



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

SAFETY EVALUATION REPORT

SAN ONOFRE NUCLEAR GENERATING STATION, UNIT NOS. 2 AND 3

EVALUATION OF COMPLIANCE WITH THE ATWS RULE 10 CFR 50.62

REQUIREMENTS FOR REDUCTION OF RISK

FROM ANTICIPATED TRANSIENTS WITHOUT SCRAM (ATWS) EVENTS

FOR LIGHT-WATER-COOLED NUCLEAR POWER PLANTS

DOCKET NOS. 50-361, 50-362

1.0 INTRODUCTION

On July 26, 1984, the Code of Federal Regulations (CFR) was amended to include the "ATWS Rule" (Section 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants"). 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.

The 10 CFR 50.62 requirements applicable to pressurized water reactors manufactured by Combustion Engineering, such as San Onofre Nuclear Generating Station, Unit Nos. 2 and 3 (SONGS-2 and 3) are:

- (1) Each pressurized water reactor must have equipment from sensor output to final actuation device that is diverse from the reactor trip system, which will 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.
- (2) Each pressurized water reactor must have a diverse scram system from the sensor output to interruption of power to the control rods. This scram 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 interruption of power to the control rods).

9002050028 900130
PDR ADDCK 05000361
P PDC

In summary, the ATWS Rule requirements for SONGS-2 and 3 are to install a diverse scram system (DSS), diverse circuitry to initiate a turbine trip (DTT) and diverse circuitry for initiation of emergency feedwater (DEFAS).

2.0 BACKGROUND

Paragraph (c)(6) of the ATWS Rule requires that detailed information to demonstrate compliance with the requirements of the Rule be submitted to the Director, Office of Nuclear Reactor Regulation (NRR). In accordance with Paragraph (c)(6) of the ATWS Rule, the Combustion Engineering Owners Group (CEOG) provided information to the staff by letter dated September 18, 1985 (Ref. 1). The letter forwarded CEN-315, "Summary of the Diversity Between the Reactor Trip System and the Auxiliary Feedwater Actuation System (AFAS) for CE Plants," for staff review.

The staff reviewed CEN-315 and, by letter dated August 4, 1986 (Ref. 2), forwarded its conclusion to the CEOG. The staff concluded that sufficient diversity did not exist between the reactor trip system and the auxiliary feedwater actuation system to achieve the degree of reduction in potential common mode failure (CMF) mechanisms by providing hardware diversity as required by the ATWS Rule. This decision affected San Onofre Nuclear Generating Station, Units 2 and 3 (SONGS-2 and 3), Arkansas Nuclear One, Unit 2 (ANO-2), and Waterford Steam Electric Station, Unit 3 (WSEC-3).

In response to the staff's evaluation of CEN-315, Southern California Edison (SCE), the licensee for SONGS-2 and 3, submitted CEN-349 to the staff by letter dated December 30, 1986 (Ref. 3). CEN-349 provided additional information to support the CEOG position stated in CEN-315. The staff reviewed CEN-349 and, by letter dated January 11, 1988 (Ref. 4), again rejected the CEOG position that the existing diversity between the RTS and the AFAS meets the requirements of the ATWS Rule.

In a further attempt to gain a favorable staff position, SCE by letter dated December 29, 1988 (Ref. 5), submitted a plant-specific request for an exemption from the portion of the ATWS Rule that requires equipment diverse from the RTS to initiate the AFAS under conditions indicative of an ATWS. The submittal also provided detailed design information on the DSS and the DTT.

Prior to the Reference 5 submittal, the staff forwarded to the licensee by letter dated August 25, 1988 (Ref. 6) a request of additional information (RAI) based on a submittal of June 6, 1986 (Ref. 7). The Reference 7 submittal addressed the DSS and the DTT. The licensee responded to the RAI by letter dated November 22, 1988 (Ref. 8).

On May 1, 1989, a meeting was held between the staff, the CEOG, and SCE representatives in which the November 22, 1988 submittal was discussed. During the discussion the staff requested additional information concerning the design details of the DTT. The licensee supplied the requested information by letter dated November 2, 1989 (Ref. 9).

This safety evaluation addresses the licensee's conformance with the ATWS Rule at SONGS-2 and 3 with respect to the DSS and the DTT. With respect to the DEFAS, the SCE plans to submit additional plant specific design information to demonstrate the conformance to the ATWS rule requirements. The staff's evaluation of the proposed DEFAS will be addressed in a separate document.

3.0 CRITERIA

The purpose of the ATWS Rule, as documented in SECY-83-293, "Amendments to 10 CFR 50 Related to Anticipated Transients Without Scram Events," is to require equipment/systems that are diverse from the existing reactor trip system and capable of preventing or mitigating the consequences of an ATWS event. The failure mechanism of concern is a common mode failure of identical components within the RTS (e.g., logic circuits; actuation devices; and instrument channel components, excluding sensors).

The hardware/component diversity required by the ATWS Rule is intended to ensure that CMFs that could disable the electrical portion of the existing reactor trip system will not affect the capability of ATWS mitigation system(s) equipment to perform its design functions. Therefore, the similarities and differences in the physical and operational characteristics of these components must be analyzed to determine the potential for CMF mechanisms that could disable both the RTS and ATWS mitigation functions.

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 to 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." The criteria used in evaluating the licensee's submittal include 10 CFR 50.62, "Rule Considerations Regarding Systems and Equipment Criteria," published in the Federal Register, Volume 49, No. 124, dated June 26, 1984. Generic Letter No. 85-06, dated April 16, 1985, "Quality Assurance Guidance for ATWS Equipment That is Not Safety Related," details the quality assurance requirements applicable to the equipment installed per ATWS Rule requirements.

To minimize the potential for common mode failures, diversity is required for diverse scram system equipment from sensor output to, and including, the components used to interrupt control rod power. The use of circuit breakers from different manufacturers is not, by itself, sufficient to provide the required diversity for interruption of control rod power.

For mitigating systems (i.e., diverse turbine trip and diverse auxiliary feedwater actuation system), diversity is required from sensor output to, but not including, the final actuation device.

Electrical independence between ATWS mitigation circuits (i.e., DSS, DTT, and DEFAS) and the existing RTS circuits is considered desirable to prevent interconnections between systems that could provide a means for CMFs to potentially affect both systems. Where electrical independence is not provided between RTS circuits and circuits installed to mitigate ATWS events, it must be demonstrated that faults within the DSS, DTT, or the DEFAS cannot degrade the reliability/integrity of the existing RTS below an acceptable level. It must also be demonstrated that a CMF affecting the RTS power distribution system, including degraded voltage and frequency conditions (the effects of degraded voltage conditions over time must be considered if such conditions can go undetected), cannot compromise both the RTS and ATWS mitigation functions.

Electrical independence of nonsafety-related ATWS mitigation circuits from safety-related circuits is required in accordance with the guidance provided in IEEE Standard 384, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," as supplemented by Regulatory Guide (RG) 1.75, Revision 2, "Physical Independence of Electric Systems."

The equipment required by 10 CFR 50.62 to reduce the risk associated with an ATWS event must be designed to perform its functions in a reliable manner. The DSS, DTT, and DEFAS circuits must be designed to allow periodic testing to verify operability while at power. Compliance with the reliability and testability requirements of the ATWS Rule must be ensured by technical specification operability and surveillance requirements or equivalent means that govern the availability and operation of ATWS equipment; thereby ensuring that the necessary reliability of the equipment is maintained.

The ATWS mitigation systems should be designed to provide the operator with accurate, complete, and timely information that is pertinent to system status. Displays and controls should be properly integrated into the main control room and should conform to good human-engineering practices in design and layout.

4.0 DISCUSSION AND EVALUATION

The following is a discussion on the licensee's compliance to the guidance contained in the Federal Register, "Statement of Considerations" and to the requirements of the ATWS Rule as discussed in Section 3 of this report.

4.1 DIVERSE SCRAM SYSTEM

A. GENERAL

SCE intends to implement the SONGS-2 and 3 Diverse Scram System (DSS) design as a control-grade system by using new pressurizer pressure transmitters on existing taps to provide signals to the DSS in a two-out-of-four energize to trip logic. High pressurizer pressure will be used as the

parameter indicative of an ATWS. The DSS will consist of four measurement channels, four two-out-of-four logics, and two trip paths. Each measurement channel consists of a pressure transmitter sensor; a signal conditioner; and an alarm block and timer block, which are part of the configured function block of a Foxboro Spec. 200 Micro Control Module.

The DSS trip setpoint will be set greater than the reactor protection system (RPS) high pressurizer pressure trip setpoint and less than the primary safety valve relief pressure setpoint. Each of the two-out-of-four logics activates one of the two trip paths to open a motor-generator (MG) set output contactor. This occurs when any two of the four measurement channels reach the high-high pressurizer pressure setpoint simultaneously.

Activation of the logic channel 1 or 3 of the two-out-of-four logic energizes the Trip Path #1 relay, which opens the MG Set #1 output contactor. Activation of the logic channel 2 or 4 of the two-out-of-four logic energizes the Trip Path #2 relay, which opens the MG Set #2 output contactor. Activation of both trip paths is required to initiate a reactor trip. Once the trip is actuated, it is sealed until manually reset at the DSS panel.

B. DIVERSITY

Hardware/component diversity is required for all diverse scram system equipment from sensor outputs to, and including, the components used to interrupt control rod power. The use of circuit breakers from different manufacturers is not, by itself, sufficient to provide the required diversity for interruption of control rod power. The DSS sensors are not required to be diverse from the RTS sensors. However, separate sensors are preferred to prevent interconnections between the DSS and the existing reactor protection system.

The SONGS-2 and 3 DSS design consists of four safety-related instrument channels, each of which provides an input to two separate two-out-of-four energize-to-actuate logic matrices. The output of each logic is used to open one of the two RTS motor-generator (MG) set output contactors. Both contactors must open to remove power from the control element assemblies (CEA), causing a reactor scram. The instrument channels consist of sensors, bistables, bistable relays, and actuation relays.

The sensors used in the DSS are separate from the existing RTS pressure transmitters. They do, however, share existing pressure sensing lines through instrument valves. The DSS transmitter circuits are completely independent from the existing RTS instrument loops. Additionally, the DSS transmitters are qualified for Class 1E application, and are Seismic Category I in design. This sensor design exceeds the requirements of the ATWS Rule.

The SONGS-2 and 3 DSS design does not specifically use bistables or bistable relays in its design. The functions of these units are performed by the Foxboro Spec. 200 Micro Control Module. For this function, the RTS uses bistables and bistable relays manufactured by Electro-Mechanics. For

actuation devices, the DSS uses Foxboro output relay modules, GE control relays, and MG set trip relays, which open the M-G set output load contactors. The actuation devices are powered from a non-Class 1E instrument AC-power panel. The parallel devices in the RTS are Teledyne solid state relays and mechanical circuit breakers powered by a Class 1E vital bus.

Based on the above, the staff concludes that the level of hardware/component diversity provided between the DSS circuits and the existing RTS circuits is sufficient to comply with the requirements of 10 CFR 50.62 (the ATWS Rule) and is, therefore, acceptable.

C. DSS ELECTRICAL INDEPENDENCE/POWER SUPPLIES

The purpose of the electrical independence requirements of the ATWS Rule is to prevent interconnections between the DSS and RTS (thereby reducing the potential for CMFs that could affect both systems) and to ensure that faults within DSS circuits cannot degrade the RTS. Electrical independence of DSS circuits from RTS circuits should be maintained from sensor outputs up to the final actuation devices. The use of a common power source for the DSS and RTS sensors is acceptable because, in accordance with the ATWS Rule, the sensors can be shared between these two systems.

The DSS receives power from two 100 percent capacity, non-Class 1E uninterruptable power supplies which are operable upon the loss of off-site power. The logic power is supplied by four Foxboro power supplies. The power supplies for logic channels 1 and 2 operate in parallel as do the power supplies for logic channels 3 and 4. Dual power supplies, manufactured by Computer Products, Inc. (CPI), supply power to the multiplexer. The RTS power source is a Power Mate 12 VDC power supply that takes its power from the Class 1E AC vital bus. In addition to power supply diversity and independence, electrical separation is also maintained; therefore, the proposed design does not need or use electrical isolation devices.

Based on the above, the staff concludes that the DSS power supply configuration is acceptable, as it minimizes the potential for CMFs and other faults to degrade both the DSS and RTS.

D. DSS RELIABILITY/TESTABILITY/MAINTENANCE

To ensure that the DSS circuits perform their safety functions when called on, the Commission issued Generic Letter (GL) 85-06 "Quality Assurance Guidance for ATWS Equipment that is not Safety Related," which details the quality assurance requires for equipment installed per ATWS Rule requirements. In addition, the staff requires that circuits be maintained and periodically tested at power in accordance with technical specifications operability and surveillance requirements or equivalent means.

The licensee has stated that a Quality Class III/ATWS will be incorporated into the SONGS-2 and 3 updated FSAR. This quality class will be controlled in accordance with NRC Generic Letter 85-06. After completion of the DSS installation, the system will be given prerequisite and preoperational tests prior to placing the DSS into service.

The proposed DSS surveillance testing program will call for a channel check once per day, a functional test performed at 92 day intervals, and at each refueling outage a channel calibration and a functional test will be performed. All DSS associated alarms will be tested. A trip test will be performed at refueling outage in which the CEDM MG contactors will be tripped. This test will be the only time that two jumpers will have to be installed at terminal strip test points specifically for the purpose of conducting the end-to-end DSS testing. The staff will audit the test procedure during the site inspection to ensure that an administrative control for jumper usage is properly addressed.

The licensee confirmed that the bypass features for maintenance and testing will be built in and will be part of the circuits. Temporary modifications of the circuits for testing and maintenance will not be required except as noted above. When a protection action is activated, or when any part of the DSS is placed in a bypass condition, an alarm annunciator is actuated in the main control room.

Based on the above, the staff concludes that the DSS surveillance testing proposed by the licensee, the means used to bypass the DSS for test and maintenance purposes, and the indication of the bypass condition are in accordance with good design practices and the requirements of 10 CFR 50.62 (the ATWS Rule) and are, therefore, acceptable.

E. OTHER DSS CONSIDERATIONS

Other system design considerations that enhance the DSS at include:

1. The energize-to-trip circuits will be used to exclude the activation of a trip by component failure.
2. The DSS equipment will be qualified for the environment in which it will be installed.
3. The DSS will have provisions for manual initiation of the system.
4. Once initiated, the DSS will seal-in and require deliberate manual operator action to reset the system.
5. The DSS alarms will be consistent with the plant's Control Room Design Review and good human-engineering practices. The control room annunciator will have one annunciator window for the ATWS/DSS labeled "ATWS/DSS TROUBLE." This alarm will alert the operator to observe the display on the Critical Functions Monitoring System (CFMS). The CFMS will display the DSS status such as trip, test, bypass, and system failure. The DSS status will also be indicated on the test panel mimic board.

F. CONCLUSION

Based on the above evaluation, the staff concludes that the proposed design of the Diverse Scram System for the San Onofre Nuclear Generating Station, Units 2 and 3, conforms to the requirements of 10 CFR 50.62 (the ATWS Rule) and is, therefore acceptable.

4.2 DIVERSE TURBINE TRIP

A. GENERAL

The Diverse Turbine Trip (DTT) design for consists of four, control-grade instrument channels that sense control element drive mechanism (CEDM) power bus undervoltage in a selective two-out-of-four logic. When the DSS causes a reactor scram, power is interrupted to the CEDM coils upstream of the rod power bus undervoltage relays. The de-energizing of these undervoltage relays actuates the diverse turbine trip circuitry.

The DTT design shares all circuit components with the DSS up to, but not including, the final turbine trip device. Those components that are unique to the DTT (i.e., undervoltage relays, trip relays, master trip relays, and the master solenoid) do not appear in any of the RTS trip paths. All of the information that is applicable to the DSS components and system, as discussed in Section 4.1 of this report, is also applicable to DTT components up to, but not including, the final trip device.

B. CONCLUSION

Based on the above evaluation, the staff concludes that the proposed design for the Diverse Turbine Trip for SONGS-2 and 3 conforms to the requirements of 10 CFR 50.62 (the ATWS Rule) and is, therefore, acceptable.

4.3 DIVERSE EMERGENCY FEEDWATER ACTUATION SYSTEM

As discussed in Section 2.0 of this report, the Auxiliary (or Emergency) Feedwater Actuation System at SONGS-2 and 3 was the subject of a Request for Exemption (RFE) from the ATWS Rule (Ref. 5). The staff has reviewed the RFE and has held several meetings with the CE Owners group. As a result of these meetings, the SCE plans to submit additional plant specific design information with respect to the diverse auxiliary feedwater actuation system to meet the ATWS Rule. The staff's evaluation of the proposed DEFAS will be addressed in a separate document.

The licensee should continue implementing the diverse DEFAS. The staff recommends that the design documentation associated with the diverse DEFAS design be provided to the staff for review as soon as it is available. However, verification of the final compliance of the DEFAS with the ATWS Rule will be determined by a post-implementation inspection at SONGS-2 and 3.

5.0 TECHNICAL SPECIFICATION REQUIREMENTS

The staff is presently evaluating the need for technical specification operability and surveillance requirements, including actions considered appropriate when operability requirements cannot be met (i.e., limiting conditions for operation) to ensure that equipment installed per the ATWS Rule will be maintained in a operable condition. In its Interim Commission Policy Statement on Technical Specification Improvements for Nuclear Power Plants [52 Federal Register 3778, 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 will provide guidance regarding the Technical Specification requirements for DSS, DTT, and DAFAS at a later date. Installation of ATWS mitigation system equipment should not be delayed pending the development or staff approval of operability and surveillance requirements for ATWS equipment.

6.0 REFERENCES

1. Letter, R. G. Wells (CEOG) to F. Rosa (NRC), "CEN-315 Summary of the Diversity Between the Emergency Feedwater Actuation System for C-E Plants," September 18, 1985.
2. Letter, D. M. Crutchfield (NRC) to R. W. Wells (CEOG), "Staff Evaluation of CEN-315," August 4, 1986.
3. Letter, M. O. Medford (SCE) to G. W. Knighton (NRC), "San Onofre Nuclear Generating Station, Units 2 and 3 (Submittal of CEN-349)," December 30, 1986.
4. Letter, G. W. Knighton (NRC) to K. P. Baskin (SCE) and J. C. Holcombe (SDG&E), "NRC Evaluation of CEN-315 and CEN-349," January 11, 1988.
5. Letter, L. T. Papay (SCE) to USNRC, "Docket Nos. 50-361 and 50-362, ATWS Rule (10 CFR 50.62) Exemption Request, San Onofre Nuclear Generating Station Units 2 and 3, TAC Numbers 59139 and 59140," December 29, 1988.
6. Letter, D. E. Hickman (NRC) to K. P. Baskin (SCE) and G. D. Cotton (SDG&E), "10 CFR 50.62 (ATWS Rule) Request for Additional Information (TAC Numbers 59139 and 59140)," August 25, 1988.
7. Letter, M. O. Medford (SCE) to G. W. Knighton (NRC), Docket Nos. 50-361 and 50-362, San Onofre Nuclear Generating Station Units 2 and 3," June 6, 1986.
8. Letter, M. O. Medford (SCE) to USNRC, "Docket Nos. 50-361 and 362, San Onofre Nuclear Generating Station Units 2 and 3," November 22, 1988.
9. Letter, F. R. Nandy (SCE) to USNRC, "Docket Nos. 50-361 and 50-362, ATWS Rule TAC Nos. 59139/40, San Onofre Nuclear Generating Station, Units 2 and 3," November 2, 1989.

Principle Contributor: Hulbert Li

Date: December 7, 1989