Georgia Power Company
333 Piedmont Avenue
Atlanta, Georgia 30308
Telephone 404 526-3195

Mailing Address
40 Inverness Center Parkway
Post Office Box 1295
Birmingham, Alabama 35201
Telephone 205 868-5581

the southern electric system

W. G. Hairston, III
Senior Vice President
Nuclear Operations

HL-2196
003362

April 29, 1992

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, D.C. 20555

PLANT HATCH - UNIT 1
NRC DOCKET 50-321
OPERATING LICENSE DPR-57
LICENSEE EVENT REPORT
SINGLE FAILURE VULNERABILITIES DISCOVERED IN
THE MAIN CONTROL ROOM ENVIRONMENTAL CONTROL SYSTEM

Gentlemen:

In accordance with the requirements of 10 CFR 50.73(a)(2)(v), Georgia Power Company is submitting the enclosed revision to a Licensee Event Report (LER) concerning single failure vulnerabilities discovered in the main control room environmental control system. This event occurred at Plant Hatch - Unit 1.

Sincerely,

W. G. Hairston, III

W. G. Hairston, III

OCV/cr

Enclosure: LER 50-321/1991-009, Rev. 1

cc: (See next page.)

JE22

Georgia Power

cc: Georgia Power Company
Mr. H. L. Sumner, General Manager - Nuclear Plant
NORMS

U.S. Nuclear Regulatory Commission, Washington, D.C.
Mr. K. Jabbour, Licensing Project Manager - Hatch

U.S. Nuclear Regulatory Commission, Region II
Mr. S. D. Ebneter, Regional Administrator
Mr. L. D. Wert, Senior Resident Inspector - Hatch

003362

NRC Form 366 (6-89) U.S. NUCLEAR REGULATORY COMMISSION APPROVED OMB NO. 3150-0104 EXPIRES: 4/30/92

LICENSEE EVENT REPORT (LER)

FACILITY NAME (1)	DOCKET NUMBER (2)	PAGE (3)
PLANT HATCH, UNIT 1	05000321	1 OF 9

TITLE (4)
SINGLE FAILURE VULNERABILITIES DISCOVERED IN THE MAIN CONTROL ROOM ENVIRONMENTAL CONTROL SYSTEM

EVENT DATE (5)			LER NUMBER (6)			REPORT DATE (7)			OTHER FACILITIES INVOLVED (8)	
MONTH	DAY	YEAR	YEAR	SEQ NUM	REV	MONTH	DAY	YEAR	FACILITY NAMES	DOCKET NUMBER(S)
									HATCH, UNIT 2	05000366
07	12	91	91	009	01	04	29	92		05000

OPERATING MODE (9): 1
POWER LEVEL: 100

THIS REPORT IS SUBMITTED PURSUANT TO THE REQUIREMENTS OF 10 CFR (11)

[ ] 20.402(b)	[ ] 20.405(c)	[ ] 50.73(a)(2)(iv)	[ ] 73.71(b)
[ ] 20.405(a)(1)(i)	[ ] 50.36(c)(1)	[X] 50.73(a)(2)(v)	[ ] 73.71(c)
[ ] 20.405(a)(1)(ii)	[ ] 50.36(c)(2)	[ ] 50.73(a)(2)(vii)	[ ] OTHER (Specify in Abstract below)
[ ] 20.405(a)(1)(iii)	[ ] 50.73(a)(2)(i)	[ ] 50.73(a)(2)(viii)(A)	
[ ] 20.405(a)(1)(iv)	[ ] 50.73(a)(2)(ii)	[ ] 50.73(a)(2)(viii)(B)	
[ ] 20.405(a)(1)(v)	[ ] 50.73(a)(2)(iii)	[ ] 50.73(a)(2)(x)	

LICENSEE CONTACT FOR THIS LER (12)

NAME	TELEPHONE NUMBER AREA CODE	
STEVEN B. TIPPS, MANAGER NUCLEAR SAFETY AND COMPLIANCE, HATCH	912	367-7851

COMPLETE ONE LINE FOR EACH FAILURE DESCRIBED IN THIS REPORT (13)

CAUSE	SYSTEM	COMPONENT	MANUFAC-TURER	REPORT TO NPRDS		CAUSE	SYSTEM	COMPONENT	MANUFAC-TURER	REPORT TO NPRDS

SUPPLEMENTAL REPORT EXPECTED (14)

[ ] YES (If yes, complete EXPECTED SUBMISSION DATE) [X] NO

EXPECTED SUBMISSION DATE (15) MONTH DAY YEAR

ABSTRACT (16)

On 7/12/91, at approximately 1205 CDT, Units 1 and 2 were in the Run mode at 2436 CMWT (100 percent of rated thermal power). At that time, nonlicensed personnel determined that the Main Control Room Environmental Control (MCREC) system did not comply with the single failure design criterion as required by the plant's Final Safety Analysis Report. Specifically, the air conditioning subsystem of the MCREC system could not sustain a single failure to the system's class 1E power supply and still maintain the Main Control Room temperature within the Technical Specifications limit. Consequently, only one of two independent, redundant MCREC systems could be assumed to be operable contrary to the plant's Technical Specifications which require that both systems be operable. A limiting condition for operation (LCO) was entered per the Technical Specifications. The design review performed per the commitment made in revision 0 of this report and subsequent testing revealed additional single failure concerns.

The causes of the single failure vulnerabilities were less than adequate design and failure to fully understand the design of the system.

Corrective actions include implementing design changes to the system and revising the system operating procedure.

TEXT

PLANT AND SYSTEM IDENTIFICATION

General Electric - Boiling Water Reactor
Energy Industry Identification System Codes are identified in the text as (EIIS Code XX).

DESCRIPTION OF EVENT

On 7/12/91, at approximately 1205 CDT, Units 1 and 2 were in the Run mode at 2436 CMWT (100 percent of rated thermal power). At that time, nonlicensed Nuclear Safety and Compliance personnel determined that the air conditioning subsystem of the Main Control Room Environmental Control (MCREC, EIIS Code VI) system did not meet the single failure criterion specified in the plant's Final Safety Analysis Report (FSAR). Specifically, a single failure resulting in the loss of one division of the Class 1E electrical power supply to the MCREC system would result in the air conditioning subsystem operating at 50 percent of its design capacity and, thus, the Main Control Room could not be maintained (MCR, EIIS Code NA) at or below 105 degrees Fahrenheit as required by Unit 2 Technical Specification, section 4.7.2.a. With the single failure criterion not met, only one as opposed to two independent MCREC trains could be assumed to be operable, which was contrary to the requirements of Unit 1 Technical Specification, section 3.12.A.1.a and Unit 2 Technical Specification, section 3.7.2.a. (The MCREC system is shared by both units.) Deficiency Card 1-91-3110 was written to document the condition and track corrective actions. Licensed personnel were notified and Limiting Conditions for Operation (LCOs) 1-91-364 (for Unit 1) and 2-91-319 (for Unit 2) were initiated per the respective unit's Technical Specifications.

The MCREC air conditioning subsystem consists of three 50 percent capacity trains. Each train includes an air handling unit (AHU; 1Z41-B003A, B, and C), a refrigeration unit (1Z41-B008A, B, and C), and support equipment. Two trains, trains 'A' and 'C', are normally in operation providing 100 percent cooling capacity and train 'B' is normally in standby. The standby train is designed to start automatically on a low flow condition occurring in either of trains 'A' or 'C'.

The MCREC air conditioning subsystem receives power from two independent and redundant Class 1E essential buses (EIIS Code EB). Division I bus 1R24-S002 supplies power to train 'A'. Division II bus 1R24-S003 supplies power to train 'B' - the standby train. Swing bus 1R24-S029 supplies power to Train 'C'. The swing bus can be configured to receive power from Division II bus 1R24-S003 (the normal supply) or from Division I bus 1R24-S002 (the alternate supply).

The normal system line-up has the 'A' and 'C' trains in operation with train 'C' being powered from Division II bus 1R24-S003 via swing bus 1R24-S029. Train 'B' was designed to provide backup cooling in the event that either train 'A' or 'C' became inoperative. If train 'A' became inoperative, then trains 'C' and 'B' would be powered from Division II bus 1R24-S003. If Division II bus 1R24-S003 failed, bus 1R24-S029 could be transferred to the Division I bus 1R24-S002 restoring power to train 'C'. In this case, trains 'A' and 'C' would be operating and both powered from Division I bus 1R24-S002.

TEXT

In 1989, plant personnel requested the Architect Engineer to specify which power supply for 1R24-S029 was the preferred normal supply and which was the alternate supply. The Architect Engineer, in responding to the request, evaluated the loading of the buses and determined that operating the 'A' and 'C' trains concurrently and powered from the same bus, 1R24-S002, or operating 'B' and 'C' trains concurrently and powered from the same bus, 1R24-S003, would result in overloading the feeder cables to the applicable bus. To address this problem, the Architect Engineer recommended that train 'C' be aligned to the divisional bus that was not supplying power to the other operating train (i.e., Division II bus 1R24-S003 if train 'A' were in operation or Division I bus 1R24-S002 if train 'B' were in operation). Accordingly, procedure 34SO-Z41-001-1S, "Control Room Ventilation System," was revised to incorporate the recommendation.

On 7/12/91, Nuclear Safety and Compliance personnel had been reviewing the adequacy of the procedural instructions in 34SO-Z41-001-1S for transferring the power supply for train 'C' when they determined that the inability to load two of the system trains simultaneously on one Class 1E divisional bus presented a single failure concern. In particular, if each bus could only power one train, then loss of either bus would result in only one train being operable, which is insufficient for cooling the Main Control Room.

Personnel also noted in the review that the power supply configuration for the controls of train 'C' also presented a single failure concern. The 'C' train controls have a dedicated power supply (Class 1E Division II bus 1R24-S003) whereas the 'C' train electrical components are powered from the swing bus, 1R24-S029. This configuration would result in a loss of control power to the 'C' train in the event that the Division II bus were inoperable. Personnel subsequently wrote a deficiency card on the two deficient conditions and notified licensed personnel.

To resolve the power supply problem for the train 'C' controls, Design Change Request (DCR) 91-130 was developed and implemented. The power supply has been reconfigured so that upon a loss of power to the train 'C' controls, a transfer can be made to an alternate supply. Regarding the potential overload problem, an evaluation of the loads on buses 1R24-S002 and 1R24-S003 showed that several specific loads can be disconnected from the buses so that two trains can be powered from one bus without creating an overload condition. Therefore, as a temporary measure, procedure 34SO-Z41-001-1S was revised to require disconnecting selected loads should two trains have to be powered from the same bus. The feeder cables of each bus are sized to handle the resulting loads.

The described changes were completed by 7/16/91. LCO's 1-91-364 and 2-91-519 were subsequently terminated at approximately 1630 CDT, on 7/16/91.

As mentioned in the "Additional Information" section of this report, three previous similar events had been identified in which the MCREC system design was found to deviate from the single failure design criterion. In each case, the design was corrected to bring the system into compliance with the design

TEXT

criterion. These events indicated a possible generic problem with the design of the system. Consequently, per the commitment made in revision 0 of this report, a design review of the system was performed. The review was completed by 12/31/91. During the review, some potential single failure vulnerabilities were identified. Testing was performed on 12/30/91 and 4/2/92 to determine if these potential vulnerabilities actually could compromise the safety function of the MCREC system (i.e., were in fact single failure problems). As a result of the testing, four additional single failure vulnerabilities were confirmed to exist.

Each of the vulnerabilities identified affected the pressurization function of the MCREC system. The MCREC system is designed to automatically align to the pressurization mode in the event of an accident. In this mode, the system is isolated from areas adjacent to the MCR and radiologically filtered air is supplied to the MCR pressurizing it to $\geq$ 0.1 inches water gauge (WG) as required by the Technical Specifications. Simulation of the single failures during testing on 4/2/92 showed that the MCREC system was capable of pressurizing the MCR in the event of such a single failure, however, not to the required 0.1 inches WG.

In two of the four cases, exhaust ducts penetrating the MCR habitability envelope were not provided with independent, redundant isolation capability. Therefore, a failure of the single isolation damper to close in any one of the ducts during a pressurization mode actuation would result in the MCR habitability zone communicating with adjacent areas, affecting the pressurization of the MCR. These cases involved the exhaust ducts for the MCR men's bathroom and the two MCR exhaust fans. It was concluded from testing on 4/2/92 that a single failure of a damper to close in any one of these exhaust ducts during a pressurization mode actuation would not prevent pressurization of the MCR; however, it would prevent pressurization to the required 0.1 inches WG.

No immediate corrective actions were required on 4/2/92 when the problems were confirmed to exist. In regard to the MCR exhaust fan discharge ducts, current operating procedure 34SO-Z41-001-1S requires that the MCR exhaust fans be secured and the discharge isolation dampers be closed during normal operation. At one time, the exhaust system had been run continuously as allowed by the FSAR. However, due to the exhaust system operation causing high noise levels in the MCR, the system has since been secured and per procedure will only be operated in the purge mode for the purposes of smoke ejection in the event of a fire or some other off-normal event. With the dampers maintained closed, isolating the ducts, no single failure vulnerability exists. Consequently, no actions were required when the problem was confirmed to exist during testing on 4/2/92.

In regard to the men's MCR bathroom exhaust ducts, the test showed that failure of its single isolation damper to close did not affect pressurization of the MCR if the bathroom door was maintained closed. The doors are equipped with automatic closing devices and are, therefore, normally maintained closed. Consequently, no actions were required when the problem was confirmed to exist during testing on 4/2/92.

TEXT

The other two single failure vulnerabilities identified involved improper system alignment caused by personnel not fully understanding the design of the air conditioning subsystem. Normal line-up of the MCREC system included the 'A' and 'C' AHUs in run and the 'B' AHU in standby. (Only AHU 'B' has the standby/auto start capability.) In this configuration, a loss of one of the operating AHUs would result in AHU 'B' automatically starting. In the past, however, either the 'A' or 'C' AHU was manually turned off and on as necessary to assist in temperature control for personnel comfort in the MCR. Procedure 34SO-Z41-001-1S allowed operation of the system in this manner. During the design review, it was determined that the control logic for the 'B' AHU could only provide an automatic start capability for AHU 'B' if both 'A' and 'C' AHUs were in run. Consequently, any time that the 'A' or 'C' AHU had been shutdown for temperature control purposes, AHU 'B' would not automatically start upon a loss of the operating AHU. Thus, in this configuration, a single failure resulting in a loss of the operating AHU would result in no AHU's running.

Since the AHUs provide a portion of the driving head for the make-up air to the MCR (with the booster fan providing most of the driving head), the ability to pressurize the MCR would most likely be adversely affected if no AHUs were running. Consequently, on 12/13/91, when plant personnel were notified by the Architect Engineer that this potential single failure vulnerability existed, conservative actions were taken. Administrative LCO 1-91-833 was issued requiring that two AHUs be operated at all times such that no single failure could result in a loss of all operating AHUs. Consequently, on 4/2/92 when the problem was confirmed to exist, no further immediate actions were required. Additionally, the testing on 4/2/92 showed that operation of the booster fan alone could pressurize the MCR, however, not to the required 0.1 inches WG.

The other single failure introduced by the aforementioned line-up of the AHUs involves the booster fan discharge dampers. In a pressurization mode actuation, one booster fan automatically starts and three discharge dampers automatically open aligning the fan to the three MCREC system AHUs. In the event that the system was aligned with only one AHU running and the booster fan discharge damper associated with the running AHU failed to open in a pressurization mode actuation, the booster fan would be aligned to the two secured AHUs. Without the operating booster fan being aligned in series with an operating AHU, the make-up air flow to the MCR would be sufficient to pressurize the MCR, however, not to the required 0.1 inches WG, as was demonstrated during the 4/2/92 test.

No immediate corrective actions were required to mitigate this problem. LCO 1-91-833, which was in effect on 4/2/92, required that two AHUs be run at all times as mentioned previously. Consequently, even if a single failure of an active component resulted in a booster fan discharge damper to an operating AHU failing to open, the discharge damper to the other operating AHU would be unaffected and the pressurization requirements would be attained.

CAUSE OF EVENT

The causes of the single failure vulnerabilities were less than adequate design and a lack of fully understanding the design of the MCREC system. In regard to

TEXT

the AHU/refrigeration unit power scheme and the lack of independent, redundant isolation dampers in the exhaust ductwork, the system design was deficient in that it did not comply with the required single failure design criterion. In regard to the improper alignment of the MCREC system AHUs, plant personnel did not fully understand the design of the air conditioning subsystem. Specifically, plant personnel did not realize that operating one AHU unit introduced single failure vulnerabilities into the system.

REPORTABILITY ANALYSIS AND SAFETY ASSESSMENT

This report is required by 10 CFR 50.73(a)(2)(v) because the design and the periodic operation of the MCREC system was such that a single failure could have prevented the fulfillment of its safety function.

The purpose of the MCREC system is twofold: 1) to maintain the Main Control Room temperature within acceptable limits during normal plant operations and following an accident, ensuring equipment reliability and Main Control Room habitability (the primary function of the air conditioning subsystem) and 2) to pressurize the MCR with radiologically filtered air in the event of an accident to limit exposure of MCR personnel to within 10 CFR 50, Appendix A limits (the function of the pressurization subsystem). The air conditioning subsystem assists in pressurizing the MCR in that the AHU fans provide a portion of the driving head for the make-up air to the MCR.

Because of the single failure vulnerability associated with the power supply to the air conditioning subsystem, an analysis was performed to determine the impact that operating the air conditioning system at 50 percent capacity would have on the Main Control Room temperature. The analysis was based on conservative assumptions, some of which were as follows. The temperature of the ultimate heat sink for the MCREC system (the Plant Service Water System (EIIS Code BS)) was assumed to be at the maximum design limit of 95 degrees Fahrenheit. The Turbine Building (EIIS Code NM) which houses the Main Control Room was assumed to be at 110 degrees Fahrenheit - the maximum temperature expected during normal operation. Also, the outside ambient air temperature was assumed to be 95 degrees Fahrenheit. Based on the analysis, should the MCREC system be reduced to 50 percent cooling capacity, the Main Control Room could potentially reach a temperature of approximately 120 degrees Fahrenheit in 40 minutes. At this temperature, the Main Control Room would be considered uninhabitable and the Main Control Room instrumentation reliability questionable.

The MCREC system provides support for systems designed to perform a safety function in that it affords habitability of the Main Control Room during normal plant operation and following a design basis accident. In an assumed worst case scenario, a single failure resulting in the operability of only one AHU (50 percent cooling capacity) could occur coincident with a design basis accident such as a LOCA or a main steam line break. In such an event, safety related systems would function automatically to shutdown the reactor and restore it to stable conditions within minutes following the initiating event. Consequently,

TEXT

ample time would be available to ensure that the reactor is stable before the Main Control Room temperature reaches 120 degrees Fahrenheit necessitating evacuation of the Main Control Room. Prior to the Main Control Room becoming uninhabitable, operation of each unit could be transferred to the Remote Shutdown system. The Remote Shutdown system has the capability for prompt hot shutdown of the reactor, including necessary instrumentation and control to maintain the unit in a safe condition during hot shutdown, and subsequent cold shutdown of the reactor through use of administrative procedures. It is postulated that within 24 hours, the MCREC air conditioning subsystem could be restored to 100 percent operating capacity. Following cooldown of the air space and testing of instrumentation, operation of the plant could then be transferred back to the Main Control Room.

The other single failure vulnerabilities addressed in this report pertained to the pressurization function of the MCREC system. The purpose of the pressurization function is to ensure that the MCR remains habitable from a radiological standpoint, limiting exposure to MCR personnel to within 10 CFR 50, Appendix A limits. The plant's Technical Specification and FSAR require that the system be able to pressurize the MCR to $\geq$ 0.1 inches WG. This limit merely ensures that an adequate margin exists to maintain a slightly positive pressure in the main control room during accident conditions. It was concluded from testing performed on 4/2/92 that with any of the postulated failures the MCR would still be capable of being pressurized in the event of an accident, thus it was concluded that exposure of MCR personnel would remain below 10 CFR 50, Appendix A limits.

Based on the above information, this event had no adverse affect on nuclear safety. This analysis applies to all operating conditions.

CORRECTIVE ACTION

DCR 91-130 was implemented to provide an alternate safety related power supply for the train 'C' controls in the event that the Division II power supply is inoperative. The DCR was completed on 7/16/91.

Procedure 34SO-Z41-001-1S was revised to provide instructions for disconnecting specific loads from buses 1R24-S002, 1R24-S003, or 1R24-S029 to allow the operation of two air conditioning trains powered from the same bus without causing an overload condition. This was a temporary corrective action. Subsequently, during the September 1991 Unit 1 Refueling Outage, the feeder cables to buses 1R24-S002 and 1R24-S003 were replaced with larger capacity cables on DCR 91-131. Selective load shedding of the buses is no longer required and the above referenced procedural instructions have been deleted.

A single failure analysis of the MCREC system was completed by 12/13/91. Potential single failure vulnerabilities were identified during the analysis. Testing of the MCREC system was performed on 12/30/91 in accordance with procedure 42SP-121991-PD-1-0S, "Test of MCREC Pressurization with 1 AHU," and on 4/2/92 in accordance with procedure 42SP-020592-PD-1-0S, "Single Failure Test of MCRECS," to assess the significance of the identified problems. Four additional single failure vulnerabilities were identified as a result of testing.

TEXT

The corrective action of each of these four single failure vulnerabilities are listed below:

1) In regard to the single failure vulnerabilities associated with the improper alignment of the AHUs, an interim corrective action was implemented on 12/13/91. Specifically, administrative LCO 1-91-833 was initiated to require two AHUs to be operating at all times. Permanent corrective action included a re-design of the MCREC system under DCR 91-194 to allow operation of one AHU. Specifically, the 'B' AHU control logic was changed such that the 'B' AHU would automatically start upon loss of an operating AHU even if the third AHU was secured. Implementation of the DCR was completed on 4/9/92.

2) To resolve the booster fan discharge damper concern, the booster fan line-up is being changed to require both booster fans be aligned in auto. (Presently, one booster fan is in auto and the other booster fan is in standby.) In this alignment, both booster fans will start in the event of a pressurization mode actuation ensuring that adequate pressurization is achieved. Once damper alignment is verified, one booster fan can be secured and placed in standby. Procedure 34SO-Z41-001-1S will be revised to reflect this change by June 1, 1992. LCO 1-91-833 will then be terminated.

3) In regard to the single failure vulnerability of the exhaust fan discharge dampers, procedure 34SO-Z41-001-1S will be revised by June 1, 1992 to note that any time one of these dampers is opened a single failure vulnerability exists and the appropriate MCREC system LCO should be entered.

4) No actions are required with respect to the MCR bathroom exhaust ducts. As mentioned in the "description of event" section, the bathroom door is normally maintained closed and is equipped with an automatic closing device. The testing on 4/2/92 showed that the required .1 inch W.G. MCR pressure was attained with the door closed and the exhaust ducts opened.

ADDITIONAL INFORMATION

No systems other than the MCREC system were affected by this event.

Three previous similar events have been identified in which the MCREC system was determined not to be in compliance with the single failure design criterion. These events were reported in LERs 50-321/87-04, Revision 1, dated 8/8/88, and 50-321/88-11, dated 6/8/88. The first event, reported in LER 50-321/87-04, Revision 1, involved a single fuse failure preventing the MCREC system from fully entering the isolation mode. The second event, also reported in LER 50-321/87-04, Revision 1, involved a failure of one chlorine gas monitor preventing the MCREC system from fully entering the pressurization mode. The third event involved the use of non-seismic area radiation monitors in the MCREC system pressurization mode actuation logic system. Failure of the monitors during a seismic event could have possibly grounded the actuation logic circuits rendering them inoperable and preventing the system from entering the pressurization mode.

TEXT

Corrective actions for these events included design changes in each case to bring the system into compliance with the single failure design criterion. These corrective actions would not have prevented this event since the portions of the system involved were unique to this event.