

ENCLOSURE 1

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

MILLSTONE NUCLEAR POWER STATION, UNIT 3

COMPLIANCE WITH ATWS RULE 10 CFR 50.62

DOCKET NO: 50-423

1.0 INTRODUCTION

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). The requirements of Section 10 CFR 50.62 apply to all commercial light-water-cooled nuclear power plants.

An ATWS is an anticipated operational occurrence (such as loss of feedwater, loss of condenser vacuum, or loss of offsite power) that 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 probability of failure to shut down the reactor following anticipated transients and to mitigate the consequences of an ATWS event.

Paragraph (c)(1) of 10 CFR 50.62 specifies the basic ATWS mitigation system requirements for Westinghouse plants. Equipment, diverse from the RTS, is required to initiate the auxiliary feedwater (AFW) system and a turbine trip for ATWS events. In response to paragraph (c)(1), the Westinghouse Owners Group (WOG) developed a set of conceptual ATWS mitigating system actuation circuitry (AMSAC) designs generic to Westinghouse plants. WOG issued Westinghouse Topical Report WCAP-10858, "AMSAC Generic Design Package," which provided information on the various Westinghouse designs.

The staff reviewed WCAP-10858 and issued a safety evaluation of the subject topical report on July 7, 1986 (Ref. 1). In this safety evaluation, the staff concluded that the generic designs presented in WCAP-10858 adequately meet the requirements of 10 CFR 50.62. The approved version of the WCAP is labeled WCAP-10858-P-A.

During the course of the staff's review of the proposed AMSAC design, the WOG issued Addendum 1 to WCAP-10858-P-A by letter dated February 26, 1987 (Ref. 2). This Addendum changed the setpoint of the C-20 AMSAC permissive signal from 70% reactor power to 40% power. On August 3, 1987, the WOG issued Revision 1 to WCAP-10858-P-A (Ref. 3), which incorporated Addendum 1 changes and provided details on changes associated with a new variable timer and the C-20 time delay. For those plants selecting either the feedwater flow or the feedwater pump/valve status logic options, a variable delay timer is to be incorporated into the AMSAC actuation logics. The variable time delay will be inverse to reactor power and will approximate the time that the steam generator takes to boil down to the low-low level setpoint upon a loss of main feedwater (MFW) from any given reactor power level between 40% and 100% power. The time delay on the C-20 permissive signal for all logics will be lengthened to incorporate the maximum time that the steam generator takes to boil down to the low-low level setpoint upon a loss of MFW with the reactor operating at 40% power. The staff considers the Revision 1 changes to be acceptable.

Paragraph (c)(6) of the ATWS Rule requires that detailed information to demonstrate compliance with the requirements be submitted to the Director, Office of Nuclear Reactor Regulation (NRR). In accordance with paragraph (c)(6) of the ATWS Rule, Northeast Nuclear Energy Company (NNECO) (licensee) provided information by letter dated April 20, 1988 (Ref. 4). The letter forwarded the detailed design description of the ATWS mitigating system actuation circuitry proposed for installation at the Millstone Nuclear Power Station, Unit 3.

The staff held several conference calls with the licensee during June, July and August of 1988 to discuss their AMSAC design. As a result of the conference calls, the licensee responded to the staff concerns by letters dated July 14, 1988 (Ref. 5), July 26, 1988 (Ref. 6), and August 12, 1988 (Ref. 7).

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, the equipment required by the ATWS Rule should be of sufficient quality

and reliability to perform its intended function while minimizing the potential for transients that may challenge the safety systems, e.g., inadvertent scrams.

The following review criteria were used to evaluate the licensee's submittals:

1. The ATWS Rule, 10 CFR 50.62.
2. "Considerations Regarding Systems and Equipment Criteria," published in the Federal Register, Volume 49, No. 124, dated June 26, 1984.
3. Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That is Not Safety Related."
4. Safety Evaluation of WCAP-10858 (Ref. 1).
5. WCAP-10858-P-A, Revision 1 (Ref. 3).

3.0 DISCUSSION AND EVALUATION

To determine that conditions indicative of an ATWS event are present, the licensee has elected to implement the WCAP-10858-P-A AMSAC design associated with monitoring the steam generator water level and activating the AMSAC when the water level is below the low-low setpoint. Also, the licensee will implement the new time delay (as described in the introduction section) associated with the C-20 permissive consistent with the requirements of Revision 1 to the WCAP.

Many details and interfaces associated with the implementation of the final AMSAC design are of a plant-specific nature. In its safety evaluation of WCAP-10858, the staff identified 14 key elements that require resolution for each plant design. The following paragraphs provide a discussion on the licensee's compliance with respect to each of the plant-specific elements.

1. Diversity

The plant design should include adequate diversity between the AMSAC equipment and the existing Reactor Protection System (RPS) equipment. Reasonable equipment diversity, to the extent practicable, is required to minimize the potential for common-cause failures.

The licensee has provided information to confirm that the microprocessor-based AMSAC logic circuits will be diverse from the logic circuits of the RPS in the areas of design, equipment, and manufacturing. This is a Westinghouse microprocessor designed AMSAC system that has had a verification and validation process performed on the software. Where similar types of components are used, such as relays, the AMSAC will utilize a relay of a different make and manufacturer.

2. Logic Power Supplies

Logic power supplies need not be Class 1E, but must be capable of performing the required design functions upon a loss of offsite power. The logic power must come from a power source that is independent from the ROS power supplies.

The licensee has provided information verifying that the logic power supplies selected for the Millstone 3 AMSAC logic circuits will be independent from the RPS power supplies. The AMSAC will be powered by an independent inverter which is backed by a battery that is totally independent from the battery supply for the RPS and capable of operating upon a loss of offsite power.

3. Safety-Related Interface

The implementation of the ATWS Rule shall be such that the existing RPS continues to meet all applicable safety criteria.

The proposed Millstone 3 AMSAC design interfaces at its input with the existing Class 1E circuits of the steam generator narrow range water level instrumentation and turbine impulse chamber pressure instrumentation. At its output, the AMSAC will interface with the Class 1E circuits of the AFW pumps. Connections with the AFW control circuits will be made downstream of approved Class 1E isolation devices. The licensee has confirmed to the staff that the existing safety-related criteria that are in effect at Millstone 3, as described in its FSAR Sections 7.1.2 and 7.2, will continue to be met after the implementation of AMSAC (i.e., the RPS will continue to perform its safety functions without interference from AMSAC). Refer to Item 9 for further discussion on this issue.

4. Quality Assurance

The licensee is required to provide information regarding compliance with Generic Letter (GL) 85-06, "Quality Assurance for ATWS Equipment That is Not Safety Related."

The criteria of the NRC quality assurance guidance (GL 85-06) were reviewed by the licensee. The licensee stated that quality assurance practices at Millstone 3, as applicable to nonsafety-related AMSAC equipment, comply with the guidance of GL 85-06.

5. Maintenance Bypasses

Information showing how maintenance at power is accomplished should be provided. Also, maintenance bypass indications should be incorporated into the continuous indication of bypass status in the control room.

The licensee provided information showing how maintenance is to be accomplished at power. The staff was informed that maintenance at power will be performed by inhibiting the operation of AMSAC's output relays, which will block the output signal and, thus, prevent it from reaching the final actuation devices. The continuous indication of bypass status will be provided in the main control board.

6. Operating Bypasses

The operating bypasses should be indicated continuously in the control room. The independence of the C-20 permissive signal should be addressed.

The licensee has provided information stating that the AMSAC operating bypass (C-20) will be used to enable the operators to bring the plant up in power during startup and to avoid spurious AMSAC actuations at power levels below 40% reactor power (the C-20 arming setpoint). Above 40% reactor power, the C-20 will automatically arm the AMSAC logics. The C-20 permissive signal will originate from existing turbine impulse chamber pressure sensors. Upon a turbine trip (loss of the Load ATWS), the C-20 permissive signal will be maintained by a timer for a period of 260 seconds. This setpoint is based on the results of plant-specific analysis, and it has been determined by the licensee that this time delay will be sufficient to ensure that AMSAC will perform its function. The C-20 permissive signal will be taken downstream from qualified isolators and thus, will not interfere with the RPC. The operating bypass will be indicated continuously in the control room via annunciation and will be consistent with the existing bypass design philosophy used in the control room.

7. Means for Bypasses

The means for bypassing shall be accomplished by using a permanently installed, human-factored, bypass switch or similar device. Disallowed methods for bypassing mentioned in the guidance should not be utilized.

The licensee stated that a permanently installed control switch will be used for the bypass function. The disallowed methods for bypassing, such as lifting leads, pulling fuses, blocking relays, or tripping breakers will not be used.

8. Manual Initiation

Manual initiation capability of the AMSAC mitigation function at the system level must be provided.

In the plant-specific submittal, the licensee discussed how manual turbine trip and auxiliary feedwater actuation are accomplished by the operator. In summary, the operator can use existing manual controls to perform a turbine trip and to start auxiliary feedwater flow should it be necessary. Thus, no additional manual initiation capability will be required as a result of installing the AMSAC equipment.

9. Electrical Independence From Existing Reactor Protection System

Independence is required from the sensor output to the final actuation device, at which point nonsafety-related circuits must be isolated from safety-related circuits by qualified Class 1E isolators.

The licensee discussed how electrical independence is to be achieved. The proposed design requires isolation between the non-Class 1E AMSAC and the Class 1E circuits associated with the steam generator (SG) level, the turbine impulse chamber pressure signals, and the AFW pumps. The licensee has informed the staff that the required isolation will be achieved using electrical isolation devices that have been qualified and tested to Class 1E electrical equipment requirements. In addition, the isolators were tested as described in Appendix A to the Safety Evaluation (Ref. 1). The test values of voltage and current used in the testing of the isolators encompass the circuit values of voltage and current presently existing in the Millstone 3 AMSAC circuits.

10. Physical Separation From Existing Reactor Protection System

The implementation of the ATWS mitigating system must be such that the separation criteria applied to the existing RPS are not violated.

The licensee stated that the AMSAC circuitry will be physically separated from the RPS circuitry. The licensee has further stated that the cable routing will be independent of protection system cable routing and that the ATWS equipment cabinets will be located so that there will be no interaction with the protection system cabinets. Separation of the Train A, B,

and non-Class 1E circuits within the AMSAC cabinet is to be achieved through a combination of metal barriers, conduit, and distance. The existing separation criteria associated with the RPS will not be compromised as a result of the AMSAC installation and implementation.

11. Environmental Qualification

The plant-specific submittal should address the environmental qualification of ATWS equipment for anticipated operational occurrences.

The licensee stated that AMSAC mitigation equipment will be located in areas of the plant that are considered to be a mild environment. The licensee also stated that the equipment will be designed to perform its function during anticipated operational occurrences that might occur associated with the respective equipment locations.

12. Testability at Power

Measures to test the ATWS mitigation system before installation, as well as periodically, are to be established. Testing of the system may be performed with the system in the bypass mode. Testing from the input sensor through the final actuation device should be performed with the plant shut down.

The licensee stated that a complete end-to-end test of the AMSAC system, including the AMSAC outputs through the final actuation devices, will be performed during each refueling outage. With the plant at power, the system will be tested with the AMSAC output actuation devices bypassed. The testing capability consists of a series of overlapping tests. These tests will verify analog channel accuracy, setpoint (bistable trip) accuracy, and coincidence logic operation including operation and accuracy of all timers. The at-power logic tests will be performed on a quarterly basis.

The bypass of the AMSAC output actuation devices will be accomplished through a permanently installed bypass switch which negates the need to

lift leads, pull fuses, trip breakers, or physically block relays. Status outputs to the plant computer and main control board, indicating that a general warning condition exists with AMSAC, will be initiated when the system's outputs are bypassed. Plant procedures will be used to test the AMSAC circuitry and outputs. These procedures will ensure that AMSAC is returned to service when testing is complete.

13. Completion of Mitigative Action

The licensee is required to verify that (1) the protective action, once initiated, goes to completion and (2) the subsequent return to operation requires deliberate operator action.

The licensee responded that the system design will be such that AMSAC is consistent with the circuitry of the auxiliary feedwater and turbine trip control systems. Once initiated, the design will ensure that protective action goes to completion. Following completion of the mitigative action, deliberate operator action will then be required to return the actuated devices to normal operation.

14. Technical Specifications

The plant-specific submittal should address technical specification requirements for AMSAC.

The licensee responded that no technical specification action is proposed with respect to the AMSAC. The licensee stated that the system does not meet NRC criteria for inclusion in the technical specifications. The surveillance interval and actions required to service the AMSAC will be administratively controlled using station procedures.

The equipment required by the ATWS Rule to reduce the risk associated with an ATWS event must be designed to perform its functions 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 limiting conditions for operation and surveillance requirements in the technical specifications.

In its Interim Commission Policy Statement of Technical Specification Improvements for Nuclear Power Plants [52 Federal Register 3788, February 6, 1987], the Commission established a specific set of objective criteria for determining which regulatory requirements and operating restrictions should be included in technical specifications. The staff is currently reviewing ATWS requirements to criteria in this Policy Statement to determine whether and to what extent technical specifications are appropriate. Accordingly, this aspect of the staff review remains open pending completion of, and subject to the results of, the staff's further review. The staff will provide guidance regarding the technical specification requirements for AMSAC at a later date.

4.0 HUMAN-FACTORS REVIEW

The licensee has indicated (Ref. 8) that the following design elements have been addressed in the conduct of a human-factors review:

- Maintenance bypass status (See Item 5 of Section 3.0).
- Operating bypass status (See Item 6 of Section 3.0).
- Bypass switch (See Item 7 of Section 3.0).
- Controls and indications for testing (See Item 12 of Section 3.0).

NNECO has reviewed the AMSAC design modification including maintenance bypass, operating bypass and testability at power features and the means for bypass (the bypass switch) against the criteria of NUREG-0700 and standards established during the performance of the Millstone Unit No. 3 control room design review and found the modification to be in compliance with the criteria and standards.

This review determined that this modification provides the operators with the information and control interface necessary. As such, the system modification reflects good human engineering practices.

5.0 CONCLUSION

The staff concludes, based on the above discussion and subject to final resolution of the technical specification issue, that the AMSAC design proposed by Northeast Nuclear Energy Company for the Millstone Nuclear Power Station, Unit 3, is acceptable and is in compliance with the ATWS Rule, 10 CFR 50.62, paragraph (c)(1).

Until staff review is completed regarding the use of technical specifications for ATWS requirements, the licensee should continue with the scheduled installation and implementation (planned operation) of the ATWS design utilizing administratively controlled procedures.

6.0 REFERENCES

1. Letter, C. E. Rossi (NRC) to L. D. Butterfield (WOG), "Acceptance for Referencing of Licensing Topical Report," July 7, 1986.
2. Letter, R. A. Newton (WOG) to J. Lyons (NRC), "Westinghouse Owners' Group Addendum 1 to WCAP-10858-P-A and WCAP-11233-A: AMSAC Generic Design Package," February 26, 1987.
3. Letter, R. A. Newton (WOG) to J. Lyons (NRC), "Westinghouse Owners' Group Transmittal of Topical Report, WCAP-10858-P-A, Revision 1, AMSAC Generic Design Package," August 3, 1987.
4. Letter, E. J. Mroczka/C. F. Sears (NNECO) to U.S. NRC, "ATWS Rule - Plant Specific Information - ATWS Mitigation System Actuation Circuitry (AMSAC) Design," April 20, 1988.

5. Letter, E. J. Mroczka/W. D. Romberg (NNECO) to U.S. NRC, "ATWS Rule - Plant Specific Information - ATWS Mitigation System Actuation Circuitry (AMSAC) Design," July 14, 1988.
6. Letter, E. J. Mroczka (NNECO) to U.S. NRC, "ATWS Rule - Plant Specific Information - ATWS Mitigation System Actuation Circuitry (AMSAC) Design," July 26, 1988.
7. Letter, E. J. Mroczka/J. F. Opeka (NNECO) to U.S. NRC, "ATWS Rule - Plant Specific Information - ATWS Mitigation System Actuation Circuitry (AMSAC) Design," August 12, 1988.
8. Letter, E. J. Mroczka (NNECO) to U.S. NRC, "Millstone Nuclear Power Station, Unit No. 3, ATWS Rule - Plant Specific Information," June 30, 1989.

Principal Contributors: L. Tran
D. Jaffe

Dated: July 17, 1989