Indian Point 3
Nuclear Power Plant
P.O. Box 215
Buchanan, New York 10511
914 736.8001

New York Power Authority

John H. Garrity
Resident Manager

August 12, 1993
IPN-93-095

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Mail Station PI-137
Washington, D.C. 20555

SUBJECT: Indian Point 3 Nuclear Power Plant
Docket No. 50-286
Licensee Event Report LER 93-005-03
"Missed Periodic Inservice Tests and Faults in AMSAC System Logic, Due to Personnel Error, Place the Plant Outside Design Basis"

Dear Sir:

The attached Licensee Event Report, LER 93-005-03, is hereby submitted in accordance with the requirements of 10CFR50.73. This LER revision is required to confirm that the Anticipated Transient Without Scram (ATWS) Mitigation System Actuation Circuitry (AMSAC) system was in a state of degraded operability from December 13, 1990 through April 10, 1991. This event is of the type defined in the requirements per 10CFR50.73 (a)(2)(ii)(B). No new commitments are being made by this submittal.

Very truly yours,

M T Peckham for

John H. Garrity
Resident Manager
Indian Point Three Nuclear Power Plant

JHG/vjm

cc: See Next Page

170025

IE22 1/1

Mr. Thomas T. Martin
Regional Administrator
Region 1
U.S. Nuclear Regulatory Commission
475 Allendale Road
King of Prussia, Pennsylvania 19406-1415

INPO Records Center
700 Galleria Parkway
Atlanta, Georgia 30339-5957

U.S. NRC Resident Inspectors' Office
Indian Point Unit 3

NRC FORM 366 (5-92) U.S. NUCLEAR REGULATORY COMMISSION

LICENSEE EVENT REPORT (LER)

FACILITY NAME (1)	DOCKET NUMBER (2)	PAGE (3)
Indian Point Unit 3	05000286	1 OF 10

TITLE (4) Missed Periodic Inservice Tests and Faults in AMSAC System Logic, Due to Personnel Error, Place the Plant Outside Design Basis

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
12	31	92	93	-- 005 --	03	08	12	93		05000
									FACILITY NAME	DOCKET NUMBER 05000

OPERATING MODE (9)	N
POWER LEVEL (10)	100

THIS REPORT IS SUBMITTED PURSUANT TO THE REQUIREMENTS OF 10 CFR §: (Check one or more) (11)

	20.402(b)		20.405(c)		50.73(a)(2)(iv)		73.71(b)
	20.405(a)(1)(i)		50.36(c)(1)		50.73(a)(2)(v)		73.71(c)
	20.405(a)(1)(ii)		50.36(c)(2)		50.73(a)(2)(vii)		OTHER
	20.405(a)(1)(iii)		50.73(a)(2)(i)		50.73(a)(2)(viii)(A)		(Specify in Abstract below and in Text, NRC Form 366A)
	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 (Include Area Code)
Federico Perdomo, Licensing Engineer	(914) 736-8029

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 15 single-spaced typewritten lines) (16)

On December 31, 1992, with the reactor at 100 percent power, a 40 second time delay in the Anticipated Transient Without Scram (ATWS) Mitigation System Actuation Circuitry (AMSAC) logic failed to operate during the performance of a surveillance test. On two separate instances, software manipulations affecting the 40 second time delay placed AMSAC in a condition of degraded operability. On February 26, 1993, with the reactor at 97 percent power, the Authority reported that certain AMSAC system periodic inservice tests had not been performed for the last two refueling outages. A unit shutdown was initiated the same day (February 26, 1993) to correct the periodic inservice test issue. Subsequently, on March 5, 1993, with the reactor at hot shutdown, the Instrumentation and Controls department discovered a design deficiency involving the AMSAC actuation logic. Due to the 40 second time delay events, inservice test issue and design deficiency, the AMSAC system did not meet the requirements of the ATWS rule (10 CFR 50.62). The cause of these separate events is attributed to human error. Various corrective action steps have been developed to address the human error causal factor. Prior to the plant achieving criticality the AMSAC system will be restored to full compliance with our commitments to 10 CFR 50.62.

FACILITY NAME (1)	DOCKET	LER NUMBER (6)			PAGE (3)
		YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	
Indian Point Unit 3	05000286	93	-- 005 --	03	02 OF 10

TEXT (If more space is required, use additional copies of NRC Form 366A) (17)

DESCRIPTION OF THE EVENT

On December 31, 1992, with the reactor at 100 percent power, a 40 second time delay in the Anticipated Transient Without Scram (ATWS) Mitigation System Actuation Circuitry (AMSAC)(JG) logic failed to operate during a semi-annual surveillance test being performed by an Instrumentation and Controls (I&C) technician. This time delay fault could have prevented the automatic start of the motor driven auxiliary feedwater (AFW) pumps during an ATWS event. On January 12, 1993 I&C Engineering and Foxboro (vendor for AMSAC) field personnel determined that this failure was caused by AMSAC system software manipulations which took place during corrective maintenance on July 8, 1992 (corrective maintenance consisted of performing troubleshooting activities using surveillance test 3PT-SA31). The software manipulations performed by the Foxboro field engineer inadvertently disabled a 40 second time delay in the AMSAC logic during the July 8, 1992 corrective maintenance. The time delay discrepancy went undetected until December 31, 1992, when a scheduled surveillance test was performed. On January 12, 1993, the time delay discrepancy was corrected, the system tested satisfactorily, and declared operable.

At 2250 hours on February 26, 1993, in response to the NRC Resident Inspector's questions, and with the reactor at 97 percent power, the Authority reported that certain AMSAC system periodic inservice tests had not been performed in accordance with the required frequency. A unit shutdown was initiated at 2300 hours on February 26, 1993 to correct these findings. As a result of the Authority's extensive review of the AMSAC system design during this shutdown, the I&C department discovered a design deficiency with the actuation logic. At 1233 hours on March 5, 1993, with the reactor at hot shutdown and during dynamic testing, the I&C department discovered that the AMSAC actuation timer did not lock in the power level from which it was activated.

INVESTIGATION OF THE EVENT

On May 12, 1992, semi-annual surveillance test 3PT-SA31 failed due to an AMSAC system hard drive failure and the hard drive was subsequently returned to Foxboro for repair. Along with the defective hard drive, a Foxboro field technician sent an uncontrolled configuration diskette ("save all disk") that was loaded onto the hard drive once it was repaired. The uncontrolled "save all disk" contained software logic which caused the system to reboot (load logic from hard drive to active memory) improperly during the performance of the July 8, 1992 corrective maintenance.

The July 8, 1992 corrective maintenance results were satisfactory until the performance of a step which verifies that AMSAC will reboot properly and not send a trip signal when power is turned off and restored. When this step was performed, AMSAC did not reboot properly and sent a trip signal when power was restored to it. In order to remedy this situation, the Foxboro field engineer manipulated the AMSAC system software so that the system would reboot properly. This manipulation appeared successful and the test was continued with no further complications. However, the software manipulations performed by the Foxboro field engineer inadvertently affected the logic which provides a 40 second time delay. The software manipulations in effect disabled the 40 second time delay in the AMSAC logic.

The subject 40 second time delay is required to assure that an AMSAC initiation signal will be maintained for at least 40 seconds. The motor driven AFW pumps have a 28 second time delay built into their starting circuits. Therefore, the 40 second time delay assures that the initiation signal is maintained sufficiently long to ensure that the motor driven AFW pumps start.

The event date is December 31, 1992 when the 40 second time delay in the AMSAC logic failed to operate during the performance of a surveillance test. On January 12, 1993 I&C Engineering and Foxboro field personnel determined the cause of failure. However, it was on January 26, 1993 that licensing personnel determined that the failure was reportable. Licensing determined that because the AMSAC system was in a state of degraded operability from August 3, 1992 (date the unit went critical) through January 12, 1993 it did not meet the reliability requirements of the ATWS rule (10 CFR 50.62) during this time period. This was reported to the Commission pursuant to 10 CFR 50.72(b)(1)(ii)(B).

The Authority performed a review of AMSAC work history records for approximately the past three years. On December 13, 1990 a new software version of the AMSAC logic was installed and the retest on the system failed. The vendor manipulated the software and a second retest was performed satisfactorily. No work was performed on the system until March 15, 1991. The surveillance test performed on March 15, 1991 indicated that the subject 40 second time delay was disabled. On April 10, 1991 the vendor again manipulated the software and the system passed a retest. The Authority has concluded that on December 13, 1990 the Foxboro technician most probably performed software manipulations in a manner similar to the manipulations which took place later on July 8, 1992. The December 13, 1990 and subsequently the July 8, 1992 software manipulations resulted in surveillance test failures due to the disabled 40 second time delay. Therefore, as a result of the December 13, 1990 software manipulations, AMSAC was also in a state of degraded operability from December 13, 1990 through April 10, 1991.

The AMSAC system is non-safety related but is classified as Category M with Category I boundaries because a commitment has been made to the Commission that AMSAC equipment will be treated under a Quality Assurance (QA) program that is consistent with and satisfies the guidance contained in Generic Letter 85-06. Investigation of this event revealed that the Final Safety Analysis Report (FSAR) and the Plant Equipment Data Base (PEDB) do not reflect that AMSAC is classified as Category M with Category I boundaries. This condition was not a direct contributor to the occurrence of this event. However, these documents will be updated as indicated in the corrective actions.

In response to the NRC Resident Inspector's questions, the Authority began a review to determine if all periodic inservice test commitments were being addressed. Subsequently, on February 26, 1993 the Authority reported that certain AMSAC system periodic inservice tests had not been performed in accordance with the required frequency. Based on these findings a unit shutdown was commenced the same day. A verification that the final output devices have received an AMSAC output signal in response to a simulated AMSAC initiation signal, and calibration of narrow range feed flow and select turbine first stage pressure instrumentation, had not been performed every refueling outage as required.

During the unit shutdown, the Authority conducted an extensive review of the AMSAC system design. The results of this review revealed a design deficiency with the AMSAC actuation logic. The I&C department performed dynamic testing of the AMSAC software on March 5, 1993 and discovered that the AMSAC actuation timer did not lock in the power level from which it was activated. The AMSAC actuation timer serves to initiate an AMSAC output after a predetermined time delay whenever turbine power is 40 percent or greater coincident with three of the four feedwater flow transmitters indicating feedwater flow of 21 percent or less.

The I&C department has indicated that dynamic testing was not included in the modification acceptance testing at the time the AMSAC system was installed. Subsequent surveillance tests performed only static input changes to the system in order to derive the required system outputs. The typical static test involves adjusting input test voltages to derive a required output. The results of both the static and dynamic tests should be approximately the same for the AMSAC system. However, dynamic test results indicated that the actuation timer deficiency caused AMSAC output to be initiated after a time delay of 166 seconds at 100 percent power. The time delay is supposed to vary from 300 seconds at 40 percent power to 25 seconds at 100 percent power.

CAUSE OF THE EVENT

The cause of the 40 second time delay discrepancy was human error in that the July 8, 1992 corrective maintenance activities were improperly performed and documented. During the performance of the corrective maintenance (utilizing 3PT-SA31) a feature of the system failed to function as required. Software manipulations were made in order to correct the cause of failure and 3PT-SA31 was continued. The July 8, 1992 corrective maintenance activities should have been documented in detail sufficient for reviewers of the work to conclude that the system required a retest to demonstrate AMSAC operability. The results of a new retest would have served to test the AMSAC system logic and would have indicated a problem with the 40 second time delay.

A contributing factor to the 40 second time delay discrepancy was inadequate document control in that a controlled "save all disk" was not maintained for the AMSAC system. Because of this, an uncontrolled version of the disk containing faulty software logic was loaded.

The periodic inservice tests were not performed according to the required frequency as a result of personnel error in that the AMSAC modification package did not adequately document the inservice testing that had been committed to in previous correspondence to the Commission.

The Authority has concluded that, as the result of personnel error, the design specifications that were provided to Foxboro did not clearly detail the specific features which the Authority required of the system. Therefore, the AMSAC actuation timer design deficiency has existed since the AMSAC system was placed in service.

CORRECTIVE ACTIONS

The following corrective actions serve to prevent recurrence of the event:

1. In addition to the existing administrative requirement that vendors/contractors perform all work in accordance with plant approved procedures, the I&C department revised Administrative Directive IC-AD-8, "Work Processing" to require that all vendor performed work is properly documented. The I&C supervisor shall ensure that vendors document their actions on the notes page of work requests (WRs) prior to WR submittal for retest requirements.

2. A cautionary note was included in AMSAC surveillance test 3PT-SA31 which requires the user to retest the system if any repair or modification to the AMSAC logic or hard drive is required. The surveillance test was revised on April 16, 1993 to include this cautionary note.

3. Administrative direction has been given to all departments that will ensure that all commitments made in correspondence with the Commission are adequately addressed, tracked, and implemented. This "directive" serves to prevent recurrence of an event such as the missed AMSAC system periodic inservice tests. The commitment had been made in previous correspondence to the Commission that we would perform the subject inservice tests. However, the AMSAC installation modification did not capture this commitment. The subject administrative direction will assure that such commitments are appropriately addressed in the future.

4. The Authority has issued a Purchase Order for Foxboro to redesign the AMSAC software so that it complies with the requirements of the ATWS Rule. The Authority will install the revised version of software logic via Minor Modification Package (MMP No. 93-3-119 AMSAC) prior to the plant achieving criticality.

5. Dynamic testing of the AMSAC logic will be performed after the installation of MMP No. 93-3-119 AMSAC and semi-annually thereafter in accordance with surveillance test 3PT-SA31. Dynamic testing will be performed prior to going above cold shutdown.

The following corrective actions do not prevent recurrence but are required:

1. The AMSAC system software is now currently being maintained as controlled "documents".

2. The FSAR will be revised to reflect that the AMSAC system is classified as Category M with Category I boundaries. The FSAR will be revised in the 1993 FSAR update which is due July 22, 1993. Also, the Plant Equipment Database has been updated to reflect the proper QA classification of all related AMSAC system components.

3. An administrative operational specification that provides reportability guidance and limiting conditions for operation, in the event AMSAC is determined to be inoperable in the future, was approved for use on April 14, 1993.

4. Surveillance Test 3PT-R145, "AMSAC System Functional Test" was written to ensure that: the AMSAC logic will generate a trip signal to all applicable final actuation devices; all instruments providing inputs to AMSAC have been calibrated; and signals from these instruments are provided to the AMSAC cabinet. This test was successfully performed on 2/28/93 indicating that all tested functions are operable.

ANALYSIS OF THE EVENT

As a result of the December 13, 1990 and the July 8, 1992 software manipulations, the AMSAC system was in a state of degraded operability from December 13, 1990 through April 10, 1991 and from August 3, 1992 through January 12, 1993 respectively. The AMSAC system did not fully meet the requirements of the ATWS rule during these time periods. This event is reportable under 10 CFR 50.73 (a)(2)(ii)(B) because the degraded operability of the AMSAC system placed the plant outside its design basis.

The additional deficiencies which were identified during the investigation of the 40 second time delay event are also reportable pursuant to 10 CFR 50.73 (a)(2)(ii)(B). Due to the missed periodic inservice tests the AMSAC system was inoperable since the end of the 7/8 refueling outage (12/23/90). Due to the actuation timer design deficiency, which existed since the system was placed in service (June 12, 1989), the AMSAC system did not meet the requirements of the ATWS rule. Therefore, the design deficiency also placed the plant outside its design basis.

SAFETY SIGNIFICANCE

The AMSAC system provides an alternate means of tripping the turbine and actuating AFW flow apart from the reactor protection system (RPS). The RPS has been operable for the entire time period in which the AMSAC has been placed in service.

The 40 second time delay discrepancy may have prevented the automatic initiation of the motor driven AFW pumps during an ATWS event. However, AMSAC would have provided the required alarms and performed all other automatic functions including tripping the main turbine generator, isolating the steam generator blowdown and sample valves, and providing a start signal to the turbine driven auxiliary feedwater pump (with manual throttling).

In the unlikely event that both trains of RPS had failed and AMSAC activation had been called upon, the combination of the AMSAC alarm and the guidance in Emergency Operating Procedure (EOP) FR-S.1, "Response to Nuclear Power Generation/ATWS" would ensure that the operators manually started the AFW pumps. One of the immediate action steps mandated by this EOP is to check that both motor driven auxiliary feedwater pumps are running. The immediate action step also requires the operator to manually start the steam driven Auxiliary Boiler Feedwater Pump (ABFP) if either motor driven pump will not start.

As reported in LER 93-004, the steam driven ABFP (800 gallon per minute capacity) was inoperable from December 3, 1992 through December 29, 1992. The LER also reported that the cumulative time a second ABFP (motor driven) was considered inoperable was 71 hours and 22 minutes. For the majority of this time (71 hours and 15 minutes) the second ABFP was considered inoperable because its emergency power source was considered inoperable due to testing. Had an ATWS occurred during this time frame, it would have been possible to power the motor driven ABFP using offsite power. However, offsite power would not have been available if the ATWS event was originally a loss of offsite power that was accompanied by failure of the reactor trip system to shut down the reactor. Therefore, if an ATWS involving loss of offsite power would have occurred from December 3, 1992 through December 29, 1992 only one motor driven auxiliary feedwater pump would have been operable with a capacity for delivering 400 gallons per minute. For the worst case ATWS event the requirement is to provide 680 gallons per minute of auxiliary feedwater.

The safety significance of having missed certain periodic inservice tests is that certain AMSAC functions and instrument calibrations have not been verified for the last two refueling outages. A verification that the final output devices have received an AMSAC output signal in response to a simulated AMSAC initiation signal, and calibration of narrow range feed flow and select turbine first stage pressure instrumentation, has not been performed for the last two refueling outages. As indicated in the corrective actions, surveillance test 3PT-R145 was developed and performed successfully indicating that the subject AMSAC functions were operable and instrument calibrations were properly calibrated. The calibration of the feedwater flow and first stage turbine pressure transmitters revealed that three out of the four flow transmitters and both of the pressure transmitters were within calibration requirements.

The lack of a design feature that would have locked in the turbine power signal in the AMSAC logic could have resulted in AMSAC initiation being delayed up to 166 seconds. This delay time for AMSAC initiation is too late for AMSAC to perform its function and mitigate the postulated scenario of Loss of Normal Feedwater without Reactor Trip and without Turbine Trip. A significant pressure excursion begins at about 90 seconds into the event and hits the American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code Level C limit of 3200 psig at about 120 seconds.

Operator action to trip the turbine before 60 seconds would have prevented the 3200 psig limit from being reached. Such operator action is required by EOPs although the operators are not time tested to perform these actions.

The safety significance of an inoperable AMSAC must consider the probability of the event. As it postulates multiple failures beyond our design basis it was not considered a safety system because the event it was to mitigate has minute probability. When loss of normal feedwater, no reactor trip and no operator action, is considered, the event probability approaches 1E-6/year.

SECURING FROM THE EVENT

On January 12, 1993, the 40 second time delay was placed in the appropriate software location, the system was tested satisfactorily, and had been declared operable. However, during the investigation and design review of this event, the Authority concluded that certain AMSAC system periodic inservice tests had not been performed and also discovered a design deficiency with the AMSAC actuation timer. Due to this situation the AMSAC system has not yet been declared operable. The AMSAC system will be verified operable prior to the plant achieving criticality.