valve lineup splits the system into two independent trains. Safety-related equipment (diesel generators, AFS supply, containment ventilation coolers, etc.) is split between the trains so that the loss of one SWS loop will affect only half of the redundant safety-related equipment capacity. Motor-operated valves which isolate non-essential SWS loads, as well as the system pumps, are operable

from the control room. Power for the SWS pumps is provided by the 480V emergency buses which can be supplied by onsite (emergency diesels) or offsite power. One SWS pump per emergency diesel is automatically started during post-accident diesel load sequencing.

Based on a review of the documentation listed in the Reference Section of this report, we conclude that the SWS complies to the current licensing criteria listed in Section 2 of this report.

5.5 CHEMICAL AND VOLUME CONTROL SYSTEM

The chemical and volume control system (CVCS) provides borated water from the boric acid tanks (BAT) or the refueling water storage tank (RWST) through three positive displacement charging pumps to the RCS. The capacity of one pump (46 gpm) is sufficient to compensate for contraction of the RCS coolant during normal cooldown. One charging pump alone, or with the boric acid transfer pump, can provide cold shutdown boration requirements immediately following reactor shutdown. Borated water for the charging pumps would be supplied from the RWST by manually opening valve 358 to bypass an air-operated valve in the charging pump suction lines. 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 which renders the system susceptible to a single failure which could prevent charging for boration and coolant contraction during cooldown. Should this occur, a redundant method of charging and boration exists by means of the high pressure safety injection (HPSI) system. Any of the three HPSI pumps can be lined up from the control room to take a suction on the BATs or the RWST and to inject borated water into the RCS via the HPSI lines.

Based on a review of the documentation listed in the Reference Section of this report, we conclude that the CVCS complies to the current licensing criteria listed in Section 2 of this report.

5.6 COMPONENT COOLING WATER SYSTEM

The component cooling water system (CCW) system consists of two pumps, two heat exchangers, a surge tank and connecting valves and piping. During normal full-power operation or for post-accident operation, one component cooling pump and one component cooling heat exchanger accommodate the heat removal loads. The standby pump and heat exchanger provide 100 percent 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 CCW pumps receive power from the redundant 480V emergency buses which can be supplied by onsite or offsite power. The CCW system is normally operated from the control room. The surge tank accommodates expansion, contraction and inleakage of water, and ensures a continuous component cooling water 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 pump inlet header 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.

Based on a review of the documentation listed in the Reference Section of this report, we conclude that the CCW system complies to the current licensing criteria listed in Section 2 of this report except for the following:

(1) The single failure criterion is NOT met because of the single discharge line from the CCW pumps through MOV-817 to the following four cooling loops: RCP 1A, RCP 1B, Reactor Support Cooling and the Excess Letdown HX. If MOV-817 were to fail in the closed position CCW to the above four loops would be lost [Ref. 8, drawing 33013-435-A].

(2) The failure of check valve 816 to remain open would cause CCW flow to the above four loops to be lost [Ref. 8, drawing 33013-435-A].

5.7 RESIDUAL HEAT REMOVAL SYSTEM

The suction line of the residual heat removal system (RHR) system is isolated from the loop A hot leg of the RCS by MOV-700 and MOV-701 in series. MOV-700 and MOV-701 normally operate in the closed position and do not change position upon loss of power (fail as is). MOV-700 is operable with either onsite or offsite power from essential bus 14 via MCC 1C. MOV-701 is operable with either onsite or offsite power from essential bus 16 via MCC 1D.

The discharge line of the RHR system is isolated from the loop B cold leg of the RCS by MOV-720 and MOV-721 in series. MOV-720 and MOV-721 normally operate in the closed position and do not change position upon loss of power (fail as is). MOV-720 is operable with either onsite or offsite power from essential bus 14 via MCC 1C. MOV-721 is operable with either onsite or offsite power from essential bus 16 via MCC 1D.

The RHR system discharge line is not used for an ECCS function that would require MOV-720 or MOV-721 to open; however, a branch of the RHR discharge line provides LPSI to the rector vessel via parallel lines. Isolation between the RHR system and LPSI injection into the reactor vessel is provided by two separate paths from the RHR discharge line, with each path containing an MOV and check valve. MOV-852A and check valve 853A provide isolation in one path, while MOV-852B and check valve 853B provide isolation in the other path. MOV-852A and MOV-852B normally operate in the closed position and do not change position upon loss of power (fail as is). MOV-852A is operable with either onsite or offsite power from essential bus 14 via MCC 1C. MOV-852B is operable with either onsite or offsite power from essential bus 16 via MCC 1D.

The suction line of the RHR system, when functioning in the injection phase of LPSI, commences at the RWST to MOV-856 and check valve 854 in series, then to a parallel branch where MOV-704A provides a path to

RHR pump 2. MOV-856 normally operates in the closed position and does not change position upon loss of power (fails as is). MOV-856 is operable with either onsite or offsite power from essential bus 14 via MCC 1C. MOV-704A and MOV-704B normally operate in the open position and do not change position upon loss of power (fail as is). MOV-704A is operable with either onsite or offsite power from essential bus 14 via MCC 1C. MOV-704B is operable with either onsite or offsite power from essential bus 16 via MCC 1D.

Two separate paths provide suction to the RHR system when it is functioning in the recirculation phase of LPSI. Both paths commence at the containment sump and terminate at the RHR pumps. MOV-850A and MOV-851A in series provide the path to RHR pump 1. MOV-850B and MOV-851B in series provide the path to RHR pump 2. MOV-850A, MOV-850B, MOV-851A and MOV-851B normally operate in the closed position and do not change position upon loss of power (fail as is). MOV-850A and MOV-851A are operable with either onsite or offsite power from essential bus 14 via MCC 1C. MOV-850B and MOV-851B are operable with either onsite or offsite power from essential bus 16 via MCC 1D.

Both RHR pumps are operable with either onsite or offsite power. RHR pump 1 is powered from essential bus 14, RHR pump 2 is powered from essential bus 16.

Section 6.1.1 of the FSAR [Ref. 9] states in part that:

> A comprehensive program of plant testing is formulated for all equipment systems and systems control vital to the functioning of ESFs. The program consists of performance tests of individual pieces of equipment, integrated tests of the system as a whole, and periodic tests of the actuation circuitry and mechanical components to assure reliable performance, upon demand, throughout the plant lifetime.

Section 6.2.1 of the FSAR [Ref. 9] states in part that:

> Design provisions are made so that active components of the SIS can be tested periodically for operability and functional performance.

Each active component can be individually activated on the normal power source at any time during plant operation.

An integrated system test can be performed during the late stages of plant cooldown when the RHR loop is in service. This test would not introduce flow into the RCS but would demonstrate the operation of the valves, pump circuit breakers, and automatic circuitry upon initiation of safety injection.

Section 6.2.5 of the FSAR [Ref. 9] states in part that:

Testing is conducted during plant shutdown to demonstrate proper automatic operation of the SIS. A test signal is applied to initiate automatic action and verification made that the SI pumps attain required discharge heads. The test demonstrates the operation of the valves, pump circuit breakers, and automatic circuitry. The test is considered satisfactory if control board indication and visual observations indicate all components have operated and sequenced properly. Flow in each of the high head SI headers and in the mainflow line for the RHR pumps is monitored by flow indicators. Pressure instrumentation is also provided for the main flow paths of the SI and RHR pumps. Accumulator isolation valves are blocked closed for this test. The sequence for recirculation operation may be tested following the above injection phase to demonstrate proper sequencing of valves and pumps.

To initiate the full operational sequence test, the SI block switch is moved to the unblock position to provide control power allowing the automatic actuation of the safety injection signal relays from the pressurizer.

Simultaneously, the breakers supplying normal power to 480-volt buses are tripped, operation of the diesel-generator power system commences automatically. The SI pumps and the RHR pumps start automatically following the prescribed loading sequence. The valves operate automatically to align the flow path for injection into the RCS.

The functional test is repeated for the various modes of operation needed to demonstrate performance at partial effectiveness, i.e., to demonstrate the proper loading sequence with loss of one of the diesel generator power sources, and to demonstrate the correct automatic starting of a second pump should the first

pump fail to respond. These latter cases are performed without delivery of water to the RCS, but include starting of all pumping equipment involved in each test.

Section 4.1.a of the Ginna Technical Specifications states that:

> Calibration, testing, and checking of analog channels and testing of logic channels shall be performed as specified in Table 4.1-1.

Table 4.1-1 entitled "Minimum Frequencies for Checks, Calibrations, and Tests of Instrument Channels" provides the following information regarding RHR/LPSI-related instrument channels:

(1) RHR Pump Flow is calibrated during each refueling shutdown; channel check and channel test are not applicable.

(2) RWST Level is calibrated during each refueling shutdown; channel check and channel test are not applicable.

(3) Containment Sump Level is calibrated during each refueling shutdown; channel check and channel test are not applicable.

Section 4.5.1.1.a of the Ginna Technical Specification states in part that:

> The Safety Injection System tests shall be 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 safety injection signal will be applied to initiate operation of the system. The safety injection and residual heat removal pump motors are prevented from starting during the test.

Section 4.5.2.1.a of the Ginna Technical Specifications states in part that:

> Except during cold or refueling shutdowns the safety injection pumps, residual heat removal pumps, and containment spray pumps shall be started at intervals not to exceed one month.

Section 4.5.2.2.a of the Ginna Technical Specifications states that:

> The refueling water storage tank outlet valves shall be tested at intervals not to exceed one month.

Section 4.4 of the SEP Review of Safe Shutdown Systems for the R.E. Ginna Nucler Power Plant [Ref. 1] states in part that:

> The RHR isolation valve operability and interlocks cannot be tested during the RHR cooling mode of operation. This test requirement is not applicable to the Ginna facility, since the interlocks function only when the RHR isolation valves are shut.

Based on a review of the documentation listed in the Reference Section of this report, we conclude that the RHR system complies to the current licensing criteria listed in Section 2 of this report except for the following:

(1) The single failure criterion is NOT met because there is a single inlet line to the RHR pumps through MOV-700 and MOV-701 in series from the RCS Loop A hot leg [Ref. 10, drawing 33013-436-A]. If either MOV-700 or MOV-701 were to fail in the closed position, the suction path to the RHR pumps would be lost.

(2) The single failure criterion is NOT met because there is a single discharge line between the RHR heat exchangers through MOV-720 and MOV-721 in series to the RCS Loop B cold leg [Ref. 10, drawing 33013-436-A]. If either MOV-720 or MOV-721 were to fail in the closed position, the discharge path of the RHR pumps would be lost.

(3) The single failure criterion is NOT met when the RHR system is functioning in the injection phase of LPSI because there is a single inlet line to the RHR pumps through MOV-856 and check valve 854 in series from the RWST [Ref. 11, drawing 33013-425-A]. If MOV-856 were to fail in the closed

position, the suction path to the RHR pumps would be lost.

(4) The RHR system testability fails to satisfy RG 1.22 because the RHR pumps are disabled during the ECCS system test. Section 6.2.5 of the FSAR states that the SI and RHR pumps are tested as a part of system functional tests. Section 4.5.1.1 of the Ginna Technical Specifications states that the SI and RHR pump motors are prevented from starting during the system test.

(5) The RHR system fails to satisfy BTP RSB 5-1 and RG 1.22 because the RHR isolation valves and their associated interlocks are not tested.

5.8 ELECTRICAL INSTRUMENTATION AND POWER SYSTEMS

Table 4.2 (see Section 4) provides a list of the instruments required 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 RCC pressure, RCS 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 indication of actual or impending degradation of system performance. The asterisk in the "instrument location" column of the table indicates which indicators are located outside the control room at local shutdown panels.

Offsite emergency power is provided through a single 4.16 kV station auxiliary transformer. Therefore the BTP RSB 5-1 [Ref. 5] assumption on loss of onsite emergency power, i.e., loss of both diesel generators renders the offsite emergency power susceptible to single failure. The acceptability of this design was reviewed during the Provisional Operating License review, and it was concluded that, because of the demonstrated high reliability of the type of transformers involved, the absence of a redundant transformer does not significantly affect the reliability of

offsite power. A secondary source of offsite power can be made available via the unit auxiliary transformer by manually disconnecting flexible connections at the main generator terminals. This design meets the current NRC requirements for offsite power supplied (GDC-17), providing that disconnection of the flexible connections at the main generator terminals can be accomplished within the time constraints imposed by coolant water inventory and battery life, even though this deviates from the guidelines of BTP RSB 5-1 [Ref. 5].

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-volt buses. Each diesel can also be started locally or from the control room.

Table 4.3 (see Section 4) details the safe shutdown systems power source and location.

6. SUMMARY

Four loops of the CCW system fail to meet the single failure criterion.

Both the suction and discharge paths of the RHR system fail to meet the single failure criterion during the RHR cooling mode of operation.

The suction path of the RHR system fails to meet the single failure criterion during the injection phase of the RHR LPSI function.

The RHR system fails to satisfy current licensing criteria because the RHR pumps are disabled during functional system tests.

The RHR system fails to satisfy current licensing criteria because the RHR isolation valves and their associated interlocks are not tested.

Offsite emergency power fails to satisfy the single failure criterion.

Each of the above items of non-compliance to current licensing criteria should be investigated and resolutions sought during the integrated DBE reviews.

REFERENCES

1. SEP Review of Safe Shutdown Systems for the R.E. Ginna Nuclear Power Plant, Revision 1, undated.

2. U.S. Nuclear Regulatory Commission, Code of Federal Regulations, Title 10, Part 50, Appendix A (General Design Criteria), 1979.

3. U.S. Nuclear Regulatory Commission, Standard Review Plan NUREG-75/087, Revision 1.

4. U.S. Nuclear Regulatory Commission, Safety Topic III-1, Classification of Structures, Systems and Components.

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

6. NRC letter, D. Ziemann to L. White, dated August 24, 1979, forwarding Amendment 29 to the Ginna Operating License.

7. Foxboro drawings BD-2 through BD-19 for the Ginna Nuclear Power Station.

8. Rochester Gas and Electric Corp. drawing 33013-435-A, Auxiliary Coolant System.

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

10. Rochester Gas and Electric Corp. drawing 33013-436-A, Auxiliary Coolant System.

11. Rochester Gas and Electric Corp. drawing 33013-425-A, Safety Injection System.

APPENDIX A
NRC SAFETY TOPICS RELATED TO THIS REPORT

III-1	Classification of Structures, Systems, and Components.
IV-2	Reactivity Control Systems, Including Functional Design and Protection Against Single Failures.
V-3	Overpressurization Protection.
V-8	Steam Generator (SG) Integrity.
V-10.A	RHR Heat Exchanger Tube Failures.
V-10.B	RHR Reliability.
V-11.A	Requirements for Isolation of High and Low Pressure Systems.
V-11.B	RHR Interlock Requirements.
VI-10.A	Testing of RTS and ESF Including Response Time Testing.
VI-10.B	Shared Engineered Safety Features, Onsite Emergency Power, and Service Systems for Multiple Unit Facilities.
VII-1.A	Isolation of RPS from Non-Safety Systems, Including Qualifications of Isolation Devices.
VII-1.B	Trip Uncertainty and Setpoint Analysis Review of Operating Data Base.
VII-2	ESF System Control Logic and Design.
VII-4	Effects of Failure in Non-Safety Related Systems on Selected ESFs.
IX-3	Station Service and Cooling Water Systems.
IX-4	Boron Addition System.
X	Auxiliary Feedwater System.
XV-1	Decrease in Feedwater Temperature, Increase in Feedwater Flow, Increase in Steam Flow, and Inadvertent Opening of a Steam Generator Relief or Safety Valve.
XV-2	Spectrum of Steam System Piping Failures Inside and Outside of Containment (PWR).

APPENDIX A (Continued)
NRC SAFETY TOPICS RELATED TO THIS REPORT

XV-4	Loss of Non-Emergency A-C Power to Station Auxiliaries..
XV-5	Loss of Normal Feedwater Flow.
XV-6	Feedwater System Pipe Breaks Inside and Outside Containment.
XV-7	Reactor Coolant Pump Rotor Seizure and Reactor Coolant Pump Shaft Break.
XV-10	CVCS Malfunction that Results in a Decrease in the Boron Concentration in the Reactor Coolant (PWR).
XV-14	Inadvertent Operation of ECCS and CVCS Malfunction that Increases Reactor Coolant Inventory.
XV-15	Inadvertent Opening of PORV.
XV-17	Radiological Consequences of Steam Generator Tube Failure (PWR).
XV-24	Loss of All A-C Power.
XVI	Technical Specifications.

CEB/amr/#5/#5