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

ENCLOSURE 2

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

REVIEW OF THE LOAD SEQUENCERS SAFEGUARDS IN THE

STATION BLACKOUT/ELECTRICAL SAFEGUARDS UPGRADE PROFECT

NORTHERN STATES POWER COMPANY

PRAIRIE ISLAND NUCLEAR GENERATING PLANT, UNIT NOS. 1 AND 2

FACILITY OPEARTING LICENSE NOS. DPR-42 AND DPR-60

DOCKET NOS. 50-282 AND 50-306

1.0 INTRODUCTION

By letters dated November 27, 1990, July 10, 1991, Northern States Power Company (NSP) submitted descriptions of proposed upgrades to the Prairie Island Nuclear Generating Plant, Units 1 & 2 Station Blackout/Electrical Safeguards (SBO/ESS) (References 1 and 3). The Instrumentation and Control Systems Branch (SICB) reviewed the use of programmable logic controllers (PLCs) in the SBO/ESS load sequencers.

To enhance the SBO/ESS, NSP proposed the addition of two emergency diesel generators (EDGs) to Prairie Island's existing station emergency power supplies, which presently consists of two EDGs shared between Units 1 and 2.

The SBO/ESS enhancement includes the installation of two new computer-based load sequencers, one for each of the Class 1E electrical buses for Unit 2. The load sequencers utilize Allen-Bradley commercial grade PLCs to execute the control functions and provide continuous monitoring of the load sequencers.

The use of commercial grade PLCs and the use of software for emergency applications requires assurance that these PLCs are qualified as Class 1E and will provide for the safe operation of the plant. The SICB staff reviewed the licensee's documentation (Reference 1) and requested additional information (RAI) to clarify several design details (Reference 2). The following evaluation is based upon the licensee's initial submittal and their response to the RAI (References 3).

2.0 EVALUATION

The load sequencer system for Unit 2 consists of redundant trains of load sequencers, each train dedicated to an Emergency Diesel Generator (EDG). A cross-tie connects the emergency power supplies in the two nuclear plants to ensure availability of an EDG during a loss of offsite power (LOOP) in one unit. Additionally, the licensee has provided battery back-up capabilities and manual access to the load sequencers. This degree of redundancy and diversity is acceptable.

A new load sequencing system is to be installed in the Unit 2 upgrade. Spectrum Technologies, Inc. (STI), a subcontractor to the SBO/ESS prime contractor, Fluor Daniel, is developing the software for the Unit 2 load sequencer. The STI load sequencer Verification and Validation (V&V) plan satisfactorily follows the guidelines in IEEE Std 1012-1986, "IEEE Standard for Software Verification and Validation Plans," (Reference 4) and the guidelines in Regulatory Guide (RG) 1.152 (Reference 5), which endorses ANSI/IEEE-ANS-7.4.3.2-1982, "American National Standard, Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations" (Reference 6). The licensee contractor's documentation describing the PLC and load sequencer logic will be provided to the licensee when the contractor delivers the load sequencer systems. Additionally, the licensee will witness the contractor's integrated systems tests to ensure its compliance with the licensee's specifications for Class 1E load sequencer system.

The verification phase of the licensee's V&V plan addresses verification of hardware requirements, software requirements, software design, software implementation, and hardware/software integration. System validation will consist of preparation and independent verification of test procedures, execution of the tests, and documentation with independent verification of the test results. The staff will audit the licensee's V&V program and documentation as part of a post-installation system audit.

The licensee will qualify the PLCs as Class 1E through dedication of the commercial grade equipment. The licensee's acceptance criteria will include a review of the contractor's commercial dedication of the PLCs. The dedication will be in accordance with Generic Letter 89-02, "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products," (Reference 7) and Generic Letter 91-05, "Licensee Commercial-Grade Procurement and Dedication Programs" (Reference 8). Both Generic Letters endorse the guidance provided in a report issued by the Electric Power Research Institute (EPRI), EPRI NP-5652, "Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications (NCIG-07)," (Reference 9). The staff will audit the results of the commercial grade equipment dedication to ensure the licensee addresses Criteria III, IV, and VII of Appendix B to 10 CFR Part 50.

The staff requested that the licensee provide a discussion of the acceptance criteria for verifying control cabinet instruments and logic. The licensee states that the control cabinet instruments and control logic functions will be fully tested during the verification and validation testing phases. This will include module testing and integrated testing. Additionally, the licensee will test load sequencer response to simulated plant events. The tests to be performed will address the following scenarios:

1. Safety injection followed 30 seconds later by a degraded voltage;

2. Safety injection with a simultaneous loss of offsite power; and

3. A loss of offsite power.

The load sequencing function is the same for all transient scenarios; consequently, the staff finds these tests to be adequate for ensuring load sequencer operability.

The licensee states that, in addition to the regularly scheduled EDG startup and bus loading tests, the load sequencer function will be tested from its input signals through the logic and counter states, relay drivers, and continuity through the relay coils on a monthly interval. The licensee states that, in the event a plant transient occurs during the testing period, the load sequencer will change from its test mode into operating mode and begin loading buses in approximately 250 milliseconds. The licensee further states that, in addition to the above tests, during preoperational testing, power will be removed from the PLC and all programmable functions will be verified to function per design requirements upon restoration of power to the PLCs. The staff finds this test program and test sequence interruption time to be acceptable.

A watchdog timer is built into the load sequencer system, such that a loss of load sequencer function is annunciated in the main control room. The watchdog timer monitors the proper functioning of software events that occur periodically. The licensee states that the operating procedures are being revised to incorporate manual actions to respond to an annunciated problem and to bypass a failed load sequencer to allow stripping the bus, starting the EDG, and loading onto the bus the equipment necessary for safe plant shutdown.

Because the time required to manually load the required buses upon failure of the load sequencer has not changed from the previous design, the staff finds the manual override provisions and the method of detecting and annunciating load sequencer problems to be acceptable. Using RG 1.47 (Reference 10) as a guideline, the staff will audit the licensee's method of providing the control room operators with load sequencer bypass indications and inoperable state indications.

The load sequencer PLCs contain on-board battery back-up capable of retaining all stored program data in the random access memory (RAM) through a continuous power outage of 12 months. The licensee will inspect the condition of the batteries every refueling outage and replace the batteries as needed. The staff finds this configuration and battery maintenance practice to be acceptable.

The PLCs use electrically erasable programmable read only memory (EEPROM) modules for nonvolatile storage of the PLC programs. The EEPROM is used to download the PLC operating program to the PLC RAM following recovery from loss of PLC power if the battery backup has not maintained RAM in a power on state. When power is restored to the PLC, the operational software will determine whether RAM has been corrupted, and either download from EEPROM or continue PLC operation. The staff finds this configuration to be acceptable.

The licensee states that the operator can manually control the load and source breakers by placing the load sequencer control switch on the main control board to the MANUAL position. This capability for manual control is acceptable.

The PLC vendor, Allen-Bradley, performed National Electrical Manufacturers Association (NEMA) Noise Susceptibility tests in accordance with NEMA ICS 2, Part 2-230, and NEMA ICS 3, Part 3-304.42. These tests subject the equipment to electrical noise that is commonly produced by electrical contacts interrupting inductive loads. Additionally, a Surge Transient Test was performed by Allen-Bradley in accordance with IEEE 472-1974 (ANSI C37.90a-1974). This test subjects the equipment to the type of electrical spikes that are generated by switching relays. The licensee will verify and have available for audit verification that the electromagnetic environment qualification at the plant is enveloped by the vendor's tests.

The licensee states that Allen-Bradley performed two tests: a Radiated Electromagnetic Susceptibility test in accordance with Scientific Apparatus Makers Association (SAMA) Standard PMC 33.1-1978 and IEC Standard 801-3, Edition 1, 1984; and a Conducted Electromagnetic Susceptibility test for line-connected equipment in accordance with MIL-STD-461/462, tests CS01, CS02, and CS06 for Class A3 equipment. The tests subjected the PLCs to frequencies of 20 MHz to 1 GHz, with a field strength of 10 V/m. This range of frequencies envelopes typical radio frequencies for portable two-way radios, which have field strengths less than 10 V/m. Consequently, the staff finds the proposed qualification program for electromagnetic interference (EMI) and radio frequency interference (RFI) to be acceptable. During the site audit, the staff will ensure that the vendor's tests envelope the EMI and RFI environment of the installed equipment.

The licensee states that the non-1E systems interfacing with the PLC are the inputs to the plant computer through a remote multiplexer unit, inputs to the annunciator system, and contacts to the main control board indicating lights. These non-1E interfaces are isolated from the PLC with coil to contact and contact to contact isolation relays. These forms of isolation are acceptable. The staff will verify the non-1E isolations during the site audit of the load sequencer implementation.

The licensee states that the NSP Electrical Systems Engineering group will be responsible for configuration control in accordance with the Prairie Island Quality Assurance Manual. Revisions to the load sequencer after installation will be in accordance with the licensee's Uniform Modification Process, including 10 CFR 50.59 evaluations. The staff finds this to be an acceptable means of ensuring load sequencer configuration control.

3.0 CONCLUSION

Based on the above evaluation, the SICB staff finds the instrumentation and control systems aspects of the Prairie Island Unit 2 load sequencer system to be acceptable. The licensee has committed to a formal V&V program, augmented by extensive testing of both the hardware and software. The V&V program satisfactorily follows the guidelines in IEEE Std 1012-1986, "IEEE Standard for Software Verification and Validation Plans," and RG 1.152, which endorses ANSI/IEEE-ANS-7.4.3.2-1982. Additionally, the licensee will verify that the PLC electromagnetic environment at the plants is enveloped by the vendor's tests, and have this information available at the plant site or the licensee's offices for staff audit. The non-1E systems are isolated from the 1E load sequencer with coil to contact and contact to contact isolation relays. These

forms of isolation are acceptable. The staff will verify the non-1E isolations during the site audit of the load sequencer implementation.

The licensee states that the NSP Electrical Systems Engineering group will be responsible for configuration control in accordance with the Prairie Island Quality Assurance Manual. Revisions to the load sequencer after installation will be in accordance with the licensee's Uniform Modification Process, including 10 CFR 50.59 evaluations. The staff finds this to be an acceptable means of ensuring configuration control.

To ensure the acceptability of the load sequencer implementation, the staff will audit:

(1) Software and hardware modifications to determine the acceptability of the V&V program;

(2) Isolation of non-1E systems from the Class 1E portion of the load sequencer;

(3) Dedication of load sequencer commercial grade components;

(4) Verification that the electromagnetic environment qualification at the plant is enveloped by the vendor's tests; and

(5) The licensee's method of providing the control room operators with bypass indications and inoperable state indications.

Principal Contributor: M. Waterman

Date: January 4, 1993

References:

(1) Letter from Northern States Power Company to U.S. Nuclear Regulatory Commission dated November 27, 1990, "Design Report for the Station Blackout/Electrical Upgrade Project."

(2) Letter from U.S. Nuclear Regulatory Commission to Northern States Power Company dated June 6, 1991, "Request for Additional Information - Station Blackout/Electrical Safeguards Upgrade Project (TAC Nos. 68588/68589)."

(3) Letter from Northern States Power Company to U.S. Nuclear Regulatory Commission dated July 10, 1991 and October 24, 1991, "Reply to Questions on Design Report for the Station Blackout/Electrical Safeguards Upgrade Project (TAC Nos. 68588/68589)."

(4) IEEE Std 1012-1986, "IEEE Standard for Software Verification and Validation Plans."

(5) Regulatory Guide 1.152, "Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants," U.S. Nuclear Regulatory Commission, November, 1985.

(6) ANSI/IEEE-ANS-7.4.3.2-1982, "American National Standard, Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations."

(7) Generic Letter 89-02, "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products," U.S. Nuclear Regulatory Commission, March 21, 1989.

(8) Generic Letter 91-05, "Licensee Commercial-Grade Procurement and Dedication Programs," U.S. Nuclear Regulatory Commission, April 9, 1991.

(9) EPRI NP-5652, "Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications (NCIG-07)," Electric Power Research Institute, June, 1988.

(10) Regulatory Guide 1.47, "Safety System Status Monitoring for Nuclear Power Plants," U.S. Nuclear Regulatory Commission, May, 1973.