UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 123 TO FACILITY OPERATING LICENSE NO. NPF-21

WASHINGTON PUBLIC POWER SUPPLY SYSTEM

NUCLEAR PROJECT NO. 2

DOCKET NO. 50-397

1.0 INTRODUCTION

By letter dated November 30, 1993, Washington Public Power Supply System (the licensee) requested an amendment to Washington Nuclear Project, Unit 2 (WNP-2), Facility Operating License No. NPF-21. The amendment involves replacing the existing analog General Electric (GE) Integrated Nuclear Measurement and Control (INMAC) Main Steamline (MSL) Logarithmic Radiation Monitor (LRM) with a digital GE Nuclear Measurement Analysis and Control (NUMAC) LRM. The proposed amendment does not require changes to the WNP-2 Technical Specifications. We evaluated the safety significance of replacing the existing analog monitoring system with digital equipment from the GE NUMAC line.

2.0 EVALUATION

Our evaluation focused on the following issues:

- Class 1E circuit independence
- temperature and radiation exposure effects
- seismic qualification
- electromagnetic and radio frequency interference
- electrostatic discharge
- software design and quality assurance
- common-mode failure defense
- training

We evaluate these issues below after describing the system and proposed system improvements.

2.1 System Description

Figure 1 shows a NUMAC-LRM functional block diagram. The safety-related

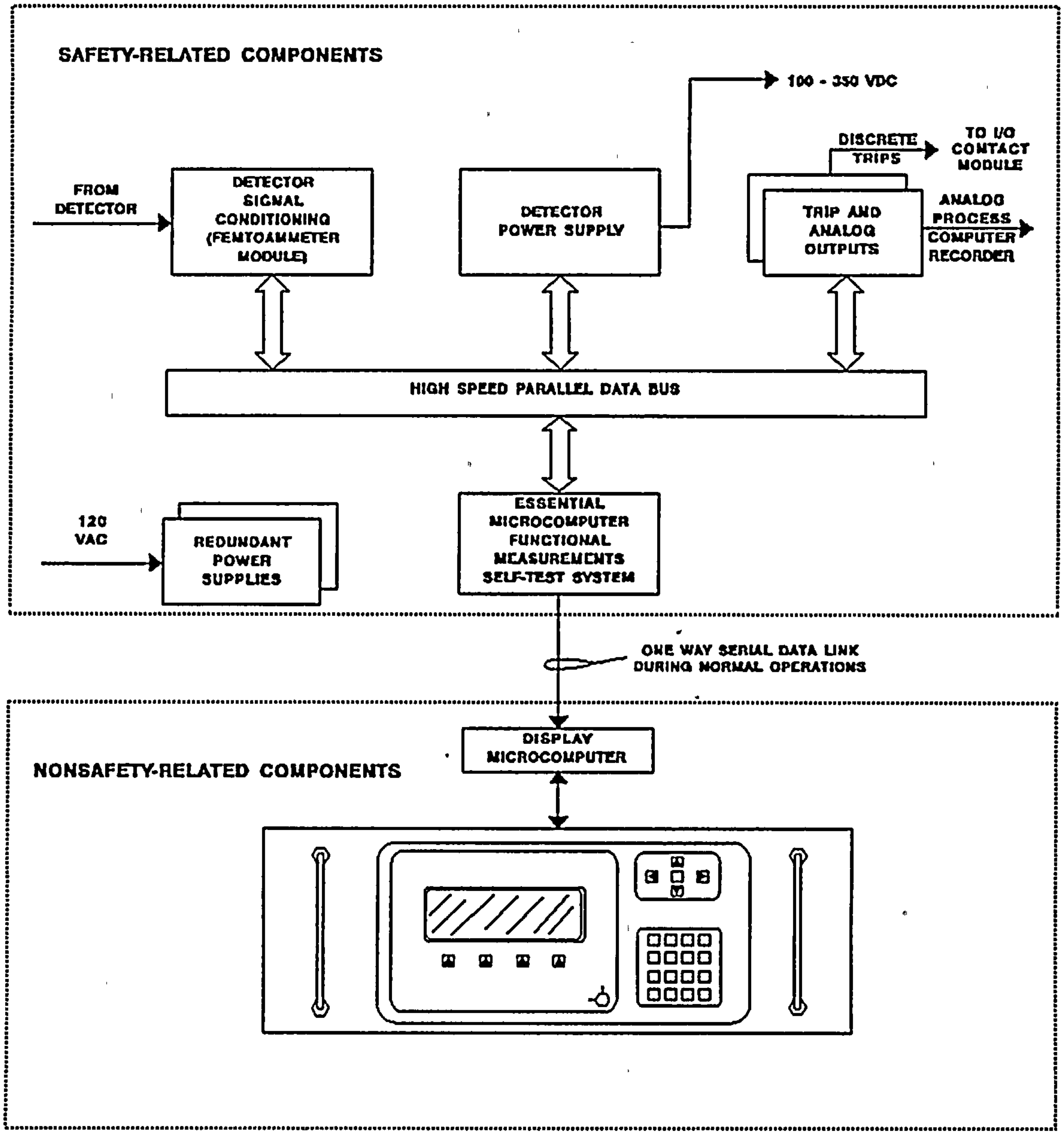

Figure 1. NUMAC-LRM functional block diagram

portion of the NUMAC-LRM consists of four channels of the following components:

- detector signal conditioning (femtoammeter module)
- detector power supply
- trip and analog outputs
- high speed parallel data bus
- essential microcomputer functional measurements self-test system
- serial data link
- Class 1E redundant 120 Vac power supplies

The display microcomputer and the front panel display are nonsafety-related components.

The detector signal conditioning (DSC) module in each monitoring channel receives femtoamp-magnitude input signals from its associated gamma-sensitive ion chamber. The ion chamber is mounted near the main steam outlet piping. The DSC processes the detector current signals into corresponding millirem per hour (mR/hr) signals. It also transmits the mR/hr signals to the essential microcomputer via an RS-485 serial connection and a signal splitter. The essential microcomputer, using a Harris 80C86 microprocessor, converts the mR/hr signals into control signals. The control signals are then transmitted to the other modules within the chassis using a high-speed parallel data bus. The essential microprocessor also transmits the signals to the display microprocessor/front panel display over an RS 232 serial data link. The essential microcomputer also performs self-test system diagnostics when not processing instrument data. The self-test feature has a lower processing priority than the safety features. Consequently, the self-diagnostic routines are automatically exited when a higher priority signal requires processing. This assures the essential microprocessor will perform the safety-related tasks in the shortest possible time.

The high speed parallel data bus is a 16-bit data/20-bit address bus on the main circuit board. The serial data link is "broadcast only" from the essential microprocessor when the key-locked Mode switch is in the OPERATE mode. Operators must put the Mode switch in the INOP mode for two way data transfer.

The nonsafety-related display microcomputer uses a National Semi-conductor NSC-800 microprocessor. This microcomputer displays the data from the safety-related essential microcomputer on the nonsafety-related front panel display. This display will replace the annunciator lights on the existing INMAC-LRM faceplates. The front panel display contains all of the circuitry necessary to interface with the display microcomputer, the front panel keyboard, and the electro-luminescent display.

Each NUMAC-LRM channel has redundant diode-auctioneered 120 Vac Class 1E instrument power supplies that supply power to the MSL LRM chassis. An adjustable 100 → 350 Vdc power supply in each channel provides power to its gamma sensitive ion chamber detector.

The safety-related outputs from each NUMAC-LRM channel consist of:

- four solid state contact output trip signals (HI-HI, HI, LO, and INOP-HVPS)
- an analog Transient Data Acquisition System (TDAS) signal (Channels A and B only), and
- a 230 Vdc output to excite the associated detector chamber ion gas

A femtoammeter amplifier transmits three trip circuit signals (HI-HI, HI and LO) to the essential computer. The essential computer processes the input trip current signals and produces independent output trip voltage signals for the input-output (I/O) contact module. Operators can preset the trip circuits to trip at any desired limit. A fourth trip circuit signal (INOP-HVPS) actuates on any of the following inoperability indicators:

- keylock position other than OPER
- internally generated exciter voltage level ±10% outside the voltage setpoint
- functional microprocessor watchdog timer timed out
- a dislodged essential module card

The NUMAC-LRM HI-HI and INOP-HVPS trip outputs input to an I/O contact module. The contact module gives an output to trip the main condenser mechanical vacuum pump and close the vacuum pump discharge valve. This trip limits main condenser coolant leakage to less than 1 percent of the main condenser volume per day for the design basis control rod drop accident. The NUMAC-LRM can also trip the RPS and initiate MSIV functions, although the safety analyses do not take credit for these actions.

A HI trip from any LRM MSL channel actuates a MSL high radiation alarm in the Main Control Room (MCR). A LO trip from any channel actuates a MSL monitor downscale alarm. The HI and LO trips provide only alarm functions. The four trips (HI-HI, HI, LO and INOP-HVPS) reset automatically. However, the trip status on the monitor screen display (for the HI-HI, HI and LO trips) and the system trip actions must be manually reset from the module display. This assures that the safety-related actions will go to completion once they are initiated.

The NUMAC-LRM electronic module diagnostic and calibration features allow the following functions:

- calibrating the loop

- adjusting trip and pretrip setpoints
- adjusting detector excitation voltage level
- indicating operational status

Operators need keylock access to control the trip setpoints and exciter voltage levels. The user can access and set these items only after entering a password.

2.2 System Improvements

This design change replaces the existing INMAC MSL LRM analog type system with an equivalent NUMAC system. The licensee is replacing the INMAC equipment because GE no longer manufactures the presently installed system. Thus, future replacement part availability is uncertain. The primary purpose of the NUMAC product line instruments is to replace nearly obsolescent equipment with present-day state of the art technology and features. The licensee compared the existing INMAC system specifications with those of the NUMAC replacement system and found the NUMAC-LRM to be an equivalent functional and physical replacement. The NUMAC leak detection instruments installed at WNP-2 in 1989 gave the operators enhanced capabilities and reliability. The licensee expects that the NUMAC-LRM will give them similar benefits.

The licensee indicates that the existing INMAC MSL LRM is susceptible to output signal drift, spiking and inaccuracy. Additionally, there has been a high rate of instrument channel drawer failures. These problems have caused many spurious trips and alarms, instrument channel inoperability, and associated "emergency" maintenance activities. The licensee indicates that the NUMAC LRM has the following improvements over the INMAC system:

- it reduces instrument drift by a factor of four
- it improves instrument accuracy and resolution by a factor of two
- microprocessor self test functions will improve MSL LRM instrument reliability and availability
- the calibration and testing features will simplify maintenance activities because the electronic modules provide self-diagnostics, calibration and setting checks, and error messages
- there is an enhanced operator/equipment interface through a digital display, menu-driven software, and a human-factored engineered front panel design

2.3 Review Criteria

The NUMAC-LRM is part of the Class 1E plant protection system. Therefore, the review guidance consists of:

- General Design Criteria (GDC)

- IEEE standard 279, "Criteria for Protection Systems for Nuclear Power Generation Station" (10 CFR 50.55a(h))

- applicable Standard Review Plan (NUREG-0800) acceptance criteria

- ANSI/IEEE-ANS- 7-4.3.2-1982, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations"

- Regulatory Guide 1.152, "Criteria for Programmable Digital Computer System Software in Safety Related Systems of Nuclear Power Plants"

2.4 Evaluation

Appendix A to 10 CFR Part 50, to GDC 2, and GDC 4 require that the safety system be designed to withstand natural phenomena effects. They also require the system to be qualified to operate in the environmental conditions to which it is exposed, including normal and postulated accident conditions. We reviewed the NUMAC equipment design to ensure that the NUMAC-LRM will perform its intended function(s) under these conditions.

2.4.1 Independence

We reviewed the equipment design using IEEE Std 384-1981, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits." The NUMAC-LRM safety-related components receive power from dedicated Class 1E power supplies, and interface with non-Class 1E equipment through qualified isolation devices. We determined that the methods of isolating the Class 1E components from the non-Class 1E components are acceptable.

2.4.2 Temperature and Radiation

GE used IEEE Standard 323-1974, "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations" to qualify the NUMAC-LRM equipment for the same temperature limits specified for the INMAC-LRM equipment being replaced. The NUMAC-LRM was designed for use in control rooms and similar environments that have a maximum operating temperature of 50°C (122°F) and a total integrated radiation dose of 1.75 Gy (175 Rads). Plant personnel will install the NUMAC-LRM equipment in the WNP-2 main control room. The control room temperature limit is 40°C (104°F). WNP-2 FSAR Appendix J, Section 6.0 shows the 40-year normal operation integrated radiation dose is 0.35 Gy (35 Rads). The licensee indicates that the airspace temperature inside the panels was assumed to be 10°C (18°F) above the MCR ambient temperature when the equipment was qualified. Thus, the maximum design basis temperature expected inside the panels where the NUMAC-LRM is to be installed is 50°C (122°F). The licensee concludes that the WNP-2 maximum operating temperature and total integrated dose values envelop the NUMAC-LRM qualification values.

We find that the NUMAC-LRM temperature and radiation qualifications envelope the WNP-2 temperature and radiation requirements. In addition, we find that temperature and radiation tests meet the intent of IEEE Standard 323-1974. Therefore, we find the temperature and radiation qualification acceptable.

2.4.3 Seismic Qualification

The NRC previously evaluated the NUMAC-LRM instrument and found the system acceptable for use in Class 1E applications. On May 17, 1985, GE submitted Licensing Topical Report NEDO-30883, "The Nuclear Measurement Analysis and Control Logarithmic Radiation Monitor (NUMAC-LRM)" to the NRC for review. The NRC evaluated the topical report and issued a Safety Evaluation (SE) on September 16, 1986. The SE concluded that the topical report, with supplemental information from GE, demonstrated that the NUMAC-LRM will reliably perform safety-related functions. The NRC cover letter with the SE indicated utilities could reference the topical report in licensing applications. Subsequently, GE issued the topical report as NEDO-30883-A in January 1987.

The licensee indicates that GE seismically qualified the NUMAC-LRM equipment in accordance with IEEE Standard 344-1975, "Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations." NEDO-30883-A has the seismic response spectra. The licensee reviewed the NUMAC-LRM seismic qualification package and compared it to the MCR seismic qualification where it is to be installed. The licensee concluded that the NUMAC-LRM installation would maintain instrument and MCR panel qualification. They based this conclusion on an analysis of the instrument mass and the response spectra. Accordingly, we conclude that the seismic qualification is acceptable.

2.4.4 Electromagnetic and Radio Frequency Interference

Electrical systems and natural electrical phenomena (such as lightning) produce electromagnetic signals. These can cause electromagnetic and radio frequency interference (EMI/RFI) with electrical equipment. This interference can affect plant safety since it can potentially lead to common-mode failures of redundant safety-related equipment.

Digital instrumentation and control (I&C) systems operate at higher frequencies than equivalent analog equipment. They are susceptible to a broad bandwidth of electromagnetic and radio frequency interference signals. We therefore emphasize our review of safety-related digital I&C equipment vulnerabilities to EMI and RFI. We used the following documents for this evaluation:

- 10 CFR Part 50, Appendix A, Criterion 4, "Environmental and Dynamic Effects Design Bases"
- the fourth paragraph of Standard Review Plan Section 7.1 Appendix B, "Guidance for Evaluation of Conformance to IEEE STD 279"

We also referenced the following standards:

- MIL-STD-461C, "Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference"

- MIL-STD-462, "Electromagnetic Interference Characteristics Measurement"
- MIL-STD-1399, "Interface Standard for Shipboard Systems, DC Magnetic Field Environment"
- SAMA PMC 33.1-1978, "Electromagnetic Susceptibility of Process Control Instrumentation"
- NRC Information Notice 83-83, "Use of Portable Radio Transmitters Inside Nuclear Power Plants"
- IEC 801-2 "Electromagnetic Compatibility for Industrial-Process Measurement and Control Equipment Part 2: Electrostatic Discharge Requirements"
- NUREG/CR-3270, "Investigation of Electromagnetic Interference (EMI)— Levels in Commercial Nuclear Power Plants"

We followed the following four steps in reviewing the effects of the EMI/RFI noise environment around safety-related digital equipment:

1. Evaluate the plant, and identify potential EMI/RFI sources.
2. Review the vendor EMI/RFI qualification methodology and the test frequency range.
3. Review the licensee's EMI/RFI qualification process for the installed equipment.
4. Review the licensee's EMI/RFI field measurement at the installed equipment, and verify that the equipment is operating within its qualified environment.

GE designed the NUMAC-LRM to account for EMI/RFI in accordance with GE EMI Susceptibility Test Guide 249A1238. The licensee surveyed the WNP-2 MCR environment with the reactor at power. They used MIL-STD 461 and 462 as the bases to determine the MCR EMI/RFI level, and to confirm that the MCR EMI/RFI levels are within the GE design envelope. The licensee will submit the site survey results to us for confirmatory review. The licensee expects the WNP-2 MCR EMI/RFI environment to be acceptable for the NUMAC-LRM installation because other NUMAC equipment has been in operation in the WNP-2 MCR for four years without any EMI/RFI problems. We conclude that the licensee and GE have acceptably addressed EMI/RFI concerns.

2.4.5 Electrostatic Discharge

Electrostatic discharge (ESD) is static charge transfer between two objects that are at different electrostatic potentials. Integrated circuit (IC) components are very sensitive to ESD. ESD can stress IC components beyond their design tolerances, which can reduce the service life of a component or

cause the component to immediately fail. Consequently, ESD can greatly reduce NUMAC-LRM system reliability, which has many IC components.

GE used IEC standard 801-2, "Electromagnetic Compatibility for Industrial-Process Measurement and Control Equipment Part 2: Electrostatic Discharge Requirements," to qualify the NUMAC-LRM. Additionally, the NUMAC-LRM operation and maintenance manual gives guidance on avoiding electrostatic damage to vulnerable modules. The precautions in the manual include:

- grounding work surfaces
- grounding all tools and test equipment
- having the technicians connect themselves to ground using a conductive bracelet
- not wearing nylon clothing or other static generating materials
- never removing or inserting a card in a card file with power applied to the card

The licensee indicates that system grounding and isolation have proven to be acceptable for the existing INMAC-LRM instruments. Additionally, maintenance procedures currently contain precautionary information on the servicing of electrical and electronic devices susceptible to ESD. The licensee has trained its maintenance personnel on this subject. We conclude that the licensee and GE have acceptably addressed ESD qualification concerns.

2.4.6 Software Design and Quality Assurance

This section discusses GE's processes for developing the NUMAC-LRM software. GE developed the system requirements specification, and the licensee independently verified it. The verification process ensured that the system requirements were correctly translated into the design specification for the INMAC-LRM instrument and the NUMAC-LRM application. Hardware/software integration testing was specified in the software validation plans and procedures. The licensee verified these were consistent with the requirements specification. GE tested each module after its design implementation phase. They then converted the software to firmware on programmable read only memory (PROM) modules, and installed it in the NUMAC-LRM chassis for system integration testing, in accordance with GE's Self-Test Integration and Software Validation Test Plans and Procedures. The software code can only be changed by replacing the PROM. The licensee will control the software under the existing GE Software Management Plan.

We reviewed GE's software development process, as described in NEDO-30883-A, and found it to be an effective design verification and validation (V&V) process for developing NUMAC instrument software. Additionally, GE updated the V&V plan (GE 23A5163, "Software Verification and Validation Plan") to more clearly describe the actual V&V processes. This revision addressed NRC SE comments that discuss a similar NUMAC instrument design change at the Brown's

Ferry plants ("Reactor Building Ventilation Radiation Monitors Replacement License Amendment," March 30, 1993).

The GE V&V method consists of logical steps with baseline reviews performed at the completion of each development process phase. They documented and maintained a list of open items for each review. The reviewers are independent from the designers, and communicate their review in written reports. The validation step includes a matrix relating each validation test to a functional requirement. We will do a confirmatory audit of the updated software development process and documentation including the V&V and configuration management records. We find the software development process to be acceptable.

2.4.7 Defense Against Common-Mode Failure

The single failure criterion of IEEE 379-1972, "IEEE Trial Use Guide for the Application of the Single Failure Criterion to Nuclear Power Generating Station Protection Systems," requires that any single failure within the protection system shall not prevent proper protective action at the system level when required. Common-mode failures are single failures that can prevent a safety feature from performing its intended function. They also can result in the loss of more than one defense-in-depth echelon provided by the monitoring, control, reactor protection, and engineered safety functions. Particularly, microprocessor-based digital systems, such as the NUMAC-LRM, which share data bases and process equipment, have a potential for common-mode failures in the software, hardware, and software/hardware interaction. Quality and diversity defend against common-mode failure.

The potential sources of NUMAC-LRM common-mode failures include the software, hardware, and their qualifications. Sections 2.4.1 through 2.4.6 discuss the quality aspects of defenses against such failures. In case of command-mode NUMAC-LRM failure, the operator can also manually perform NUMAC-LRM actuation functions from the MCR using information from the MSL radiation indicators and alarms. This capability gives additional diversity from the NUMAC-LRM. We conclude that the NUMAC-LRM defense against common-mode failures is acceptable.

2.4.8 Training

Training is an important part of installing and operating the NUMAC-LRM. The licensee will train the operators and technicians in using and repairing the new system. The licensee indicates that the NUMAC-LRM will reduce the need for an instrument drawer to be removed for servicing. This will increase redundant instrument availability. Spare parts will be available from a complete onsite spare module. The licensee will revise operational and maintenance procedures, and will train plant staff before startup from the R-9 outage. Additionally, the licensee indicates that WNP-2 maintenance and operations staff are familiar with NUMAC instrumentation because similar NUMAC instrumentation has been in operation at WNP-2 since 1989. We find the licensee's commitments in this area to be acceptable.

3.0 STATE CONSULTATION

In accordance with the Commission's regulations, the Washington State official was notified of the proposed issuance of the amendment. The State official had no comments.

4.0 ENVIRONMENTAL CONSIDERATION

Pursuant to 10 CFR 51.21, 51.32, and 51.35, an environmental assessment and finding of no significant impact was published in the Federal Register on June 2, 1994 (59 FR 28432). Accordingly, based on the environmental assessment, the Commission has determined that issuance of this amendment will not have a significant effect on the quality of the human environment.

5.0 CONCLUSION

We find that the design changes related to replacing the existing MSL LRM equipment with digital NUMAC equipment meet the following criteria and are, therefore, acceptable:

- IEEE 279 and GDC 2 and 4 requirements for single failure and environmental qualification
- RG 1.152 guidelines for digital system design

The Commission concludes, based on the considerations discussed above, that (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, (2) such activities will be conducted in compliance with the Commission's regulations, and (3) the issuance of the amendment will not be inimical to the common defense and security or to the health and safety of the public.

Principal Contributor: Michael Waterman
Date: June 2, 1994