September 23, 1986

Docket Nos.: 50-348
and 50-364

Mr. R. P. McDonald
Senior Vice President
Alabama Power Company
Post Office Box 2641
Birmingham, Alabama 35291

DISTRIBUTION
Docket File
*NRC PDR
*Local PDR
*PAD#2 Rdg
*T. Novak
*OGC-Bethesda
*E. Jordan
*B. Grimes
*J. Partlow
*N. Thompson
E. Reeves (2)
*D. Miller
*ACRS (10)
*Gray File

*Without enclosures

Dear Mr. McDonald:

SUBJECT: ANTICIPATED TRANSIENTS WITHOUT SCRAM - JOSEPH M. FARLEY UNITS 1 AND 2

The Nuclear Regulatory Commission (NRC) staff has completed its review of the Westinghouse Owners' Group (WOG) Topical Report WCAP-10858 "AMSAC Generic Design Package" submitted in response to 10 CFR 50.62 "Requirements for Reduction of Risk from Anticipated Transient Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants." Guidance for meeting the requirements of 10 CFR 50.62 was provided in the preamble to that rule and was further provided to all licensees in Generic Letter 85-06 "Quality Assurance Guidance for ATWS Equipment That is Not Safety Related."

The results of the staff's review of the generic design for the ATWS mitigation system actuation circuitry (AMSAC) are contained in the attached Safety Evaluation (SE). The staff has concluded that the generic design is acceptable; however, many plant specific details needed in order to ensure conformance with the rule are not addressed by the WOG generic design. These details needed by the NRC to complete the review are defined in the SE.

We request that you review the SE and provide, within 30 days of receipt of this letter, your schedules for addressing the plant specific design features discussed in Appendix A of the SE, and for implementation following the staff's approval of your plant specific design.

This request for information is covered under OMB clearance number 3150-0011 which expires September 30, 1986.

If you have any questions, please contact me at (301) 492-4782.

Sincerely,

Original Signed by

Edward A. Reeves, Project Manager
PWR Project Directorate #2
Division of PWR Licensing-A

Enclosure: As Stated

cc: See next page

LA:PAD#2	PM:PAD#2	PD:PAD#2
DMiller	EReeves:hc	LRubenstein
9/ /86	9/11/86	9/ /86

cc:
Mr. W. O. Whitt
Executive Vice President
Alabama Power Company
Post Office Box 2641
Birmingham, Alabama 35291

Mr. Louis B. Long, General Manager
Southern Company Services, Inc.
Post Office Box 2625
Birmingham, Alabama 35202

Chairman
Houston County Commission
Dothan, Alabama 36301

Ernest L. Blake, Jr., Esquire
Shaw, Pittman, Potts and Trowbridge
1800 M Street, N.W.
Washington, DC 20036

Robert A. Buettner, Esquire
Balch, Bingham, Baker, Hawthorne,
Williams and Ward
Post Office Box 306
Birmingham, Alabama 35201

Resident Inspector
U.S. Nuclear Regulatory Commission
Post Office Box 24 - Route 2
Columbia, Alabama 36319

D. Biard MacGuineas, Esquire
Volpe, Boskey and Lyons
918 16th Street, N.W.
Washington, DC 20006

Charles R. Lowman
Alabama Electric Corporation
Post Office Box 550
Andalusia, Alabama 36420

Regional Administrator, Region II
U.S. Nuclear Regulatory Commission
101 Marietta Street, Suite 2900
Atlanta, Georgia 30303

Claude Earl Fox, M.D.
State Health Officer
State Department of Public Health
State Office Building
Montgomery, Alabama 36130

Mr. J. D. Woodard
General Manager - Nuclear Plant
Post Office Box 470
Ashford, Alabama 36312

ENCLOSURE

SAFETY EVALUATION OF TOPICAL REPORT (WCAP-10858) "AMSAC GENERIC DESIGN PACKAGE"

1.0 INTRODUCTION

In response to 10 CFR 50.62 "Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants", Westinghouse on behalf of the Westinghouse Owner's Group (WOG) has submitted for review WCAP-10858 "AMSAC Generic Design Package." This document details the WOG's proposed generic ATWS Mitigation System Actuation Circuitry (AMSAC) designs for compliance with 10 CFR 50.62.

2.0 BACKGROUND

On July 26, 1984 the Code of Federal Regulations (CFR) was amended to include Section 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants" (known as the "ATWS Rule"). An ATWS is an expected operational transient (such as loss of feedwater, loss of condenser vacuum, or loss of offsite power) which is accompanied by a failure of the reactor trip system (RTS) to shut down the reactor. The ATWS rule requires specific improvements in the design and operation of commercial nuclear power facilities to reduce the likelihood of failure to shut down the reactor following anticipated transients, and to mitigate the consequences of an ATWS event.

3.0 CRITERIA

The basic requirement for Westinghouse plants is specified in paragraph (c)(1) of 10 CFR 50.62, "Each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system,

to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system."

The criteria used in evaluating the Westinghouse report include; (1) 10 CFR 50.62, (2) guidance and information published as the preamble to that Rule, and (3) Generic Letter 85-06 "Quality Assurance Guidance for ATWS Equipment that is not Safety-Related." The evaluation was done on a generic basis, and the relevant criteria is presented below.

The systems and equipment required by 10 CFR 50.62 do not have to meet all of the stringent requirements normally applied to safety-related equipment. However, this equipment is part of the broader class of structures, systems, and components defined in the introduction to 10 CFR 50, Appendix A (General Design Criteria). GDC-1 requires that "structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed." Generic Letter 85-06 "Quality Guidance for ATWS Equipment that is not Safety-Related" details the quality assurance that must be applied to this equipment.

In general, the equipment to be installed in accordance with the ATWS rule is required to be diverse from the existing RTS, and must be testable at power. This equipment is intended to provide needed diversity (where only minimal diversity currently exists) to reduce the potential for common mode failures that could result in an ATWS leading to unacceptable plant conditions.

The ATWS mitigation design is not required to be safety-related (e.g., meet IEEE-279). However, the implementation should incorporate good engineering practice and must be such that the existing protection system continues to meet all applicable safety related criteria. Equipment diversity to the extent reasonable and practicable to minimize the potential for common cause failures is required from the sensors to, but not including the final actuation device. All mitigating system instrument channel components (excluding sensors and isolation devices) must be diverse from the existing RTS. It is desirable, but not required, to use sensors and isolation devices that are not part of the RTS.

The basis for not requiring diverse isolators is that the RTS unavailability and AMSAC availability (without a reactor trip signal) are similar with or without the addition of a diverse isolator. Furthermore, with the addition of a new component (e.g., the diverse isolator) within AMSAC, the probability of not getting a reactor trip signal or AMSAC signal will be increased somewhat by the additional failure rate of the diverse isolator. However, if existing RTS sensors and isolators are utilized, particular emphasis should be placed on the method(s) used to qualify the isolators for their particular function. This

should include an analysis and tests which will demonstrate that the existing isolator will function under the maximum worst case fault conditions. The required method for qualifying the isolators is presented in Appendix A.

The capability for test and surveillance at power is required, however, surveillance frequencies have not been established at this time. During surveillance at power, the mitigating system may be bypassed, however, the bypass condition must be automatically and continuously indicated in the main control room. The AMSAC system design may also permit bypass of the mitigating function to allow for maintenance, repair, test, or calibration to prevent inadvertent actuation of the protective action at the system level. Where operating requirements necessitate automatic or manual bypass of a mitigating system, the design should be such that the bypass will be removed automatically whenever permissive conditions are not met.

The use of a maintenance bypass should not involve lifting leads, pulling fuses or tripping breakers or physically blocking relays. A permanently installed bypass switch or similar device should be used.

The design should be such that once the ATWS mitigation system has been initiated, the protective action at the system level shall go to completion. Return to operation should require subsequent deliberate operator action.

Manual initiation capability of the mitigating systems at the system level is desirable but not required. Manual initiation should depend upon the operation

of a minimum of equipment. The mitigating system should be designed to provide the operator with accurate, complete and timely information pertinent to its own status.

Displays and controls for manual bypass and initiation of the mitigating system should be integrated into the main control room through system functional analysis and should conform to good human engineering practices in design and layout. It is important that the displays and controls added to the control room as a result of the ATWS rule not increase the potential for operator error. A human factor analysis should be performed taking into consideration:

(a) the use of this information and equipment by an operator during both normal and abnormal plant conditions,

(b) integration into emergency procedures,

(c) integration into operator training, and

(d) the presence of other alarms during an emergency and need for prioritization of alarms.

The power supplies are not required to be safety-related but they must be capable of performing safety functions with a loss of offsite power. Logic power must be from an instrument power supply <u>independent</u> from the power supplies for the existing reactor trip system. Existing RTS sensor and instrument channel power

supplies may be used only if the possibility of common mode failure is prevented.

The most severe ATWS scenarios were determined (see NUREG-0460 Appendix IV, WCAP-8330 and subsequent Westinghouse submittals) to be those in which there was a complete loss of normal feedwater. These included:

Loss of Normal Feedwater/ATWS Transient (LONF/ATWS)

A complete loss of normal feedwater occurs which results from a malfunction in the feedwater condensate system or its control system from such causes as the simultaneous trip of all condensate pumps, the simultaneous trip of all main feedwater pumps or the simultaneous closure of all main feedwater control, pump discharge or block valves. Because of a postulated common mode failure in the RPS, the reactor is incapable of being automatically tripped when any of several plant process variables have reached their reactor trip setpoints.

Loss of Load/ATWS Transient (LOL/ATWS)

The most severe plant conditions that could result from a loss of load occur following a turbine trip from full power when the turbine trip is caused by a loss of main condenser vacuum. Because of a common mode failure in the protection system, the reactor is incapable of being automatically tripped as a result of the turbine trip or as the result of any of several other reactor trip signals that occur later in time when several plant process variables reach their reactor trip setpoints.

Upon loss of the main condenser vacuum, the main feedwater turbine-driven pumps that exhaust into the main condenser are tripped, thereby cutting off feedwater flow to the steam generators. Not all nuclear plants are subject to this transient since many plants have motor-driven main feedwater pumps or they have turbine-driven pumps which do not exhaust into the main condenser. Since there is a complete loss of normal feedwater during both these transients (LONF/ATWS and LOL/ATWS), both transients assumed auxiliary feedwater (AFW) flow is started 60 seconds after the initiating event for long term reactor protection. Also the Complete Loss of Normal Feedwater transient assumed a turbine trip 30 seconds after the initiating event to maintain short term RCS pressures below 3200 psig. Normally these features would be actuated by the Reactor Protection System (RPS) and the Engineered Safety Features Actuation System (ESFAS).

The primary safety concern from these two transients is the potential for high pressure within the RCS. If a common mode failure in the RPS and the ESFAS incapacitates AFW flow initiation and/or turbine trip in addition to prohibiting a scram, then an alternate method of providing AFW flow and a turbine trip is required to maintain the RCS pressure below 3200 psig. The final rule which was approved by the Commissioners on November 11, 1983, requires that Westinghouse designed plants install ATWS Mitigating System Actuation Circuitry (AMSAC) to initiate a turbine trip and actuate AFW flow independent of the RPS (from the sensor output). These two functions, turbine trip and AFW flow actuation, are provided via the AMSAC.

4.0 DESIGN DESCRIPTION

The Westinghouse Owners Group (WOG) has developed generic designs to meet the requirements of 10 CFR 50.62. Three designs were developed which permits each utility to select the design which best fits a particular plant's needs. Factors that may determine the design utilized at a plant range from the current control and protection system design to the ease and cost of installation. The three designs are as follows:

The first design would actuate a turbine trip and auxiliary feedwater flow upon sensing that the steam generator inventory is below the low-low level setpoint. This logic senses conditions indicative of an ATWS event when a loss of heat sink has occurred but will not actuate until after the reactor protection signals should have been generated. A turbine trip and start-up of all auxiliary feedwater pumps will occur upon receipt of an AMSAC signal.

The steam generator blowdown isolation and sample isolation valves would be automatically closed in all loops when AMSAC is actuated.

The AMSAC signal will be generated by low water level signals in the steam generators using existing sensor/transmitter units. For two loop plants, AMSAC will use two channels per loop with 3/4 coincidence to actuate AMSAC. The AMSAC coincidence logic for three loop plants is 2/3 with one channel per steam generator and the four loop plants coincidence logic is 3/4 with one channel per steam generator.

The AMSAC signal will be automatically blocked below 70% power since short term protection against high reactor coolant system pressure is not required until 70% of nominal power. This will prevent spurious AMSAC actuation during start-up. To ensure that AMSAC remains armed long enough to perform its function in the event of a turbine trip, a C-20 permissive signal will be maintained for approximately 60 seconds. The AMSAC signal will be delayed by approximately 25 seconds to permit the RPS to respond first.

The second design mitigates the consequences of an ATWS loss of heat sink event by initiating AMSAC on low main feedwater flow measurements.

Actuation of AMSAC will occur on low main feedwater flow as measured by existing main feedwater flow sensor/transmitters. The setpoint to actuate AMSAC is 50% of nominal main feedwater flow. Although 50% flow is more than ample to protect against overpressure in the event of an ATWS, instrumentation error would become unacceptably large if a substantially lower setpoint were used.

To avoid inadvertent AMSAC actuation on the loss of one main feedwater pump, AMSAC actuation will be delayed approximately 25 seconds to permit the unfaulted main feedwater pump(s) to automatically increase the flow rate to above the AMSAC actuation setpoint. Recovery in this circumstance is possible since each main feedwater pump is capable of delivering typically 60% of full load capacity.

A turbine trip and start-up of all auxiliary feedwater pumps will occur upon receipt of an AMSAC signal. The steam generator blowdown isolation and sample

isolation valves should be automatically closed in all loops when AMSAC is actuated.

The AMSAC signal will be generated by low main feedwater flow to the steam generators. The AMSAC logic is two channels per loop with 3/4 coincidence logic for two loop plants; one channel per loop with 2/3 coincidence logic for three loop plants; and 3/4 coincidence logic for four loop plants.

As in the first design, the AMSAC signal will be automatically blocked below 70% power; the AMSAC signal will be delayed by 25 seconds; removal of the C-20 permissive signal will be delayed by approximately 60 seconds.

The third design determines that conditions indicative of an ATWS event are present by monitoring the feedwater control and isolation valves and the feedwater pump status.

Actuation of AMSAC will occur when it has been determined that all main feedwater pumps have been tripped or when main feedwater flow to the steam generators has been blocked due to valve closures.

Failures in the main feedwater system upstream of the main feedwater pumps that could result in the loss of main feedwater to the steam generators, e.g., tripping of all condensate pumps, will result in automatic main feedwater pump trips on low suction pressure. Therefore, explicit actuation of AMSAC based on failures of components upstream of the main feedwater pumps is not necessary.

Since AMSAC anticipates the plant response due to the loss of main feedwater pumps prior to the reactor protection system detecting an anticipated operational occurrence, it is desirable to delay AMSAC actuation. A 30 second delay is sufficient to allow the reactor protection system to respond.

Either of two different AMSAC concepts may be used, depending upon whether or not the main feedwater flow to the steam generators is split during normal power operation. Plants which contain D-4 and D-5 steam generators have split flow during normal ~~power~~ operation. All other plants do not, although all plants with preheaters will have a minimal bypass flow through the feedwater bypass tempering valve (FBTV). For preheater plants which have split flow during normal power operation, approximately 10 to 20% of the total feedwater flow is passed through the feedwater preheater bypass valves (FPBV), while most of the remaining flow is passed through the feedwater isolation valve (FIV). If all FIVs were to close simultaneously, the flow through the FPBV would increase substantially and still provide protection against RCS overpressurization in the event of an ATWS. Therefore the accidental closure of all FIVs is not a factor for plants which contain D-4 or D-5 steam generators. All other plants however must account for the accidental closure of all FIVs as well as the accidental closure of all feedwater control valves (FCVs) and the accidental tripping of all main feedwater pumps.

A turbine trip and start-up of all auxiliary feedwater pumps will occur upon receipt of an AMSAC signal. The steam generator blowdown isolation and sample

isolation valves should be automatically closed in all loops when AMSAC is actuated.

The AMSAC signal will be generated by the simultaneous tripping of all main feedwater pumps or the blocking of all main feedwater lines to the steam generators due to valve malfunctions. The AMSAC coincidence logic is as follows:

	Coincidence	
Loops	FW Valves Closed	FW Pumps Tripped
2	3/4	N/N
3	2/3	N/N
4	3/4	N/N

where N is the number of main feedwater pumps.

As in the first two designs, the AMSAC signal will be automatically blocked below 70% power and the removal of the C-20 permissive signal shall be delayed by approximately 60 seconds.

5.0 CONCLUSION:

Generic

The staff has reviewed the Westinghouse Topical Report WCAP-10858, "AMSAC Generic Design Package" and has concluded that the generic designs presented in WCAP-10858 adequately meet the requirements of 10 CFR 50.62 and follow the review guidelines that have been discussed previously.

Plant specific

WCAP-10858 presents a generic design, however many details and interfaces are of a plant specific nature. The staff will review the implementation of plant specific designs to evaluate compliance with ATWS rule requirements. Key elements of the plant specific design reviews are denoted below.

o Diversity

The plant specific submittal should indicate the degree of diversity that exists between the AMSAC equipment and the existing Reactor Protection System. Equipment diversity to the extent reasonable and practicable to minimize the potential for common cause failures is required from the sensors output to, but not including, the final actuation device, e.g., existing circuit breakers may be used for the auxiliary feedwater initiation. The sensors need not be of a diverse design or manufacture. Existing protection system instrument-sensing lines, sensors, and sensor power supplies may be used. Sensor and instrument sensing lines should be selected such that adverse interactions with existing control systems are avoided.

- Logic power supplies

  The plant specific submittal should discuss the logic power supply design. According to the rule, the AMSAC logic power supply is not required to be safety-related (Class 1E). However, logic power should be from an instrument power supply that is independent from the reactor protection system (RPS) power supplies. Our review of additional information submitted by WOG indicated that power to the logic circuits will utilize RPS batteries and inverters. The staff finds this portion of the design unacceptable, therefore, independent power supplies should be provided.

- Safety-related interface

  The plant specific submittal should show that the implementation is such that the existing protection system continues to meet all applicable safety criteria.

- Quality assurance

  The plant specific submittal should provide information regarding compliance with Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment that is not Safety-Related."

- Maintenance bypasses

  The plant specific submittal should discuss how maintenance at power is accomplished and how good human factors engineering practice is incorporated into the continuous indication of bypass status in the control room.

- Operating bypasses

  The plant specific submittal should state that operating bypasses are continuously indicated in the control room; provide the basis for the 70% or plant specific operating bypass level; discuss the human factors design aspects of the continuous indication; and discuss the diversity and independence of the C-20 permissive signal (Defeats the block of AMSAC).

- Means for bypassing

  The plant specific submittal should state that the means for bypassing is accomplished with a permanently installed, human factored, bypass switch or similar device, and verify that disallowed methods mentioned in the guidance are not utilized.

- Manual initiation

  The plant specific submittal should discuss how a manual turbine trip and auxiliary feedwater actuation are accomplished by the operator.

- Electrical independence from existing reactor protection system

  The plant specific submittal should show that electrical independence is achieved. This is required from the sensor output to the final actuation device at which point non-safety-related circuits must be isolated from safety related circuits by qualified Class 1E isolators. Use of existing isolators is acceptable. However, each plant specific submittal should provide an analysis and tests which demonstrates that the existing isolator will

function under the maximum worst case fault conditions. The required method for qualifying either the existing or diverse isolators is presented in Appendix A.

o Physical separation from existing reactor protection system

Physical separation from existing reactor protection system is not required, unless redundant divisions and channels in the existing reactor trip system are not physically separated. The implementation must be such that separation criteria applied to the existing protection system are not violated. The plant specific submittal should respond to this concern.

o Environmental qualification

The plant specific submittal should address the environmental qualification of ATWS equipment for anticipated operational occurrences only, not for accidents.

o Testability at power

Measures are to be established to test, as appropriate, non safety related ATWS equipment prior to installation and periodically. Testing of AMSAC may be performed with AMSAC in bypass. Testing of AMSAC outputs through the final actuation devices will be performed with the plant shutdown. The plant specific submittals should present the test program and state that the output signal is indicated in the control room in a manner consistent with plant practices including human factors.

- Completion of mitigative action

  AMSAC shall be designed so that, once actuated, the completion of mitigating action shall be consistent with the plant turbine trip and auxiliary feedwater circuitry. Plant specific submittals should verify that the protective action, once initiated, goes to completion, and that the subsequent return to operation requires deliberate operator action.

- Technical specifications

  Technical specification requirements related to AMSAC will have to be addressed by plant specific submittals.

APPENDIX A
AMSAC ISOLATION DEVICE -
REQUEST FOR ADDITIONAL INFORMATION

Each light water cooled nuclear reactor shall be provided with a system for the mitigation of the effects from anticipated transients without scram (ATWS). The Commission approved requirements for the ATWS are defined in the Code of Federal Regulations (CFR) Section 10, paragraph 50.62.

The staff has reviewed the Westinghouse Owner's Group generic functional AMSAC designs for compliance with the ATWS Rule. As a result, the staff has determined that the use of isolators within AMSAC will be reviewed on a plant specific basis. The following additional information is required to continue and complete the plant specific isolator review:

Isolation Devices

Please provide the following:

a. For the type of device used to accomplish electrical isolation, describe the specific testing performed to demonstrate that the device is acceptable for its application(s). This description should include elementary diagrams when necessary to indicate the test configuration and how the maximum credible faults were applied to the devices.

b. Data to verify that the maximum credible faults applied during the test were the maximum voltage/current to which the device could be exposed, and define how the maximum voltage/current was determined.

c. Data to verify that the maximum credible fault was applied to the output of the device in the transverse mode (between signal and return) and other faults were considered (i.e., open and short circuits).

d. Define the pass/fail acceptance criteria for each type of device.

e. Provide a commitment that the isolation devices comply with the environment qualifications (10 CFR 50.49) and with the seismic qualifications which were the basis for plant licensing.

f. Provide a description of the measures taken to protect the safety systems from electrical interference (i.e., Electrostatic Coupling, EMI, Common Mode and Crosstalk) that may be generated by the ATWS circuits.

g. Provide information to verify that the Class 1E isolator is powered from a Class 1E source.