UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

SAFETY EVALUATION BY THE OFFICE NUCLEAR REACTOR REGULATION

COMPLIANCE WITH ATWS RULE 10 CFR 50.62

RELATING ALTERNATE ROD INJECTION (ARI) AND

RECIRCULATING PUMPS TRIP (RPT) SYSTEMS

JAMES A. FITZPATRICK NUCLEAR POWER PLANT

DOCKET NO. 50-333

1.0 INTRODUCTION

On July 26, 1984, the Code of Federal Regulation (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 operation 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 shutdown 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 shutdown the reactor following anticipated transients, and to mitigate the consequences of an ATWS event.

For each boiling water reactor, three systems are required to mitigate the consequences of an ATWS event.

1. It must have an alternate rod injection (ARI) system that is diverse (from the reactor trip system) from sensor output to the final actuation devices. The ARI system must have redundant scram air header exhaust valves. The ARI system must be designed to perform its function in a reliable manner and be independent (from the existing reactor trip system) from sensor output to the final actuation device.

2. It must have a standby liquid control system (SLCS) with a minimum flow capacity and boron content equivalent in control capacity to 86 gallons per minute of 13 weight percent sodium pentaborate solution. The SLCS and its injection location must be designed to perform its function in a reliable manner.

3. It must have equipment to trip the reactor coolant recirculating pumps automatically under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner.

By letters dated October 11, 1985, April 15, 1987, and June 10, 1988, New York Power Authority (the licensee) provided information regarding this equipment installation in accordance with the ATWS Rule. This safety evaluation report, addresses the ARI system (Item 1) and the ATWS/RPT system (Item 3). The SLCS (Item 2) was addressed in a separate safety evaluation report dated September 8, 1987.

2.0 REVIEW CRITERIA

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 important to safety defined in the introduction of 10 CFR 50, Appendix A, General Design Criteria (GDC). 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 Assurance 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 in the RTS) to reduce the potential for common mode failures that could result in an ATWS leading to unacceptable plant conditions.

The staff's position on diversity requirements is addressed in Appendix 1 of this report. The criteria used in evaluating the licensee's submittal include 10 CFR 50.62, "Rule Considerations Regarding Systems and Equipment Criteria" published in Federal Register Volume 49, No. 124 dated June 26, 1984 and Generic Letter 85-06 "Quality Assurance Guidance for ATWS Equipment That is not Safety Related."

3.0 FITZPATRICK ARI SYSTEM DESCRIPTION

The FitzPatrick ARI system is designed in accordance with the guidance specified in the BWROG Topical Report NEDE-31096. The ARI system will utilize five valves at the scram pilot air header. One 3-way solenoid ARI valve will be installed in series with the existing backup scram valves. Four two-way solenoid ARI valves will be installed one each at the East Scram Discharge Volume (SDV) piping, the West SDV piping, the Hydraulic Control Units (HCU) bank A subheader, and the HCU bank B subheader. The ARI logic will be "one-out-of-two" taken twice for reactor vessel low water level or reactor vessel high pressure. ARI circuitry will be installed in the ECCS cabinets which are separate from the RPS cabinets. The ARI valves will be sealed in for 25 seconds following an ARI initiation to ensure the completion of the scram pilot air headers depressurization. The ARI logic will be testable during plant operation.

4.0 EVALUATION OF ARI SYSTEM

The licensee participated in the BWR Owners' Group ATWS implementation alternatives program. The BWR Owners' Group submitted a licensing topical report NEDE-31096-P "Anticipated Transients Without Scram, Response to NRC ATWS Rule 10 CFR 50.62" (Reference 2) for staff review. The staff acceptance of the licensing topical report NEDE-31096-P is discussed in Reference 3. Reference 1 summarizes the licensee's compliance with the ATWS Rule. The staff's evaluation is addressed in the following sections.

4.1 ARI SYSTEM FUNCTION TIME

The ARI logic is initiated immediately upon receipt of a high Reactor Vessel (RV) pressure signal or upon receipt of a low-low RV water level signal. Rod injection will begin within 15 seconds after ARI Solenoid Valves (SOVs) have tripped. Within 25 seconds all control rods injection will have been completed. A preoperational test will be performed to verify the ARI system function time (by measuring the scram air header pressure depressurization time). The staff finds this acceptable.

4.2 SAFETY-RELATED REQUIREMENTS

The ATWS Rule does not require the ARI system to be safety grade, but the implementation must be such that the existing protection system continues to meet all applicable safety-related criteria.

The ARI system initiation signals are originated from the Emergency Core Cooling System (ECCS) output relays. The ARI system does not interface with the Reactor Trip System (RTS). Any failures in the ARI system will not prevent the existing reactor trip system from performing its protective functions. The interface between the ECCS and the ARI system is from relay to contact isolation which is qualified as a Class 1E isolator. The staff finds this acceptable.

4.3 REDUNDANCY

The ARI system has redundant valves at the scram air header. The ARI system performs a function redundant to the back up scram system. All vent paths will function to meet the design basis rod injection times. This is in conformance with the BWROG design guideline. The staff finds this acceptable.

4.4 DIVERSITY FROM THE EXISTING RTS

The licensee stated that the ARI system is diverse and independent from the reactor trip system. The ARI solenoid valves are DC powered with the solenoid valves energized to open. Based on the licensee submittal dated June 10, 1988, the licensee stated that the ARI system will use Rosemount 510 DU analog trip units which are the same type and model as the units used for the reactor trip system.

It is the staff's position that the ARI system components are required to be diverse from the reactor trip system from sensor output to the final actuation device. Diversity was the most important factor regarding the implementation of the ATWS mitigation equipment because the common mode failures were determined to be a larger safety risk than random failures. Based on the relative importance of this diversity requirement, the staff has concluded that the type of signal conditioning (Rosemount analog transmitter/trip units) provided for the FitzPatrick ARI system is not acceptable in that it is identical to the reactor trip system signal conditioning equipment.

The staff learned that compatible trip unit circuit boards manufactured by a different vendor, which are fully qualified as a replacement for the Rosemount ATTUs, are available. If the alternate boards were used in the ARI system, sufficient diversity would exist between the ARI system and the RTS. Such a modification appears reasonable and practical. However, implementation of the ARI system should not be slowed to resolve this issue since there is a clear safety benefit even with Rosemount ATTUs.

Having considered the need for additional time to change from the existing Rosemount trip units to provide compliance with 10 CFR 50.62, the Commission agrees with an extension of time to fully comply with 10 CFR 50.62 until no later than the end of the next refueling outage. Another alternative, permitted by the provisions of 10 CFR 50.12, would be to request an exemption from 10 CFR 50.62. However, we do not recommend this option.

4.5 ELECTRICAL INDEPENDENCE FROM THE EXISTING RTS

The ARI actuation logic is independent form the RTS logic. Independent trip cards and relays located in separate cabinets are utilized for each system. The ARI circuits are totally independent from RTS circuits. The staff finds this acceptable.

4.6 PHYSICAL SEPARATION FROM THE EXISTING RTS

The ARI system is physically separated from the RTS. All ARI system analog trip and actuation logic components are located in cabinets which are physically separate from the cabinets which house RTS components. In addition, sensors and the final actuation devices (ARI SOVs) for the ARI System are physically separate from those used in the RTS. ARI SOVs and RTS SCRAM SOVs are located in different areas of the Reactor Building. The staff finds this acceptable.

4.7 ENVIRONMENTAL QUALIFICATION

The ARI equipment is not required to function for any design basis accident or high energy line break. The ARI equipment to be installed at FitzPatrick, will be qualified to conditions of temperature, pressure, humidity, and radiation levels postulated to exist during an ATWS event (up to the time the ARI function is completed) and therefore is acceptable.

4.8 QUALITY ASSURANCE

The licensee stated that the Quality Assurance Program will comply with Generic Letter 85-06 requirements. The staff finds this acceptable.

4.9 SAFETY-RELATED POWER SUPPLY

The ARI power is independent from the RTS and is powered by separate safety related 125 Vdc systems. The ARI system can perform its function during any loss of offsite power event. During normal operation the continuous dc load is supplied by the battery chargers which are connected to the dc buses. The redundant dc power system batteries have adequate capacity to supply their emergency loads for at least two hours without charging. The staff finds this acceptable.

4.10 TESTABILITY AT POWER

The ATWS Rule guidance states that the ARI system should be testable at power. The ARI system is designed such that the periodic surveillance test can be performed during normal plant operation. The testing includes the relay logic to initiate ARI valves actuation. Testing of the final actuation device (ARI valves) while the reactor is at power is not required.

The staff has reviewed the licensee's ARI system circuitry. The staff finds that the design does not permit testing of the ARI valve actuating relay and the ARI valve itself. This is not in conformance with the ARI system design guideline which only exempts the ARI valve testing while the plant is at power operation. During a conference call dated July 7, 1988, the licensee committed to modify the ARI system test scheme such that all the ARI system components are testable during normal plant operation. A bypass switch will be used during the on-line testing to minimize the inadvertent actuation. The bypass status is automatically and continuously indicated in the main control room. The licensee is required to document the modified design for staff audit. This is a confirmatory item.

4.11 INADVERTENT ACTION

The ARI design utilizes the "one-out-of-two" twice coincident logic. Both channels must be tripped in order to initiate the mitigative actions. The ARI actuation setpoints will not challenge scram setpoints. The staff finds this acceptable.

4.12 MANUAL INITIATION

The ARI system can be manually initiated from the control room. The staff finds this acceptable.

4.13 INFORMATION READOUT

ARI valve position indicating lights are provided on the ARI logic panel in the relay room as well as on panel 09-5 in the control room. An ARI test light and a scram header air pressure indicator are also located on panel 09-5 in the control room. There will be an annunciator to alert the operator that the ARI system has been initiated. The staff finds this acceptable.

4.14 COMPLETION OF PROTECTIVE ACTION ONCE IT IS INITIATED

Both the automatic and manual actuator signals for the ARI design will have a seal-in feature to ensure the completion of protective action once it is initiated. After removal of the initiating signal, this seal-in is required to be manually reset. The staff finds this acceptable.

4.15 CONCLUSION ON ARI SYSTEM

As stated in Reference 3, the staff SER on BWROG Topical Report NEDE-31096-P, the staff does not intend to repeat its review of the design information described in the BWROG Topical Report and found acceptable when the report appears as a reference in a specific license application. Reference 1 summarizes the licensee's compliance with the ATWS Rule. The staff finds that one area (e.g. diversity) of FitzPatrick ARI design is not in compliance with the ATWS Rule, 10 CFR 50.62, and as a result, the ARI system is not acceptable. This is discussed in more detail in section 4.4, of this evaluation. The licensee is required to document the design modification on ARI system test scheme as discussed in section 4.10 of this evaluation.

5.0 FITZPATRICK ATWS/RPT SYSTEM DESCRIPTION

The existing ATWS/RPT system uses a single trip coil to trip the 4.16 KV motor generator feeder breaker, thus opening the breaker for each recirculation system M-G set drive motor. Each recirculation system M-G set is tripped independently of the other M-G set. The trip logic is arranged in a "one-out of-two" logic scheme. The trip signal is initiated by either one of two reactor vessel low water level or one of two reactor vessel high pressure. The ATWS/RPT system and the ARI system use the same transmitters, and trip units. These components are located in the ECCS cabinets.

6.0 EVALUATION OF ATWS/RPT SYSTEM

6.1 RECIRCULATING PUMP BREAKER RELIABILITY

During the staff's review of the Brunswick (Docket No. 50-324) ATWS/RPT system, the staff raised a concern that the Brunswick design has only one trip coil in a single breaker to trip the pump while the previously approved Monticello (Docket No. 50-263) design has redundant coils in a single breaker to trip the pump. The staff required the Brunswick licensee to demonstrate that their present RPT design can perform its function in a reliable manner equivalent to the Monticello design. Based on the failure rate calculation presented by the licensee, and an independent survey from Region I, the staff concluded that the reliability of the Brunswick RPT system is equivalent to the Monticello RPT system and therefore is acceptable. The main reason for accepting the Brunswick design is that Brunswick uses more reliable 4KV high-voltage breakers to trip the pumps and the trip initiation logic has been upgraded to satisfy the ATWS Rule guidelines.

The FitzPatrick design uses the same type of high-voltage breakers as Brunswick. Based on the reliability assessment presented by FitzPatrick submittal, the staff concludes that the recirculating pump breaker reliability concern is resolved. The single coil arrangement at FitzPatrick RPT design is acceptable.

6.2 RECIRCULATING PUMP TRIP INITIATION LOGIC

The FitzPatrick RPT initiation logic design uses a "one-out-of-two" logic scheme. The trip signal is initiated by either one of two reactor vessel low water level or one of two reactor vessel high pressure. The staff finds that the "one-out-of-two" logic scheme is not in conformance with ATWS Rule guideline in two aspects:

1. The ATWS Rule requires that the RPT shall be designed such that periodic surveillance tests can be performed during normal plant operation to provide assurance that the RPT logic and controls are capable of functioning as designed. The staff finds that the FitzPatrick RPT design does not satisfy this requirement.

2. The ATWS Rule guidance states that the design should be such that the frequency of inadvertent actuation and challenges to other safety systems is minimized. The staff finds that with a "one-out-of-two" trip scheme, the potential for inadvertent actuation is higher than the coincident logic scheme. In view of the recent LaSalle Unit 2 power oscillation event (NRC Bulletin No. 88-07), the inadvertent recirculation pump trip was the trigger event. The staff concluded that the "one-out-of-two" trip scheme is not a prudent design to minimize the inadvertent recirculation pump trip.

Most BWR ATWS/RPT trip systems are tripping both pumps using the same logic configuration. The FitzPatrick design the trips two pumps independently. The licensee should demonstrate that this arrangement still satisfies the objective of the ATWS mitigation function.

6.3 CONCLUSION ON ATWS/RPT SYSTEM

The staff finds that the FitzPatrick ATWS/RPT initiation logic design is not in conformance with the ATWS Rule, 10 CFR 50.62, and as a result, the ATWS/RPT system is not acceptable.

7.0 TECHNICAL SPECIFICATION MODIFICATION

The equipment required by the ATWS Rule to reduce the risk associated with an ATWS event must be designed to perform its function in a reliable manner. A method acceptable to the staff for demonstrating that the equipment satisfies the reliability requirements of the ATWS Rule is to provide equipment technical specifications including operability and surveillance requirements. Although the FitzPatrick plant technical specifications have incorporated the ATWS/RPT system, the operability and surveillance requirements have not been fully specified. It is expected that this issue will be addressed coincidently with the other outstanding non-conforming issues described herein.

8.0 REFERENCES

1. New York Power Authority letter John C. Brons to NRC Document Control Desk, dated April 15, 1987.

2. BWROG Topical Report NEDE-31096-P "Anticipated Transients Without Scram; Response to NRC ATWS Rule 10CFR50.62," dated December 1985.

3. Staff SER on BWROG Topical Report NEDE-31096-P. Letter from Gus Lainas (NRC) to Terry A. Pickens (BWR Owners' Group Chairman), dated October 21, 1986.

4. New York Power Authority letter John C. Brons to NRC Document Control Desk, dated October 11, 1985.

5. New York Power Authority letter John C. Brons to NRC Document Control Desk, dated June 10, 1988.

APPENDIX 1: THE STAFF POSISTION ON DIVERSITY REQUIREMENTS

The basic premise behind the ATWS rule as documented in SECY-83-293, "Amendments to 10 CFR 50 Related to Anticipated Transients Without Scram (ATWS) Events" is to require systems/equipment that are diverse (and independent) to those portions of the existing reactor trip system (RTS) where only minimal diversity is currently provided, and which are capable of preventing or mitigating the consequences of an ATWS event. An ATWS event is defined as 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 RTS to shutdown the reactor. The failure mechanism of concern is a common mode failure of identical components within the RTS (e.g., logic channels, actuation devices and instrument channels excluding sensors).

Common mode failures (CMFs) are failures of identical components due to the same failure mechanism (e.g., manufacturing defect, design defect, calibration or maintenance error). Common cause failures are a broader class of failures consisting of the failure of multiple components, not necessarily identical in design, due to the same cause, typically environmental in nature (e.g., extreme temperature, humidity induced corrosion, vibration). Although existing RTS are considered to have by design sufficient redundancy and testability features to prevent random failures from leading to system unavailability, because the redundant components are in general identical in manufacturer and design, they are subject to potential common mode failures. Existing reactor trip systems are typically located in controlled environments, and thus, the potential for many types of common cause failures is minimized. Common mode failures are a subset of common cause failures. Common mode failures, but not necessarily common cause failures, can be eliminated by providing total/absolute diversity. The diversity required by the ATWS rule is intended to ensure that common mode failures which disable the electrical portion of the existing reactor trip system will not affect the capability of systems/equipment installed in accordance with ATWS rule requirements (to prevent or mitigate the consequences of ATWS events) to perform their design functions. Therefore, the diversity required by the ATWS rule is hardware/component diversity (to prevent CMFs from disabling both the existing RTS and ATWS preventive/mitigative systems). It is recognized that total/absolute component/hardware diversity can be difficult and sometimes impossible to achieve. For these instances, acceptable level of component/hardware diversity can be achieved in accordance with combinations of allowable methods such as energication states, AC versus DC power, functional capability, and the use of components from different manufacturers.

The concept of equipment/hardware diversity has been firmly established and well documented throughout the history of the ATWS issude and rulemaking process. Appendix C (ATWS Equipment Requirements) to NUREG-0460, "Anticipated Transients Without Scram for Light Water Reactors," Volume 3 (published in December 1978) states that the equipment (installed to prevent/mitigate the consequences of ATWS events) shall be independent and separate from components for systems that initiate the anticipated transient(s) being analyzed and diverse from the normal scram system (postulated to fail) to minimze the probability of the ATWS disabling its operation.

The supplementary information provided with the Federal Register notification of the ATWS rule includes guidance concerning the diversity required of diverse reactor trip systems (diverse scram systems) and mitigating systems from the existing reactor trip system. The guidance states that equipment diversity to minimize the potential for common cause failures is required from sensor output to and including the components used to interrupt control rod power (circuit breakers from different manufacturers alone is not sufficient to provide the required diversity for interruption of control rod power) for diverse scram systems, and from sensor output to, but not including, the final actuation device for mitigating systems (e.g., diverse turbine trip and diverse auxiliary feedwater actuation). Therefore, all diverse scram system and mitigating systems instrument channel components (excluding sensors and signal conditioning equipment upstream of the bistables) and logic channel components, and all diverse scram system actuation devices must be diverse from the existing RTS in accordance with the methods of achieving required equipment diversity identified above to obtain a level of diversity acceptable to satisfy the requirements of the ATWS rule. Identical components used in both the existing RTS and the diverse scram system or mitigating systems are subject to potential common mode failures, and therefore, are not acceptable.

November 18, 1988

Docket No. 50-333

DISTRIBUTION

Docket File	DLaBarge
NRCPDR	JJohnson
Local PDR	OGC
PDI-1 Rdg.	EJordan
SVarga	BGrimes
BBoger	ACRS (10)
RCapra	CVogan
SNewberry	JMauck

Mr. John C. Brons
Executive Vice President, Nuclear Generation
Power Authority of the State
of New York
123 Main Street
White Plains, New York 10601

Dear Mr. Brons:

SUBJECT: ATWS IMPLEMENTATION STATUS

By letters dated June 14, 1985 and October 11, 1985, you submitted your proposed schedule, as required by 10 CFR 50.62(d), for completing the Anticipated Transients Without Scram (ATWS) modifications required for the FitzPatrick Nuclear Power Plant. You proposed to implement the required modification by the end of the third refueling outage after the ATWS rule effective date of July 26, 1984. The rule requires that justification be provided for a schedule calling for final implementation later than the second refueling outage after the effective date of the rule.

In your June 14, 1985 letter you delineated the major modifications related to the ATWS Rule which were planned for the second refueling outage following the effective date of the ATWS rule. Your letter also stated that, because of the total number and scope of modifications planned, and the necessity that the ATWS modifications be performed during an outage, all modifications could not be completed by the end of the 1985 outage. Additionally, your letter of October 11, 1985 indicated that the valves comprising the Alternate Rod Injection (ARI) System, which will be installed to comply with the ATWS rule, are long lead items with a delivery time of about 50 weeks. Taking into consideration the time required for engineering, design, and material procurement, you stated that the ARI system could not be installed before the following (1988) refueling outage. This was found to be acceptable to the NRC and transmitted to you in a letter to you dated November 29, 1985.

In your letter of April 15, 1987 you presented information demonstrating conformance with the ATWS Rule. For the ARI system you supplied a completed checklist from Appendix A of the Safety Evaluation, stated that the requirements for qualification information related to isolation valves contained in Appendix B of the Safety Evaluation will be met and briefly described the separation and testability aspects of the design. For the Recirculation Pump Trip (RPT) system you endorsed the BWR Owner's Group position that redundant trip coils in the circuit breaker for each recirculation pump are not required to comply with the ATWS Rule.

In your June 10, 1988 letter you supplied further information concerning the ARI and RPT systems. This included an analysis of the ARI and reactor protection system (RPS) separation design to comply with the ATWS Rule

8811210204 3PP

concerning diversity which led to your position that the ARI meets the diversity requirement and is consistent with the BWR Owner's Group licensing topical report. Since the modifications are being made during the present refuel outage, you requested an extension of at least one more cycle if the design is considered unacceptable. The conclusion was also reached in your letter that the RPT breaker design was consistent with the ATWS Rule.

We have reviewed these submittals and have concluded that the ARI & RPT designs are not completely acceptable. However, we do not believe that these issues are of sufficient safety significance to delay implementation of the ARI system, replace equipment already installed, or delay startup from the present refuel outage. In order to comply with the ATWS Rule, the ARI system should be provided with instrument components that are diverse from the reactor trip system, the RPT initiation logic should be modified for diversity, and logic testing features should be provided before restart following the next refueling outage. Our SER, which provides the review details regarding this conclusion is enclosed. Your letter of August 25, 1988 outlining the proposed logic testing revisions is under review. It is expected that its provisions will be included in a subsequent submittal to address the remaining ARI/RPT issues outlined herein.

Sincerely,

original signed by

David L. LaBarge, Project Manager
Project Directorate I-1
Division of Reactor Projects, I/II

Enclosures:
1. Safety Evaluation
2. Appendix 1

cc: See next page

OFC	:PDI-1	:PDI-1	:PDI-1	:	:	:
NAME	:CVogan	:DLaBarge:dlg	:vr:RCapra	:	:	:
DATE	:11/ /88	:11/17/88	:11/18/88	:	:	:

OFFICIAL RECORD COPY

Mr. John C. Brons
Power Authority of the State of New York

James A. FitzPatrick Nuclear
Power Plant

cc:

Mr. Gerald C. Goldstein
Assistant General Counsel
Power Authority of the State
of New York
10 Columbus Circle
New York, New York 10019

Resident Inspector's Office
U. S. Nuclear Regulatory Commission
Post Office Box 136
Lycoming, New York 13093

Mr. Radford J. Converse
Resident Manager
James A. FitzPatrick Nuclear
Power Plant
Post Office Box 41
Lycoming, New York 13093

Mr. J. A. Gray, Jr.
Director Nuclear Licensing - BWR
Power Authority of the State
of New York
123 Main Street
White Plains, New York 10601

Mr. Robert P. Jones, Supervisor
Town of Scriba
R. D. #4
Oswego, New York 13126

Mr. J. P. Bayne, President
Power Authority of the State
of New York
10 Columbus Circle
New York, New York 10019

Mr. Richard Patch
Quality Assurance Superintendent
James A. FitzPatrick Nuclear
Power Plant
Post Office Box 41
Lycoming, New York 13093

Charlie Donaldson, Esquire
Assistant Attorney General
New York Department of Law
120 Broadway
New York, New York 10271

Ms. Donna Ross
New York State Energy Office
2 Empire State Plaza
16th Floor
Albany, New York 12223

Regional Administrator, Region I
U.S. Nuclear Regulatory Commission
475 Allendale Road
King of Prussia, Pennsylvania 19406

Mr. A. Klausman
Senior Vice President - Appraisal
and Compliance Services
Power Authority of the State
of New York
10 Columbus Circle
New York, New York 10019

Mr. George Wilverding, Manager
Nuclear Safety Evaluation
Power Authority of the State
of New York
123 Main Street
White Plains, New York 10601

Mr. R. E. Beedle
Vice President Nuclear Support
Power Authority of the State
of New York
123 Main Street
White Plains, New York 10601

Mr. S. S. Zulla
Vice President Nuclear Engineering
Power Authority of the State
of New York
123 Main Street
White Plains, New York 10601

Mr. R. Burns
Vice President Nuclear Operations
Power Authority of the State
of New York
123 Main Street
White Plains, New York 10601

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

SAFETY EVALUATION BY THE OFFICE NUCLEAR REACTOR REGULATION

COMPLIANCE WITH ATWS RULE 10 CFR 50.62

RELATING ALTERNATE ROD INJECTION (ARI) AND

RECIRCULATING PUMPS TRIP (RPT) SYSTEMS

JAMES A. FITZPATRICK NUCLEAR POWER PLANT

DOCKET NO. 50-333

1.0 INTRODUCTION

On July 26, 1984, the Code of Federal Regulation (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 operation 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 shutdown 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 shutdown the reactor following anticipated transients, and to mitigate the consequences of an ATWS event.

For each boiling water reactor, three systems are required to mitigate the consequences of an ATWS event.

1. It must have an alternate rod injection (ARI) system that is diverse (from the reactor trip system) from sensor output to the final actuation devices. The ARI system must have redundant scram air header exhaust valves. The ARI system must be designed to perform its function in a reliable manner and be independent (from the existing reactor trip system) from sensor output to the final actuation device.

2. It must have a standby liquid control system (SLCS) with a minimum flow capacity and boron content equivalent in control capacity to 86 gallons per minute of 13 weight percent sodium pentaborate solution. The SLCS and its injection location must be designed to perform its function in a reliable manner.

8811210205 10pp

3. It must have equipment to trip the reactor coolant recirculating pumps automatically under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner.

By letters dated October 11, 1985, April 15, 1987, and June 10, 1988, New York Power Authority (the licensee) provided information regarding this equipment installation in accordance with the ATWS Rule. This safety evaluation report, addresses the ARI system (Item 1) and the ATWS/RPT system (Item 3). The SLCS (Item 2) was addressed in a separate safety evaluation report dated September 8, 1987.

2.0 REVIEW CRITERIA

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 important to safety defined in the introduction of 10 CFR 50, Appendix A, General Design Criteria (GDC). 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 Assurance 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 in the RTS) to reduce the potential for common mode failures that could result in an ATWS leading to unacceptable plant conditions.

The staff's position on diversity requirements is addressed in Appendix 1 of this report. The criteria used in evaluating the licensee's submittal include 10 CFR 50.62, "Rule Considerations Regarding Systems and Equipment Criteria" published in Federal Register Volume 49, No. 124 dated June 26, 1984 and Generic Letter 85-06 "Quality Assurance Guidance for ATWS Equipment That is not Safety Related."

3.0 FITZPATRICK ARI SYSTEM DESCRIPTION

The FitzPatrick ARI system is designed in accordance with the guidance specified in the BWROG Topical Report NEDE-31096. The ARI system will utilize five valves at the scram pilot air header. One 3-way solenoid ARI valve will be installed in series with the existing backup scram valves. Four two-way solenoid ARI valves will be installed one each at the East Scram Discharge Volume (SDV) piping, the West SDV piping, the Hydraulic Control Units (HCU) bank A subheader, and the HCU bank B subheader. The ARI logic will be "one-out-of-two" taken twice for reactor vessel low water level or reactor vessel high pressure. ARI circuitry will be installed in the ECCS cabinets which are separate from the RPS cabinets. The ARI valves will be sealed in for 25 seconds following an ARI initiation to ensure the completion of the scram pilot air headers depressurization. The ARI logic will be testable during plant operation.

4.0 EVALUATION OF ARI SYSTEM

The licensee participated in the BWR Owners' Group ATWS implementation alternatives program. The BWR Owners' Group submitted a licensing topical report NEDE-31096-P "Anticipated Transients Without Scram, Response to NRC ATWS Rule 10 CFR 50.62" (Reference 2) for staff review. The staff acceptance of the licensing topical report NEDE-31096-P is discussed in Reference 3. Reference 1 summarizes the licensee's compliance with the ATWS Rule. The staff's evaluation is addressed in the following sections.

4.1 ARI SYSTEM FUNCTION TIME

The ARI logic is initiated immediately upon receipt of a high Reactor Vessel (RV) pressure signal or upon receipt of a low-low RV water level signal. Rod injection will begin within 15 seconds after ARI Solenoid Valves (SOVs) have tripped. Within 25 seconds all control rods injection will have been completed. A preoperational test will be performed to verify the ARI system function time (by measuring the scram air header pressure depressurization time). The staff finds this acceptable.

4.2 SAFETY-RELATED REQUIREMENTS

The ATWS Rule does not require the ARI system to be safety grade, but the implementation must be such that the existing protection system continues to meet all applicable safety-related criteria.

The ARI system initiation signals are originated from the Emergency Core Cooling System (ECCS) output relays. The ARI system does not interface with the Reactor Trip System (RTS). Any failures in the ARI system will not prevent the existing reactor trip system from performing its protective functions. The interface between the ECCS and the ARI system is from relay to contact isolation which is qualified as a Class 1E isolator. The staff finds this acceptable.

4.3 REDUNDANCY

The ARI system has redundant valves at the scram air header. The ARI system performs a function redundant to the back up scram system. All vent paths will function to meet the design basis rod injection times. This is in conformance with the BWROG design guideline. The staff finds this acceptable.

4.4 DIVERSITY FROM THE EXISTING RTS

The licensee stated that the ARI system is diverse and independent from the reactor trip system. The ARI solenoid valves are DC powered with the solenoid valves energized to open. Based on the licensee submittal dated June 10, 1988, the licensee stated that the ARI system will use Rosemount 510 DU analog trip units which are the same type and model as the units used for the reactor trip system.

It is the staff's position that the ARI system components are required to be diverse from the reactor trip system from sensor output to the final actuation device. Diversity was the most important factor regarding the implementation of the ATWS mitigation equipment because the common mode failures were determined to be a larger safety risk than random failures. Based on the relative importance of this diversity requirement, the staff has concluded that the type of signal conditioning (Rosemount analog transmitter/trip units) provided for the FitzPatrick ARI system is not acceptable in that it is identical to the reactor trip system signal conditioning equipment.

The staff learned that compatible trip unit circuit boards manufactured by a different vendor, which are fully qualified as a replacement for the Rosemount ATTUs, are available. If the alternate boards were used in the ARI system, sufficient diversity would exist between the ARI system and the RTS. Such a modification appears reasonable and practical. However, implementation of the ARI system should not be slowed to resolve this issue since there is a clear safety benefit even with Rosemount ATTUs.

Having considered the need for additional time to change from the existing Rosemount trip units to provide compliance with 10 CFR 50.62, the Commission agrees with an extension of time to fully comply with 10 CFR 50.62 until no later than the end of the next refueling outage. Another alternative, permitted by the provisions of 10 CFR 50.12, would be to request an exemption from 10 CFR 50.62. However, we do not recommend this option.

4.5 ELECTRICAL INDEPENDENCE FROM THE EXISTING RTS

The ARI actuation logic is independent form the RTS logic. Independent trip cards and relays located in separate cabinets are utilized for each system. The ARI circuits are totally independent from RTS circuits. The staff finds this acceptable.

4.6 PHYSICAL SEPARATION FROM THE EXISTING RTS

The ARI system is physically separated from the RTS. All ARI system analog trip and actuation logic components are located in cabinets which are physically separate from the cabinets which house RTS components. In addition, sensors and the final actuation devices (ARI SOVs) for the ARI System are physically separate from those used in the RTS. ARI SOVs and RTS SCRAM SOVs are located in different areas of the Reactor Building. The staff finds this acceptable.

4.7 ENVIRONMENTAL QUALIFICATION

The ARI equipment is not required to function for any design basis accident or high energy line break. The ARI equipment to be installed at FitzPatrick, will be qualified to conditions of temperature, pressure, humidity, and radiation levels postulated to exist during an ATWS event (up to the time the ARI function is completed) and therefore is acceptable.

4.8 QUALITY ASSURANCE

The licensee stated that the Quality Assurance Program will comply with Generic Letter 85-06 requirements. The staff finds this acceptable.

4.9 SAFETY-RELATED POWER SUPPLY

The ARI power is independent from the RTS and is powered by separate safety related 125 Vdc systems. The ARI system can perform its function during any loss of offsite power event. During normal operation the continuous dc load is supplied by the battery chargers which are connected to the dc buses. The redundant dc power system batteries have adequate capacity to supply their emergency loads for at least two hours without charging. The staff finds this acceptable.

4.10 TESTABILITY AT POWER

The ATWS Rule guidance states that the ARI system should be testable at power. The ARI system is designed such that the periodic surveillance test can be performed during normal plant operation. The testing includes the relay logic to initiate ARI valves actuation. Testing of the final actuation device (ARI valves) while the reactor is at power is not required.

The staff has reviewed the licensee's ARI system circuitry. The staff finds that the design does not permit testing of the ARI valve actuating relay and the ARI valve itself. This is not in conformance with the ARI system design guideline which only exempts the ARI valve testing while the plant is at power operation. During a conference call dated July 7, 1988, the licensee committed to modify the ARI system test scheme such that all the ARI system components are testable during normal plant operation. A bypass switch will be used during the on-line testing to minimize the inadvertent actuation. The bypass status is automatically and continuously indicated in the main control room. The licensee is required to document the modified design for staff audit. This is a confirmatory item.

4.11 INADVERTENT ACTION

The ARI design utilizes the "one-out-of-two" twice coincident logic. Both channels must be tripped in order to initiate the mitigative actions. The ARI actuation setpoints will not challenge scram setpoints. The staff finds this acceptable.

4.12 MANUAL INITIATION

The ARI system can be manually initiated from the control room. The staff finds this acceptable.

4.13 INFORMATION READOUT

ARI valve position indicating lights are provided on the ARI logic panel in the relay room as well as on panel 09-5 in the control room. An ARI test light and a scram header air pressure indicator are also located on panel 09-5 in the control room. There will be an annunciator to alert the operator that the ARI system has been initiated. The staff finds this acceptable.

4.14 COMPLETION OF PROTECTIVE ACTION ONCE IT IS INITIATED

Both the automatic and manual actuator signals for the ARI design will have a seal-in feature to ensure the completion of protective action once it is initiated. After removal of the initiating signal, this seal-in is required to be manually reset. The staff finds this acceptable.

4.15 CONCLUSION ON ARI SYSTEM

As stated in Reference 3, the staff SER on BWROG Topical Report NEDE-31096-P, the staff does not intend to repeat its review of the design information described in the BWROG Topical Report and found acceptable when the report appears as a reference in a specific license application. Reference 1 summarizes the licensee's compliance with the ATWS Rule. The staff finds that one area (e.g. diversity) of FitzPatrick ARI design is not in compliance with the ATWS Rule, 10 CFR 50.62, and as a result, the ARI system is not acceptable. This is discussed in more detail in section 4.4, of this evaluation. The licensee is required to document the design modification on ARI system test scheme as discussed in section 4.10 of this evaluation.

5.0 FITZPATRICK ATWS/RPT SYSTEM DESCRIPTION

The existing ATWS/RPT system uses a single trip coil to trip the 4.16 KV motor generator feeder breaker, thus opening the breaker for each recirculation system M-G set drive motor. Each recirculation system M-G set is tripped independently of the other M-G set. The trip logic is arranged in a "one-out-of-two" logic scheme. The trip signal is initiated by either one of two reactor vessel low water level or one of two reactor vessel high pressure. The ATWS/RPT system and the ARI system use the same transmitters, and trip units. These components are located in the ECCS cabinets.

6.0 EVALUATION OF ATWS/RPT SYSTEM

6.1 RECIRCULATING PUMP BREAKER RELIABILITY

During the staff's review of the Brunswick (Docket No. 50-324) ATWS/RPT system, the staff raised a concern that the Brunswick design has only one trip coil in a single breaker to trip the pump while the previously approved Monticello (Docket No. 50-263) design has redundant coils in a single breaker to trip the pump. The staff required the Brunswick licensee to demonstrate that their present RPT design can perform its function in a reliable manner equivalent to the Monticello design. Based on the failure rate calculation presented by the licensee, and an independent survey from Region I, the staff concluded that the reliability of the Brunswick RPT system is equivalent to the Monticello RPT system and therefore is acceptable. The main reason for accepting the Brunswick design is that Brunswick uses more reliable 4KV high-voltage breakers to trip the pumps and the trip initiation logic has been upgraded to satisfy the ATWS Rule guidelines.

The FitzPatrick design uses the same type of high-voltage breakers as Brunswick. Based on the reliability assessment presented by FitzPatrick submittal, the staff concludes that the recirculating pump breaker reliability concern is resolved. The single coil arrangement at FitzPatrick RPT design is acceptable.

6.2 RECIRCULATING PUMP TRIP INITIATION LOGIC

The FitzPatrick RPT initiation logic design uses a "one-out-of-two" logic scheme. The trip signal is initiated by either one of two reactor vessel low water level or one of two reactor vessel high pressure. The staff finds that the "one-out-of-two" logic scheme is not in conformance with ATWS Rule guideline in two aspects:

1. The ATWS Rule requires that the RPT shall be designed such that periodic surveillance tests can be performed during normal plant operation to provide assurance that the RPT logic and controls are capable of functioning as designed. The staff finds that the FitzPatrick RPT design does not satisfy this requirement.

2. The ATWS Rule guidance states that the design should be such that the frequency of inadvertent actuation and challenges to other safety systems is minimized. The staff finds that with a "one-out-of-two" trip scheme, the potential for inadvertent actuation is higher than the coincident logic scheme. In view of the recent LaSalle Unit 2 power oscillation event (NRC Bulletin No. 88-07), the inadvertent recirculation pump trip was the trigger event. The staff concluded that the "one-out-of-two" trip scheme is not a prudent design to minimize the inadvertent recirculation pump trip.

Most BWR ATWS/RPT trip systems are tripping both pumps using the same logic configuration. The FitzPatrick design the trips two pumps independently. The licensee should demonstrate that this arrangement still satisfies the objective of the ATWS mitigation function.

6.3 CONCLUSION ON ATWS/RPT SYSTEM

The staff finds that the FitzPatrick ATWS/RPT initiation logic design is not in conformance with the ATWS Rule, 10 CFR 50.62, and as a result, the ATWS/RPT system is not acceptable.

7.0 TECHNICAL SPECIFICATION MODIFICATION

The equipment required by the ATWS Rule to reduce the risk associated with an ATWS event must be designed to perform its function in a reliable manner. A method acceptable to the staff for demonstrating that the equipment satisfies the reliability requirements of the ATWS Rule is to provide equipment technical specifications including operability and surveillance requirements. Although the FitzPatrick plant technical specifications have incorporated the ATWS/RPT system, the operability and surveillance requirements have not been fully specified. It is expected that this issue will be addressed coincidently with the other outstanding non-conforming issues described herein.

8.0 REFERENCES

1. New York Power Authority letter John C. Brons to NRC Document Control Desk, dated April 15, 1987.

2. BWROG Topical Report NEDE-31096-P "Anticipated Transients Without Scram; Response to NRC ATWS Rule 10CFR50.62," dated December 1985.

3. Staff SER on BWROG Topical Report NEDE-31096-P. Letter from Gus Lainas (NRC) to Terry A. Pickens (BWR Owners' Group Chairman), dated October 21, 1986.

4. New York Power Authority letter John C. Brons to NRC Document Control Desk, dated October 11, 1985.

5. New York Power Authority letter John C. Brons to NRC Document Control Desk, dated June 10, 1988.

APPENDIX 1: THE STAFF POSISTION ON DIVERSITY REQUIREMENTS

The basic premise behind the ATWS rule as documented in SECY-83-293, "Amendments to 10 CFR 50 Related to Anticipated Transients Without Scram (ATWS) Events" is to require systems/equipment that are diverse (and independent) to those portions of the existing reactor trip system (RTS) where only minimal diversity is currently provided, and which are capable of preventing or mitigating the consequences of an ATWS event. An ATWS event is defined as 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 RTS to shutdown the reactor. The failure mechanism of concern is a common mode failure of identical components within the RTS (e.g., logic channels, actuation devices and instrument channels excluding sensors).

Common mode failures (CMFs) are failures of identical components due to the same failure mechanism (e.g., manufacturing defect, design defect, calibration or maintenance error). Common cause failures are a broader class of failures consisting of the failure of multiple components, not necessarily identical in design, due to the same cause, typically environmental in nature (e.g., extreme temperature, humidity induced corrosion, vibration). Although existing RTS are considered to have by design sufficient redundancy and testability features to prevent random failures from leading to system unavailability, because the redundant components are in general identical in manufacturer and design, they are subject to potential common mode failures. Existing reactor trip systems are typically located in controlled environments, and thus, the potential for many types of common cause failures is minimized. Common mode failures are a subset of common cause failures. Common mode failures, but not necessarily common cause failures, can be eliminated by providing total/absolute diversity. The diversity required by the ATWS rule is intended to ensure that common mode failures which disable the electrical portion of the existing reactor trip system will not affect the capability of systems/equipment installed in accordance with ATWS rule requirements (to prevent or mitigate the consequences of ATWS events) to perform their design functions. Therefore, the diversity required by the ATWS rule is hardware/component diversity (to prevent CMFs from disabling both the existing RTS and ATWS preventive/mitigative systems). It is recognized that total/absolute component/hardware diversity can be difficult and sometimes impossible to achieve. For these instances, acceptable level of component/hardware diversity can be achieved in accordance with combinations of allowable methods such as energication states, AC versus DC power, functional capability, and the use of components from different manufacturers.

The concept of equipment/hardware diversity has been firmly established and well documented throughout the history of the ATWS issude and rulemaking process. Appendix C (ATWS Equipment Requirements) to NUREG-0460, "Anticipated Transients Without Scram for Light Water Reactors," Volume 3 (published in December 1978) states that the equipment (installed to prevent/mitigate the consequences of ATWS events) shall be independent and separate from components for systems that initiate the anticipated transient(s) being analyzed and diverse from the normal scram system (postulated to fail) to minimze the probability of the ATWS disabling its operation.

ENCLOSURE

The supplementary information provided with the Federal Register notification of the ATWS rule includes guidance concerning the diversity required of diverse reactor trip systems (diverse scram systems) and mitigating systems from the existing reactor trip system. The guidance states that equipment diversity to minimize the potential for common cause failures is required from sensor output to and including the components used to interrupt control rod power (circuit breakers from different manufacturers alone is not sufficient to provide the required diversity for interruption of control rod power) for diverse scram systems, and from sensor output to, but not including, the final actuation device for mitigating systems (e.g., diverse turbine trip and diverse auxiliary feedwater actuation). Therefore, all diverse scram system and mitigating systems instrument channel components (excluding sensors and signal conditioning equipment upstream of the bistables) and logic channel components, and all diverse scram system actuation devices must be diverse from the existing RTS in accordance with the methods of achieving required equipment diversity identified above to obtain a level of diversity acceptable to satisfy the requirements of the ATWS rule. Identical components used in both the existing RTS and the diverse scram system or mitigating systems are subject to potential common mode failures, and therefore, are not acceptable.

ENCLOSURE