NRC FORM 366 (4-95) U.S. NUCLEAR REGULATORY COMMISSION

APPROVED OMD NO. 3150-0104
EXPIRES: 04/30/98
ESTIMATED BURDEN PER RESPONSE TO COMPLY WITH THIS INFORMATION COLLECTION REQUEST: 50.0 HRS. FORWARD COMMENTS REGARDING BURDEN ESTIMATE TO THE INFORMATION AND RECORDS MANAGEMENT BRANCH (MNBB 7714), U.S. NUCLEAR REGULATORY COMMISSION, WASHINGTON, DC 20555-0001, AND TO THE PAPERWORK REDUCTION PROJECT (3150-0104), OFFICE OF MANAGEMENT AND BUDGET, WASHINGTON, DC 20503.

LICENSEE EVENT REPORT (LER)

FACILITY NAME (1)	DOCKET NUMBER (2)	PAGE (3)
Oconee Nuclear Station, Unit One	05000 269	1 OF 10

TITLE (4) Low Temperature Overpressure Protection System Technically Inoperable Due To A Design Oversight

EVENT DATE (5)			LER NUMBER (6)				REPORT DATE (7)			OTHER FACILITIES INVOLVED (8)	
MONTH	DAY	YEAR	YEAR	SEQUENTIAL NUMBER	REVISION NUMBER		MONTH	DAY	YEAR	FACILITY NAME	DOCKET NUMBER(S)
										Unit Two	05000 270
06	17	1998	1998	- 09	- 02		10	01	1998	Unit Three	05000 287

OPERATING MODE (9)	N	THIS REPORT IS SUBMITTED PURSUANT TO THE REQUIREMENTS OF 10 CFR (Check one or more of the following) (11)			
POWER LEVEL (10)	100%	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)(A)	73.71(c)
		20.405(a)(1)(ii)	50.36(c)(2)	50.73(a)(2)(vii)	OTHER (Specify in
		20.405(a)(1)(iii)	X 50.73(a)(2)(i)(B)	50.73(a)(2)(viii)(A)	Abstract below and
		20.405(a)(1)(iv)	X 50.73(a)(2)(ii)(B)	50.73(a)(2)(viii)(B)	in Text, NRC Form
		20.405(a)(1)(v)	50.73(a)(2)(iii)(A)	50.73(a)(2)(x)	366A)

LICENSEE CONTACT FOR THIS LER (12)

NAME	TELEPHONE NUMBER	
	AREA CODE	
J.E. Burchfield, Regulatory Compliance Manager	(864)	885-3292

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

CAUSE	SYSTEM	COMPONENT	MANUFACTURER	REPORTABLE TO NPRDS		CAUSE	SYSTEM	COMPONENT	MANUFACTURER	REPORTABLE TO NPRDS	

SUPPLEMENTAL REPORT EXPECTED (14)		EXPECTED SUBMISSION DATE (15)	MONTH	DAY	YEAR
YES (If yes, complete EXPECTED SUBMISSION DATE)	X NO				

ABSTRACT (Limit to 1400 spaces, i.e. approximately fifteen single-space typewritten lines) (16)

In June 1997, the Oconee Safety Related Designation Clarification Project identified several items for further review regarding Low Temperature Overpressure Protection (LTOP). Detailed reviews of the LTOP system design determined that the system was not single failure proof for several scenarios. Failure of a low range Reactor Coolant System pressure transmitter could impact both LTOP trains. This transmitter provides a control signal for the Power Operated Relief Valve and also is input to alarms that alert the operators of a potential LTOP event via pressurizer high level or high pressure alarms. On June 17, 1998, an operability evaluation concluded that the design basis was not met for single failure criteria of the LTOP system. At 1512 hours, with all three Units at 100% power, the NRC was notified via the Emergency Notification System. Continued review of LTOP scenarios has identified one other computer alarm that is affected by this transmitter. Also, the loss of Decay Heat Removal LTOP scenario might not be protected by the previously credited alarms. The root cause is inadequate design configuration due to a design oversight. Corrective actions include re-calibrating another pressure transmitter and modifying the original design.

EVALUATION:

Background

Low Temperature Overpressure Protection (LTOP) is designed to protect the Reactor Coolant System (RCS) [EIIS:AB] from overpressurization at temperatures less than 325 F by providing a relief path. The requirements are outlined in Technical Specification (TS) 3.1.2.9. Two trains of LTOP are required. The first train is an active train which consists of a Power Operated Relief Valve set to relieve at a low pressure setpoint. The second train is a train which consists of the instrumentation and controls necessary to assure that operator action can be taken, during a LTOP event, to prevent overpressurization of the RCS. TS's allow one train to be out of service for four hours without compensatory actions (designating a LTOP Operator) to monitor for indications of a LTOP event.

The requirements of the second train consist of a combination of limits and administrative controls as follows:

1) Limits on RCS pressure and pressurizer level.

2) Deactivation of both Core Flood [EIIS:BP] Tanks.

3) Deactivation of both High Pressure Injection [EIIS:BG] trains.

4) Restrictions on RCS makeup flow.

5) Certain computer alarms must be operable.

6) Controls on the high pressure nitrogen system.

The Oconee Safety Related Designation Clarification Project was originated in part to clarify the scope of equipment used at Oconee for design basis accident mitigation. In order to scope out the accident mitigation equipment, the project first defined the scope of accidents and transients which were to be reviewed. The LTOP event was among the accidents and transients reviewed.

Description of Event

In order for the Oconee Safety Related Designation Clarification (OSRDC) Project to successfully define the scope of equipment for each postulated event, a number of licensing basis issues had to be resolved. These issues were identified and placed into the corrective action program in mid 1997. For the Low Temperature Overpressurization Protection (LTOP) System, these corrective actions required that seismic, single failure, and loss of instrument air design capabilities of the LTOP System be better clarified.

In May 1998, a detailed licensing review of the LTOP system was completed. A review of the LTOP System design was conducted to determine if there were any single failures which could potentially disable both LTOP trains. The review found that a 0-600 psig low range pressure transmitter originates a high pressure alarm for the LTOP train that requires Operator action and also feeds the Power Operated Relief Valve (PORV) low setpoint in the active LTOP train. This determination verified that a single failure vulnerability existed. A Problem Investigation Process Report was initiated and an operability evaluation was performed.

On May 14, 1998, the present operability evaluation concluded that the passive LTOP train on all three units was technically inoperable since a postulated single failure of the low range pressure transmitter might disable both LTOP trains. At this time, the susceptibility for a single failure would apply only for inadvertent actuation of the pressurizer heaters. Unit 2 was at operating conditions requiring LTOP mitigation. Compensatory actions to station a designated LTOP Operator were initiated. Units 1 and 3 were not in LTOP mitigation modes. Operational guidance to dedicate a LTOP Operator was provided to Units 1 and 3 should they enter the LTOP mitigation mode.

On June 11, 1998, engineering completed a review of the low range pressure transmitter and concluded that no failures of the transmitter had occurred that would have affected LTOP operability. However, this evaluation did not adequately consider the Technical Specification (TS) 3.1.2 Bases. The TS Bases state that for evaluating LTOP system

acceptability the most limiting single failure must be assumed during a LTOP event. Thus, even though it was shown that the system would have been functional in the past, the design basis had not been met. As a result, the LTOP mitigation system was classified as being past inoperable on June 17, 1998.

On June 17, 1998, at 1512 hours, the NRC was notified via the Emergency Notification System of the postulated failure scenario. As allowed by TS 3.1.2, compensatory actions consisting of a dedicated LTOP Operator will be put in place on each unit when required.

Engineering continued to review the LTOP design analyses while determining appropriate methods for removing the single failure vulnerability. Additional LTOP scenarios were identified that affect the same single failure. On July 23, 1998, engineering determined that the same Low Range Pressure Instrument also affects one of the three high level alarms needed to alert the operator in these additional scenarios.

Specifically, the current logic for identifying a "Pressurizer Level High" alarm initiates an audible alarm if the temperature corrected level is greater than or equal to 225 inches while either the RCS Pressure is greater than 100 psig or if any High Pressure Injection (HPI) pumps are running. This section of LTOP Logic uses the same Low Range Pressure Instrument that initiates the high pressure alarm for the second train of LTOP and controls the PORV in the active LTOP train.

On July 24, 1998, engineering completed an evaluation and concluded that a failure of the pressure transmitter could disable the "Pressurizer Level High" alarm along with the "LTOP High Pressure" Alarm and also disable the PORV. Thus the susceptibility for a single failure to disable the LTOP mitigation system would not only apply to the inadvertent actuation of the pressurizer heaters but also for the makeup control valve (HP-120) failing open and loss of decay heat removal (DHR) LTOP design scenarios.

On August 18, 1998, a second low range RCS pressure channel was added for Unit 1. It consists of re-calibrating a narrow range RCS pressure instrument to provide the alarms required for the second train of LTOP mitigation. This measure will be implemented when LTOP mitigation is required until a second RCS low range pressure transmitter is added. The Operations procedure for LTOP was revised for Unit 1 only.

On August 27, 1998, while the continued review of engineering analyses was in progress, it was determined that alarms for the second train of LTOP would not be adequate to detect some loss of DHR LTOP scenarios. When the LTOP calculation was originally performed, it was judged that the control room operator would immediately be made aware of a loss of DHR by various alarms. Some of the alarms indicating a loss of DHR were listed in the calculation. When the RCS low range pressure instrument single failure vulnerability was identified, an analysis was initiated to review the alarms used for the second train of LTOP. In the worst case operating conditions, the control room operator would not immediately recognize that cooling water to the Low Pressure Injection cooler was lost.

On September 16, 1998, a re-calibrated narrow range RCS pressure instrument to provide the alarms required for the second train of LTOP mitigation for Unit 2. This measure will be implemented when LTOP mitigation is required until a second RCS low range pressure transmitter is added.

On September 17, 1998, a more detailed analysis of the loss of decay heat removal scenarios was completed. It reveals that the "LTOP Pressurizer High Level" alarm and "LTOP High Pressure" alarm provide the required function when the single failure vulnerability is removed.

Based on this re-analysis and the use of a re-calibrated narrow range RCS pressure instrument, the vulnerability of the LTOP mitigation system to be disabled by a single failure of the pressure transmitter has been eliminated for Units 1 and 2. The functional testing for the use of a re-calibrated narrow range pressure instrument has not been completed for Unit 3. It is expected to be completed before the Unit 3 shutdown for refueling on October 8, 1998. With the completion of

the engineering review of the LTOP design basis and crediting of operator actions, the present LTOP is capable of performing its intended function. Both trains of the LTOP mitigation system are currently considered to be fully operable.

Conclusion

The development and review of the LTOP System design occurred in the mid 1980s following the Three Mile Island Unit 2 (TMI-2) event. Duke addressed the single failure requirement by stating that there were two independent, diverse means (trains) of LTOP available for mitigation of postulated low temperature pressurization events.

Based on a review of the licensing basis documentation and operating procedures it is apparent that the single failure issue associated with Low Temperature Overpressure Protection (LTOP) was not adequately addressed.

The Oconee Safety Related Designation Clarification project identified issues related to LTOP. The single failure issue involves a failure of the low pressure transmitter while there is no designated LTOP Operator and could have impacted the ability of operators to mitigate a LTOP event at Oconee. The ability of alarms to detect a loss of decay heat removal scenario was also questioned and a re-analysis determined that this function could be performed by the "Pressurizer Level High" alarms and the "LTOP RCS High Pressure" alarm. This would not have been the case in the past due to the single failure vulnerability. There might not have been 10 minutes available for operator action if a loss of decay heat removal had occurred when operating conditions were susceptible to a LTOP scenario.

Therefore, the root cause of this event is an inadequate design configuration due to a design oversight that occurred in the mid 1980s.

A review of LERs and the Operating Experience Data Base for inadequate design configurations over the last two years was conducted. There have been no LERs associated with LTOP inadequate design configurations. There have been LERs with design deficiencies but

they were associated with deficient design analysis. Design oversight LERs have not been a recent occurrence. The design processes and procedures in place currently should preclude oversights similar to those identified in this event. There was no operating experience associated with LTOP inadequate design configurations. Therefore, this event is considered non-recurring.

This postulated event did not result in personnel injuries, radiation overexposures, or releases of radioactive materials. There were no equipment failures associated with this event.

CORRECTIVE ACTION:

Immediate:

1. Compensatory action guidelines were established. These guidelines require a designated Low Temperature Overpressure Protection (LTOP) Operator to be stationed if a unit enters the LTOP mitigation mode of operation. This is required until measures are in place to restore the LTOP mitigation system to operable status.

Subsequent:

1. Procedures were revised to require a narrow range pressure transmitter to be re-calibrated prior to entering and after exiting LTOP operating regions. This provides an acceptable method for the second train of LTOP on all three Oconee Units.

Planned:

1. The current design of the LTOP system will be modified to add a second low range pressure transmitter.

2. Functional testing for Unit 3 narrow range pressure transmitter re-calibration will be satisfactorily completed.

3. Training of affected personnel will be conducted regarding reportability requirements associated with this event.

Planned corrective action number 2 is an NRC Commitment item. This is the only NRC Commitment item contained in this LER.

SAFETY ANALYSIS:

This event involves a postulated failure of the low range pressure transmitter. The transmitter provides the comparison signal for the Power Operated Relief Valve lift setpoint (active Low Temperature Overpressure Protection (LTOP) train), and also feeds the high pressure alarms which alert the operators of a potential LTOP event (passive LTOP train). It also arms a pressurizer level alarm if Reactor Coolant System (RCS) pressure is greater than 100 psig.

The Technical Specification Bases describe seven LTOP initiating events for evaluating the adequacy of the passive LTOP train. The following scenarios have the potential to result in a LTOP event:

1) Makeup control valve (HP-120) fails full open.

2) Erroneous opening of a core flood tank (CFT) discharge valve.

3) Erroneous actuation of the High Pressure Injection (HPI) system.

4) All Pressurizer Heaters erroneously energized.

5) Temporary loss of decay heat removal.

6) Thermal expansion of the RCS after starting a Reactor Coolant Pump due to stored energy in the Steam Generator.

7) Erroneous addition of high pressure nitrogen.

Of these seven possible initiators of LTOP transients, only Scenarios 1, 4, and 5 would be affected by a failure of the low range pressure transmitter because these scenarios rely on low range RCS pressure and/or pressurizer level indication as the primary alerting indication of a LTOP event.

Scenario 1 is where the makeup control valve (HP-120) fails open to its travel stop. The travel stop position limits the maximum make-up flowrate to a value determined by the LTOP calculation. This maximum flowrate allows for a 10 minute operator action time beginning from the time that a RCS high pressure alarm or pressurizer level high alarm is received in the control room. If there is no alarm, the Pressure/Temperature curve limit might be exceeded. However, an Operator at the controls is trained to scan the plant parameters including RCS pressure and pressurizer level even when there is no dedicated LTOP Operator. Once the high flowrate is recognized, the Operator can take appropriate actions to reduce flow by stopping HPI pump(s) or manually throttling makeup.

Scenario 4 is where all Pressurizer heaters are erroneously energized. This LTOP initiating event credits use of the low range pressure transmitter as the primary alerting instrument for Operators to mitigate a LTOP event. Pressurizer heater use is manually controlled by operators utilizing procedures to maintain RCS pressure at desired levels. It is unlikely all the heaters would energize while in manual except by operator action. Indicating lights in the control room illuminate when Pressurizer Heaters are energized. It is unlikely that this condition would continue unnoticed to the point of exceeding LTOP conditions since an operator is controlling them in manual. There are also other pressure transmitters that are available to the operator to aid in detection and termination of a LTOP event. The 0-2500 psig (wide range) pressure transmitter(s) are not utilized for LTOP events but would be available to the operator. They could be utilized to determine if the RCS pressure was unexpectedly increasing.

Scenario 5 is a LTOP event where a temporary loss of decay heat removal occurs. In this scenario, there are control room alarms associated with the Low Pressure Injection (LPI) [EIIS:BP] system and LPSW system which could actuate and alert the Operator to take appropriate action. However, the alarms are not adequate for all possible initial RCS conditions and decay heat removal system alignments. A revision to the LTOP analysis has determined that the "Pressurizer High Level" and "LTOP High Pressure" alarms will provide adequate notification for loss of decay heat removal events. The alarms originally credited would not be necessary. However, the

single failure vulnerability would have prevented these alarms from actuating. In the event the Operator At The Controls (OATC) did not immediately recognize the loss of decay heat removal, there might not be sufficient time to prevent exceeding the Pressure/Temperature curves.

Technical Specification 3.1.2.9.2 and operating procedures require that both CFTs and both HPI trains be isolated from the RCS, thus precluding the occurrence of Scenarios 2 and 3. Scenario 6 is a self limiting LTOP transient in which RCS pressurization terminates after the primary and secondary systems reach thermal equilibrium. Operator action is not required to terminate this scenario since analyses have shown that the pressure-temperature limits are not exceeded. Scenario 7 is also precluded from this event since administrative controls require that the high pressure nitrogen system be isolated from the RCS via a tagged closed valve.

The ability to mitigate LTOP events is normally required for a period of approximately two to three days during each unit startup and shutdown.

Also, there is a low probability of LTOP events at Babcock and Wilcox (B&W) designed plants since these plants are not normally operated in a water solid condition. The LTOP analyses credit the fact that Oconee has a pressurizer bubble present at all times (either steam or nitrogen) excluding hydro testing of the system.

The health and safety of the public was not affected by this event.