Docket Nos. 50-315
and 50-316

May 13, 1994

Mr. E. E. Fitzpatrick, Vice President
Indiana Michigan Power Company
c/o American Electric Power Service Corporation
1 Riverside Plaza
Columbus, Ohio 43215

Dear Mr. Fitzpatrick:

SUBJECT: DONALD C. COOK NUCLEAR PLANT, UNIT NOS. 1 AND 2 - REVISED SAFETY EVALUATION FOR AMENDMENT NOS. 175 AND 160 RE: REACTOR PROTECTION SYSTEM UPGRADE PROJECT (TAC NOS. M84839 AND M84840)

On January 7, 1994, the Commission issued Amendment No. 175 to Facility Operating License No. DPR-58 and Amendment No. 160 to Facility Operating License No. DPR-74 for the Donald C. Cook Nuclear Plant, Unit Nos. 1 and 2. The amendments modified your licenses to allow the replacement of the existing Foxboro protection systems with Foxboro's SPEC 200 and SPEC 200 MICRO digital instrumentation in response to your application dated December 16, 1992, as supplemented December 22, 1993.

Subsequent to the issuance of the amendments several inaccuracies regarding the descriptions of system operations were identified in the associated safety evaluation. The enclosed revised safety evaluation corrects those errors. Vertical lines in the right margin indicate the areas of change.

Sincerely,

Original signed by

John B. Hickman, Project Manager
Project Directorate III-1
Division of Reactor Projects - III/IV
Office of Nuclear Reactor Regulation

Enclosure:
Revised Safety Evaluation

cc w/enclosure:
See next page

OFFICE	LA:PD31	PM:PD31	BC:NICB	D:PD31
NAME	CJamerson	JHickman:	JWermiel	LMarsh
DATE	6/9/94	5/9/94	5/11/94	5/13/94

OFFICIAL RECORD COPY FILENAME: G:\ WPDOCS\DCCOOK\C084839.AMD

180007

DF01

DATED: May 13, 1994

REVISED SAFETY EVALUATION FOR AMENDMENT NO. 175 TO FACILITY OPERATING LICENSE NO. DPR-58-D. C. COOK UNIT 1

REVISED SAFETY EVALUATION FOR AMENDMENT NO. 160 TO FACILITY OPERATING LICENSE NO. DPR-74-D. C. COOK UNIT 2

Docket File
NRC & Local PDRs
PDIII-1 Reading
J. Roe
J. Zwolinski
L. B. Marsh
J. Hickman
C. Jamerson
OGC-WF
D. Hagan, 3302 MNBB
G. Hill (4)
C. Grimes, 11/F/23
S. Rhow
R. Pulsifer
ACRS (10)
OPA
OC/LFDCB
W. Kropp, R-III
SEDB

cc: Plant Service list

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

REVISED SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION RELATED TO AMENDMENT NO. 175 TO FACILITY OPERATING LICENSE NO. DPR-58 AND AMENDMENT NO. 160 TO FACILITY OPERATING LICENSE NO. DPR-74 INDIANA MICHIGAN POWER COMPANY DONALD C. COOK NUCLEAR PLANT, UNIT NOS. 1 AND 2 DOCKET NOS. 50-315 AND 50-316

1.0 INTRODUCTION

By letter dated December 16, 1992, as supplemented December 22, 1993, the Indiana Michigan Power Company (the licensee) requested amendments to Facility Operating License Nos. DPR-58 and DPR-74 for the Donald C. Cook Nuclear Plant, Unit Nos. 1 and 2. The proposed amendments would upgrade portions of the reactor protection system (RPS) instrumentation for the D. C. Cook Nuclear Plant, Units 1 and 2. The December 22, 1993, letter provided clarifying information which did not change the staff's initial proposed no significant hazards consideration determination.

This modification to the RPS is necessary due to the increased maintenance required on the existing Foxboro H-Line protection system and the difficulty in obtaining qualified replacement parts. The upgrade involves the installation of Foxboro SPEC 200 MICRO Line of microprocessor-based instrumentation. This upgrade would provide the licensee with configurable, microprocessor-based protection and control system modules. The SPEC 200 MICRO system processes the same inputs as the current analog system, performs the same calculation and bistable functions, and supplies contact outputs to the reactor protection logic for initiating a reactor trip and engineered safety feature (ESF) functions. The system also includes isolated analog outputs to indicators, recorders, plant computer and various control systems. The specific equipment and configuration of this upgrade has been previously approved by the NRC for use in the RPS at the Haddam Neck plant in 1990. Therefore, the staff review of the D. C. Cook RPS Upgrade incorporated direct comparison to the previously approved Haddam Neck design, and focused on aspects specific to D.C. Cook.

2.0 OBJECTIVE

The objective of this safety evaluation (SE) is to assess the adequacy of the proposed Foxboro SPEC 200 MICRO microprocessor-based system, with emphasis on replacement system features that differ from the previously approved design. Attendant key issues addressed in the SE are the specific design bases for the new system, potential hardware vulnerabilities and susceptibilities, software

development, verification and validation (V&V), configuration management, potential control/protection systems interactions, system failure modes and effects, reliability, and the developmental and operational history of the system equipment. The hardware and software design was reviewed against applicable NRC and industry standards including the requirements and guidance of IEEE Standard 279-1971 and ANSI/IEEE-ANS-7-4.3.2-1982, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Station."

3.0 TECHNICAL APPROACH TO THE EVALUATION

3.1 General

The licensee was requested to demonstrate compliance with the appropriate criteria and demonstrate that the use of microprocessor-based equipment will not degrade the reliability of the RPS relative to the plant design basis. Pertinent criteria used in this review included the Standard Review Plan and Regulatory Guide (RG) 1.152, "Criteria for Programmable Digital Computer System Software in Safety Related Systems of Nuclear Power Plants," which endorses ANSI/IEEE-ANS-7-4.3.2-1982. The staff reviewed the following major topics which are important to safety and required licensee/vendor support in providing appropriate documentation and personal interface with the reviewers:

1. Assessment of functional equivalence of the upgrade relative to the original design basis.

2. Assessment of the vendor's design (functional requirements and specifications) and V&V processes.

3. Assessment of licensee and vendor procedures and methodologies for the transformation of functional requirements to the software configuration that implements the requirements.

4. Assessment of the licensee's development of the design modification with respect to the design basis.

5. Assessment of the licensee's configuration management process for the new design.

These major topics are addressed from hardware, software, and systems engineering perspectives. In executing the review, a "thread concept" evaluation approach was used, whereby a single functional (sensor through actuator) requirement was followed from design through implementation, V&V testing, and any retesting required when a failure is encountered. Where necessary, additional functional requirements were examined to sufficiently cover the hardware, software, and systems evaluation criteria.

3.2 Approach to Hardware and Systems Assessment

The licensee was asked to demonstrate that hardware/system vulnerabilities and susceptibilities that have potentially greater significance in a digital system than in an analog system have been addressed in the design. It was

requested that particular attention be placed on interfaces of the new digital equipment with old equipment or circuits, including power sources. As part of the review, the licensee and vendor also provided evidence of the enhancements provided by the new equipment such as higher reliability and more accurate control capability, such as a reduction in instrument setpoint drift. Areas of potential vulnerability/susceptibility addressed by the licensee and assessed in the staff review include the following:

1. Environment-temperature (particularly within cabinets) and humidity.

2. Electrical voltage and frequency surge withstand capability credible faults (system tolerance to power surges), and the use of existing inverters to supply power to the new equipment.

3. Electromagnetic interference (EMI) including radio frequency interference (RFI) - radiated EMI/RFI susceptibly and noise propagation via power lines to the new equipment.

4. Failure Modes and Effects

   a. Detectability of failures and recovery.

   b. Special failure modes (for example, system stall, timing errors/instability) and the effects on frequency and severity of transients.

5. Technology Upgrade Comparisons

   a. Comparison of reliability/availability of new equipment to the original equipment.

   b. Identification of failure mode differences between new and old equipment.

6. Independence

   a. Physical and electrical separation and barriers.

   b. Isolation devices and their application.

   c. Independence of various software functions.

7. Seismic Qualification

To effectively perform the review, the licensee was requested to provide sufficient description of the design change to enable a comparison of the original RPS to the proposed RPS upgrade. The licensee provided the following documentation:

1. A functional block diagram of the RPS.

2. A hardware block diagram of the RPS including interfaces (before and after the upgrade).

3. Clear definition on the above drawings of protection/control system boundaries, protection division (channel and train) boundaries, power sources/supplies, and isolation devices or other methods of assuring independence that are used at these interfaces.

4. The modification package, supporting design documentation, and safety evaluation.

5. Identification of the standards, criteria, specifications, calculations, analyses and tests that address the hardware attributes of interest. The criteria, assumptions, and methodology used to establish the design basis for the electrical environment and EMI environment, and demonstration of compliance to the design basis were of special interest.

Also, the licensee provided or made available for review the following:

1. Factory acceptance test reports

2. Site acceptance test reports

3. Operating and maintenance procedures

4. Test procedures/reports for periodic testing of the system

5. Data on self-diagnostic failures

3.3 Approach to Software Assessment

The inclusion of microprocessors and their concomitant software in the RPS marks a significant departure from the original analog electronic design. While the transition to digital systems may provide significant performance and safety advantages, it may also introduce issues and concerns that have not been encountered previously and have not undergone a thorough safety review at D.C. Cook.

For the software assessment, the licensee must demonstrate that the software is in accordance with the functional design, and that the implementation process will result in reliable software. The licensee must also demonstrate that an adequate program is in place to assure that the reliability of the software is maintained for the entire software life cycle including revisions to the permanent software and user configurable software.

To assess these points of concern, the software audit focused on three main areas:

1. The design, development and operational history of the vendor's software.

2. The procedures and methodologies in use by the licensee/vendor to ensure that the vendor-supplied hardware and software control blocks are functionally equivalent to the design basis for the RPS.

3. The procedures and V&V processes used by the licensee/vendor to control the user configurable software elements.

To perform the software assessment, the licensee/vendor was asked to make available the following information:

1. A description of the design development and operational history of the vendor's software components.

   a. A description of the design and software development activities.

   b. The scope and results of static and dynamic tests for the software.

   c. A description of the acceptance testing performed and the results of the testing.

   d. Documentation of all software modifications performed since its release.

   e. A description of the programmable read only memory (PROM) "burn in" process and what procedures are in place to ensure that the finished PROM is correct.

2. A description of the procedures and methodology used by the licensee to ensure that the functional design basis is implemented.

   a. The functional specification for the system and the derivation of the control block configuration.

   b. The procedures and methods used to ensure that the control block configuration will implement the control logic as specified.

   c. A description of the licensee's user configurable software management program.

   d. The results of testing the completed system, the list of errors, and how the errors were detected and corrected.

3. A description of the procedures and V&V processes used to control the configuration of software for the control blocks.

   a. A description of the vendor's verification activities for the control block software.

   b. The results of verification activities during the development including characterization of the errors found by type and percentage of the total errors.

c. The results of validation activities during testing including characterization of the errors found by type and percentage of total errors.

d. A description of the steps taken to ensure the independence of the verifier and the verifier's recourse in the event that discrepancies or errors are found.

4.0 DESCRIPTION OF SYSTEM UNDER REVIEW

4.1 Scope of System Modification

The proposed RPS modification is limited to replacing power supplies and process signal conditioning instrumentation. The process signal conditioning instrumentation prepares signals from existing process sensors, determines when protective action is required, and initiates a channel trip at a predetermined limit. The modification does not change the existing RPS actuation logic. The licensee chose a design approach that limits duplication of existing functions of the RPS instrument cabinets and minimizes the impact to external cabling and power sources.

4.2 Functional/System Description

The proposed changes are intended to modernize the D. C. Cook Reactor Control and Protection System instrumentation by replacing a portion of the original equipment supplied for processing the following parameter inputs: Pressurizer Pressure, Pressurizer Level, Reactor Coolant Flow, Steam Generator (SG) Narrow Range Level, SG Steam Flow, SG Pressure, Feedwater Flow, Reactor Coolant System (RCS) Delta Temperature, RCS Average Temperature, Containment Pressure, Turbine Impulse Pressure, Wide Range RCS Temperature, Wide Range RCS Pressure, Refueling Water Storage Tank (RWST) Level, Containment Level, Auxiliary Feedwater Flow, $T_{SAT\ (Saturation)}$ Input Select, and Condensate Storage Tank Level. To implement the input processing, the licensee has procured a series of microprocessor-based control modules that have been installed in the existing Foxboro SPEC 200 racks at the D.C. Cook Nuclear Plant. The following new equipment will perform the same functions as the equipment it replaces:

1. Foxboro SPEC 200 Type Analog Input Signal Conditioning, which changes the various types and values of input signals from the sensors into a common type of analog output signal that represents the input values at the channel level.

2. Foxboro SPEC 200 MICRO Digital Signal Processing Equipment, which takes the analog signal from the SPEC 200 analog input equipment at the channel level and:

   a. Changes the analog signals to digital signals.

   b. Processes the digital signals and compares them against predetermined limits, as well as performs dynamic functions and calculations.

   c. Changes the processed digital signals back to analog output signals.

3. Foxboro SPEC 200 Analog Output Signal Conditioning Equipment, which takes the analog output signals from the SPEC 200 MICRO and conditions them for use in the control system, as well as for indication and recording use.

4. Foxboro SPEC 200 Type Contact Output Equipment, which produces discrete trip signals from the SPEC 200 MICRO and provides trip signals for input to the reactor protection logic equipment.

5. Foxboro SPEC 200 Type Power Distribution Equipment, which powers the signal conditioning and processing equipment discussed above.

6. 75 VDC Multi-loop and +15 VDC Multi-nest Power Supplies, which provide power for the field transmitters and SPEC 200 equipment.

4.3 Hardware Description

The new hardware is based upon the application of the Foxboro SPEC 200 MICRO Control System. The system consists of control cards mounted within the existing cabinets and display stations located at the various control panels within the control room. The control card is a rack-mounted microprocessor-based unit which performs signal conditioning, regulatory control and logic control functions. The control functions are provided by the user configuration of up to 6 control blocks from a menu of 21 different types. Most block types have multi-functions available. The Continuous Display Station provides user interface to logic control blocks. These displays provide sequential paging to display more than one control block. Two 9-digit alphanumeric readouts provide configurable loop tag identification, digital readout of the block parameters in percent or engineering units, and the ability to modify control block tuning parameters.

The hardware items were tested to and accepted against the requirements of IEEE 344-1975 and portions of IEEE 323-1974. Environmental specifications to provide compatibility with the control room environment were identified for the equipment. The units are powered from the vital buses.

4.4 Software Description

The SPEC 200 MICRO is a software-based control system that uses a digital card to implement a wide range of control structures and logic. The SPEC 200 MICRO software was based on general functional requirements derived from the collective functions of approximately 100 existing Foxboro SPEC 200 analog control cards. The software is presented as 21 modules (control blocks) that can be configured for specific applications by a menu-driven setup process. The responses selected from the menu by the licensee fill out internal tables which then control the operation of the specific control functions and logic.

On a single digital control card, an executable module for each of the 21 Processor Control Blocks is contained in the PROM and cannot be changed by the licensee. Up to six of these modules can be configured by the licensee at the site on any one control card to implement the required control logic. The system is configured by using a personal computer. The configuration software provides menu-driven "fill-in-the-form" displays. These displays

allow the control scheme to be configured, or the control blocks contained within the control card to be modified. Configuration is the process of selecting control block types and interconnecting these blocks to produce the desired control scheme. Displays allow the monitoring of the system parameters to verify selected control schemes.

The licensee stated that the D. C. Cook RPS application uses only 6 of the available 21 Control Blocks: CALC, ALRM, LLAG, GATE, SSEL, and RAMP. A brief description of these blocks follows:

CALC provides facilities for executing simple arithmetic equations. Fourteen functions are available and can be combined with data inputs and intermediary results to form an equation. The format is similar to that used on programmable calculators.

ALRM provides the facilities for setting alarm points for data inputs from the sensors. It includes absolute alarms, deviation alarms, rate alarms, output alarms and output limiting.

LLAG provides the facilities for setting lead-lag compensation parameters. The lead is defined by the configurator as an amplification factor of the lag term, and the lag is defined as a time constant.

GATE provides eight 2-input logic gates which allow configuration of various Boolean algebra (and, or, etc.) functions.

SSEL provides the facilities for selecting from up to eight separate input signals including the highest, lowest, or median.

RAMP provides a dual linear ramp generator with a single output.

5.0 TECHNICAL EVALUATION

The scope of the staff review of the Foxboro upgrade of the D. C. Cook Nuclear Plant, Units 1 and 2, RPS includes the new RPS equipment to be installed, the interfaces of that equipment with existing equipment, and the environment encompassing the new Foxboro RPS equipment. This evaluation is based on the guidelines of RG 1.152. RG 1.152 states that the NRC staff encourages the application of advanced technology such as programmable digital computers in the operation of nuclear power plants if such technology serves to enhance safety. RG 1.152 endorses, with certain exceptions, IEEE Standard 603-1980 which establishes criteria for safety systems, structures and equipment necessary for plant safety.

Section 5 of IEEE 603-1980 establishes the criteria for safety system performance and equipment. The following sections discuss these criteria and the implementation of these criteria as established during the audit of the Foxboro facility and documentation. Included in the scope of the staff review against these criteria was the licensee's channel setpoint methodology, human factors considerations, grounding, electromagnetic and radio frequency interference, use of the configurator, and various tests that establish the

acceptability of the Foxboro SPEC 200 and SPEC 200 MICRO equipment installed for this application.

Sections 6 and 7 of IEEE Standard 603-1980 establish criteria for sensing, command, execute, and functional design requirements. The staff review addressed these items as discussed subsequently.

Section 8 of IEEE Standard 603-1980 addresses power sources. The power for the upgraded RPS did not require change. The existing power sources were found by the licensee to be capable of supplying the additional loading associated with the upgrade. Therefore, the power sources are acceptable.

5.1 Completion of Protective Action

Section 5.2 of IEEE Standard 603-1980 addresses the completion of the protective action by a safety system. If started either manually or automatically, the intended sequence of protective actions is to carry through to completion. Deliberate operator action is required to return the safety systems to normal. Seal-in of individual channels is not required. The upgraded RPS equipment consists of modules that affect individual channels. Individual channel trips may occur with no reactor trip. These individual channel trips are automatically removed if the process (level, pressure, temperature, etc.) returns to the non-trip side of the system setpoint. The upgraded equipment does not affect the Solid State Protection System where the individual channel trips are combined and the seal-in process occurs. Two or more channels must be in a trip state concurrently to affect a safety system actuation. The replacement equipment is only in individual signal processing channels and, as such, supports the completion of a safety function. This is acceptable to the staff.

5.2 Quality

Section 5.3 of IEEE Standard 603-1980 states that the quality of the components and modules is to be consistent with minimum maintenance requirements and low failure rates. Safety system equipment is designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program.

5.2.1 Hardware

Section 6.0 of the American Electric Power Service Corporation specification for the subject equipment addresses quality, documentation, testing, and checkout requirements. The quality requirements include:

1. IEEE Standard 323-1974 as supplemented by IEEE Standard 381-1977

2. IEEE Standard 344-1975, and the requirement to produce and furnish the equipment "under an approved QA program that complies with 10 CFR 50, Appendix B"

The Foxboro Company Quality Assurance Program is governed by Foxboro document CQA-2. This document was reviewed by the staff during the audit inspection and found acceptable for the upgraded RPS components. It is utilized throughout various Engineering Operating Procedures. Based on the Foxboro Company Quality Assurance Program and the above specification quality requirements, the hardware satisfies the quality requirements of IEEE Standard 603-1980.

5.2.2 Software

RG 1.152 specifies that ANSI/IEEE-ANS-7-4.3.2-1982 is the basis for the staff review of digital systems after 1985. Section 4.1 of ANSI/IEEE-ANS-7-4.3.2-1982 addresses the software development plan. Selected portions of IEEE Standard 730.1-1989, "IEEE Standard for Software Quality Assurance Plans," have been used by the licensee to describe and document its compliance to Section 4.1 of ANSI/IEEE-ANS-7-4.3.2-1982. The software portion of this upgrade can be divided into two parts: (1) Executive and Control Block algorithms running on the control cards, and (2) data used to configure the specific functioning of the Executive and Control Block algorithms which is developed and maintained by the hardware vendor, packaged as firmware (PROM), and cannot be modified by the licensee. The licensee may, however, set up and modify configuration files that control how the firmware operates. The process of assuring the quality of the software, therefore, involves looking at (1) the vendor's software life cycle for the Executive and Control Block firmware, (2) the mechanisms utilized by the licensee for establishing configuration requirements, and (3) the means for verifying and maintaining change control of that configuration. The quality of the configuration management process used to create and maintain the data fed from the configurator to the control cards is addressed in Section 5.11 of this report. The remainder of this section discusses the quality of the vendor-supplied firmware.

The vendor's software development process was previously audited by the NRC for the Haddam Neck RPS upgrade. Several aspects of the process were noted at that time including lack of independence during reviews and inadequate documentation of the organizational structure for review of test results, and follow up actions taken as the result of the reviews. These concerns were subsequently resolved as discussed below:

Methods used to assess software quality included (1) review of the licensee-provided Qualification Compliance Report (Vendor's Standard CES 281) which describes how each of the applicable portions of ANSI/IEEE-ANS-7-4.3.2-1982 and IEEE Standard 730.1-1989 were met, (2) review of the documents referenced in this report, and (3) follow-up interviews with vendor personnel, as needed. Information provided in the Qualification Compliance report served as a guide to the documents and processes reviewed.

According to ANSI/IEEE-ANS-7-4.3.2-1982, Section 3.2, the requirements for safety systems utilizing software shall be documented and verified. Some 12 areas are defined that require specification. The vendor's functional specification for the SPEC 200 MICRO CCA Control Card Software along with the design documentation was examined. As augmented by various other formal documents, all areas requiring specification were properly documented. The

sign-off and review history for these specifications was also examined and found acceptable.

According to ANSI/IEEE-ANS-7-4.3.2-1982, Section 3.3, the requirements for the integration testing shall be documented and verified. Hardware and software integration testing, in the case of this upgrade, refers to both the vendor testing done during the development of the control card hardware and software, and the testing of the configured system. The test plan for the software was developed prior to release by the vendor and executed at that time, but the results of the test were not formally documented. To rectify this, the vendor re-ran the test procedures as documented in the Foxboro Report 92-9024, "Evaluation of SPEC 200 MICRO Control Card and SPEC 200 MICRO Displays," May 1992. This factory acceptance test has been designated by the licensee as the hardware and software integration test procedure for acceptance of the software and hardware.

ANSI/IEEE-ANS-7-4.3.2-1982, Section 4.0, specifies that the software development process shall consist of several phases including, as a minimum, a development plan phase, a design phase, and an implementation phase. Verification of each phase is required. Compliance to the general requirement relating to the development plan has been demonstrated through compliance to IEEE Standard 730.1-1989. Section 3.3 of IEEE Standard 730.1-1989 requires that the project management be described in terms of organization, tasks, and responsibilities. This information was reported in the Qualification Compliance Report. The vendor resolved the independence issue that surfaced during the Haddam Neck review by redoing the questionable walkthroughs and tests. In all cases, the repeat reviews included individuals outside the program development team.

Section 3.4 of IEEE Standard 730.1-1989 specifies that the documentation governing the development, V&V, use, and maintenance of the software be identified, as well as the methods for checking the accuracy of that documentation. Included in the list of minimum documents to be identified are software requirement specifications, software design descriptions, software V&V plans, software V&V reports, and user documentation. Details relating to each of these types of documentation are adequately provided in the Quality Compliance Report as well as in Foxboro Report QOAAE03. Appendix C of QOAAE03 includes a listing of documents, walk-through dates, reader, and recorder. It should be noted that the types of documentation that were produced and maintained for the SPEC 200 MICRO do not match exactly with the names called out for the documents in the standard; however, the staff confirmed that their purpose and function as described in the Qualification Compliance Report was equivalent to the criteria of the standard. Of particular note was the lack of a software V&V plan during the original software development. As explained in QOAAE03, the development team did follow an organized methodology to verify and validate the software developed. A recently released report of the software V&V was provided, as noted in Foxboro Engineering Document EDO2134, Revision C.

Section 3.5 of IEEE Standard 730.1-1989 provides criteria for software design as detailed in the Quality Compliance Report. The vendor's corporate engineering standards were in place from the inception of the project,

including Corporate Engineering Standards (CES) 281:18, 19, 22, and 24 and CES 280:1. The Qualification Compliance Report also describes how well the vendor complied with these standards, practices, and conventions. During the staff review, an entire software function (thread) was traced for the GATE, SSEL, and RAMP algorithms to verify that the above CES actually existed and were followed during the software design. CALC, ALRM, and LLAG algorithms were previously reviewed by the staff during the Haddam Neck review. In the case of the standards regarding vendor technical reviews, there appeared to be less than adequate compliance, especially in the completion of review documentation and correspondence. However, the reviews themselves appeared to be properly conducted, as ascertained by direct interviews with one of the reviewers and the supervising managers. Several of the vendor's quality assurance standards have been upgraded recently, including CQA 3.3.1 to require more detailed documentation. The vendor, in response to the previous audit findings of inadequate documentation and independence, re-performed a number of the software walkthroughs to confirm its adequacy.

Section 3.8 of IEEE Standard 730.1-1989 provides guidance on documentation of software problems. The staff verified compliance with these criteria through interviews with the vendor's staff and review of the problem report and release list included in the SPEC 200 MICRO Panel System Test and Evaluation Report. The latest problem report was dated May 10, 1987. The problem identified in the May 10, 1987, report was corrected in release version SA-11 which was released in May 1987.

Compliance with the criteria of Section 3.9 of IEEE Standard 730.1-1989 concerning software V&V is detailed in the Qualification Compliance Report. Several reports produced through the use of the V&V tools discussed in the report including the Duane Growth Concept (Foxboro Report Number 87-SRR-001F, "Control Card Software," February 1987) and the McCabe Cyclometric Complexity Index (Foxboro Report Number 87-SRR-008F, "Software Complexity Analysis") were reviewed as was the overall description of the methods for performing white box testing (Foxboro Report QOAAE03 Revision B, "SPEC 200 MICRO Software Validation and Validation," October 1988).

Sections 3.10, 3.11, and 3.13 of IEEE Standard 730.1-1989 which contain criteria on the software change process are governed by Foxboro standards CES 281:15, CES 281.11, and CES 280:20, respectively. The general change and document control process used by the vendor was also discussed with vendor representatives. No problems were noted and the vendor's procedures were properly exercised.

As described above, the staff verified the existence of the referenced software documentation and compliance to standards through a systematic trace (thread audit) of the documentation relating to the GATE, SSEL, and RAMP control algorithms. Problems were found with the accuracy and completeness of some of the record-keeping in terms of dates, times, and findings of various walkthroughs. However, when problems were noted during the reviews, there appeared to be a complete documentation trail to prove that those problems had been adequately addressed and the necessary changes incorporated in the specification, design, or code as appropriate.

At a higher level, the staff assessed the corporate attitudes and climate relative to the importance of ensuring software quality. Interviews were conducted with various project members, project leaders, and quality representatives. These personnel were asked to discuss their views and attitudes regarding software quality. Without exception, those interviewed demonstrated a good awareness and an internalized commitment to corporate quality standards and procedures and the importance of that commitment. Some personnel were very aware of national quality trends relative to software engineering and are working to incorporate the latest concepts and approaches into their work. The staff was made aware of several upgraded vendor quality standards and found no evidence of forces or trends that would undermine the future quality of the software. The staff finds that acceptable quality assurance is provided for the RPS upgrade.

5.3 Equipment Qualification

Section 5.4 of IEEE Standard 603-1980 provides criteria for equipment qualification. Qualification of Class 1E equipment is accomplished by meeting the criteria of IEEE Standard 323-1974. The qualification of safety system equipment is established by type test, previous operating experience, analysis, or a combination of these methods. Qualification ensures the capability for system hardware to meet the performance requirements specified in the design basis.

The RPS equipment is located in the control room which is a mild environment. The purchase specification lists the qualification temperature range as 0°C [32°F] to 50°C [122°F] at ambient pressure. The humidity ranges between 10 percent and 90 percent. The maximum post-accident dose of radiation is specified at 1E+4 Rads, total integrated dose.

The staff identified a discrepancy in that the equipment manufactured by Foxboro is rated for operation down to 5°C [41°F] rather than the 0°C [32°F] specified lower limit. Per the Updated Final Safety Analysis Report (UFSAR), the control room normal ambient environment is maintained at 75°F±15°F [23.9°C±8.3°C]. Heat rise occurs within the RPS instrument racks due to their operation. Because of the controlled environment and the rack heat rise, it is unlikely that the ambient temperature at the RPS equipment will drop below 5°C [41°F]. Therefore, the lower operating limit of 5°C [41°F] is acceptable.

Heat rise testing within cabinets similar to the D. C. Cook AMCO instrument racks was documented in Hurst Engineering report 2985-HEI-05. That testing showed a maximum heat rise of 9°C [48.2°F] within the AMCO rack. That, when added to the maximum control room ambient temperature of 50°C [122°F] specified in the UFSAR is within the qualification temperature limit tested for the Foxboro equipment (60°C [140°F]). Therefore, the Foxboro equipment is suitable for operation within the D. C. Cook control room temperature limits. Additional margin is realized since the normal ambient upper limit of the control room temperature, per the UFSAR, is 90°F [32.2°C].

Seismic qualification was established by type testing of the Foxboro components and analysis of the Foxboro equipment in the existing racks. The qualification testing encompassed both the operating basis earthquake and the

safe shutdown earthquake acceleration values for the D. C. Cook Nuclear Plant site. The following standards and criteria were used to establish satisfactory seismic qualification: IEEE Standard 344-1975; IEEE Standard 381-1977; NRC RG 1.100, "Seismic Qualification of Electrical Equipment for Nuclear Power"; IEEE Standard 420-1982.

The seismic qualification testing and analysis is documented in Foxboro Type Test Report QOAAB01 and Hurst Engineering Reports 2985-HEI-07 and 2985-HEI-08. The materials inspected during the audit document the capability of the Foxboro SPEC 200 MICRO components installed in the AMCO instrument racks to remain functional before, during, and after an operating basis and safe shutdown earthquake at the D. C. Cook Nuclear Plant.

Voltage surges in the digital RPS can occur as the result of lightning, switching transients, electrical faults, and other fast transients. Testing for surge withstand capability was specified by the licensee to meet the criteria of IEEE Standard 472-1974. However, testing per Foxboro Test Plan IT-220, which was completed in June 1993, follows the criteria of more recent standards such as ANSI/IEEE Standards C62.41-1991 and C62.45-1987. The testing covers electrostatic discharge, common mode rejection, normal mode rejection, high frequency transients, surge withstand capability, and lightning effects. The staff confirmed that the proposed testing methodology is acceptable to demonstrate surge withstand capability. The current injection method of testing for electrostatic discharge, ranging between 2 kVdc and 6 kVdc, was applied to operator accessible surfaces. The staff reviewed the surge withstand capability test results documented in IT-22A, Rev. 0, dated July 16, 1993, and found the results acceptable.

Surge withstand capability will be tested at 2.5 kVdc for common mode surges and at 1.5 kVdc for normal mode surges, at a burst frequency of 120 Hz for two seconds. Lightning effects will be simulated by 0.5 kVdc and 1.0 kVdc in the normal mode and 1.0 kVdc and 2.0 kVdc in the common mode on the system. Electromagnetic and radio-frequency interference withstand capability is discussed in Section 5.15 of this report.

The replacement of wiring and cables is minimized by the design of the RPS upgrade project. Replacement equipment is to be mounted in existing instrument racks. The licensee committed that any replacement cables with splices and connections will comply with the criteria of IEEE Standard 383-1974.

The staff finds that the upgrade of the D. C. Cook RPS with Foxboro SPEC 200 modules has been demonstrated to meet applicable equipment qualification requirements, and the system is, therefore, capable of acceptable operation in the anticipated environmental conditions.

5.4 System Integrity

Section 5.5 of IEEE Standard 603-1980 specifies that a safety system be designed such that it accomplishes the safety function under the full range of applicable design basis conditions (system function). The RPS upgrade to install Foxboro equipment updates the components of each of the four channels

and does not affect the original system functional design or logic. The system integrity is maintained with this upgrade of system components. Therefore, the requirements of Section 5.5 of IEEE Standard 603-1980 are satisfactorily met.

5.5 Independence and Physical Separation

Section 5.5 of IEEE Standard 603-1980 also specifies a design where (1) there is independence and physical separation between redundant portions of a safety system, (2) there is independence and physical separation between the safety system equipment and the effects of a design basis event, (3) there is independence and physical separation between safety systems and other systems, and (4) a single failure in a non-safety system will not cause a design basis event which negates the safety system function designed to mitigate that event. There are specific requirements on the classification of equipment, isolation between safety system equipment and non-safety system equipment, and separation from (barriers between) safety system equipment and non-safety equipment.

The D. C. Cook Plant has a drawing control program that controls the physical equipment layout, design analysis and evaluations, adjustments, calculations, and system configuration. Foxboro designed the RPS replacement components into the existing system consistent with the plant drawing control program. The Foxboro design responsibilities included functional, rack loading, wiring, termination, and power supply drawings, along with database configuration information. The database configuration information includes the Configurator settings for the SPEC 200 MICRO modules as discussed in Section 5.11 of this report.

To confirm acceptable provisions for system isolation. the staff examined an N-2AO-V2H voltage to current (V/I) isolator. This module is a custom factory modification of a standard V/I converter. Power supply isolation is added to the circuit board. This allows the module to withstand a maximum credible fault, as documented in Foxboro Report 92-0029a. Testing of the RPS modification included the application of (1) grounded output leads, (2) 250 Vac rms at 60 Hz from both output leads to ground, (3) 250 Vac rms at 60 Hz across the output leads, (4) 480 Vac rms at 60 Hz from both output leads to ground, and (5) 480 Vac rms at 60 Hz across the output leads. System isolation is provided for the safety signal to non-safety uses such as control room displays. The testing satisfactorily demonstrated that the module meets the isolation criteria of Section 5.6.3.1 of IEEE Standard 603-1980.

The Foxboro equipment is being installed in the existing RPS instrument racks. The Configurator is physically remote from the RPS cabinets and is not connected to any module in the RPS racks. The staff finds that acceptable independence and separation are, therefore, maintained per the criteria of IEEE Standard 603-1980.

5.6 Capability for Test and Calibration

Sections 5.7 and 6.5 of IEEE Standard 603-1980 contain specific criteria regarding safety system equipment testing and calibration. Testing of Class

1E Systems should be accomplished in accordance with the guidance of ANSI/IEEE Standard 338-1977.

The capability for periodic testing and calibration is retained in the Foxboro SPEC 200 MICRO instrument upgrade. The test panel supplied with new equipment will provide comparable capability for test and calibration utilizing present manual methods and permanently installed test facilities very similar to what has been in use with the existing H-Line equipment. In fact, additional test points are provided with the new system to enhance in-place testing and calibration of rack mounted components.

The SPEC 200 MICRO control cards are individually removed from the instrument rack for configuration and calibration. The control card is configured using a personal computer (PC) with Foxboro configuration software (Configurator). This software provides menu-driven "fill-in-the-form" monitor displays for entry of initial settings. The initial settings (configuration) for each channel, including ranges, setpoints, deadband, and lead/lag functions, are downloaded to the control cards as required for each function using the menu-driven displays and the PC keyboard. Once the configuration is complete, the Configurator is disconnected from the control card. The control card is then reinstalled in the instrument rack for service. An on-board lithium battery maintains the installed configuration while the control card is in transit.

Channel Functional Testing will be accomplished utilizing present manual methods and installed test facilities due to the similarity in channel architecture between the original and modified system. The licensee plans to use existing H-Line equipment procedures with minor changes to perform Channel Functional Testing.

By letter dated December 22, 1993, the licensee responded to a concern regarding overlap testing. The licensee stated that the first rack test point is the key overlap point and the loop current is monitored at each calibration test segment. The test program results in a total end-to-end loop check through overlapping. The licensee stated that this test methodology is the past and current D. C. Cook plant practice and is common for the industry. The licensee further stated that the test point resistor tolerances do not impact loop accuracy or performance. There are no effects caused by test point resistor tolerances because these effects are calibrated out as a result of the system design and the D. C. Cook plant calibration methods. Test point resistor tolerances are invisible to the operators and to the performance of automatic actuation functions.

The staff finds that the test and calibration capability and procedures are acceptable, and in conformance with the criteria of IEEE 338-1977.

5.7 Information Display

Section 5.8 of IEEE Standard 603-1980 addresses the criteria for safety system information displays. These criteria encompass information displays for system status indication, bypasses, and manually controlled actions. Displays for manually controlled actions must also be in accordance with the guidelines of RG 1.97, "Instrumentation for Light Water Cooled Nuclear Power Plants to

Assess Plant and Environs Conditions During and Following an Accident," for post-accident monitoring instrumentation.

The proposed RPS upgrade contains no new information channel displays, and the existing displays were not disturbed. The existing information displays included in the D. C. Cook RPS design have been previously reviewed and approved by the staff.

5.8 Control of Access

Section 5.9 of IEEE Standard 603-1980 addresses the criteria for administrative control of access to safety equipment. Administrative control of access to the SPEC 200 MICRO equipment is provided by physical access control of the installed equipment, to configuration hardware, software, and data. The RPS cabinets are kept locked and the keys are under administrative control. Configuration hardware, software, and data are controlled via plant procedures and policy.

The administrative control of access to the Foxboro hardware, software, and data was reviewed by the staff. The staff determined that all hardware, software, and configuration changes are adequately controlled through approved procedures. The procedures include reviews and sign-offs to ensure that the impact of all changes are properly implemented throughout all plant operating aspects (e.g., procedures, training, drawings, maintenance, and testing).

The Foxboro RPS modules are located in existing instrument racks that have key-locked doors. The existing equipment in those racks will be removed, except for the terminal blocks and the field wiring connected to those terminal blocks. Any rack door that is open causes an annunciator to light in the control room (one annunciator module per RPS channel). The control room itself has restricted access. Work done on the RPS is controlled and administered by procedure and key control. While there are zero and span adjustments on the Foxboro SPEC 200 analog modules, access to those modules is controlled. The Configurator is physically remote from the RPS cabinets and is not connected to any module in the RPS racks. The staff finds that acceptable access control to the RPS is provided.

5.9 Identification

Section 5.11 of IEEE Standard 603-1980 addresses the criteria for the identification of safety system components and associated documentation. The distinct identification for each redundant portion of a safety system is to be in accordance with the guidelines of IEEE Standard 384-1977 and IEEE Standard 420-1973. In addition, the associated documentation is to be distinctly identified in accordance with the guidelines of IEEE Standard 494-1974.

The licensee has committed to retain channel identification consistent with the channel identification of the original H-Line equipment. Redundant channel cabling is color coded, and the RPS instrument cabinets are appropriately labeled in accordance with the above IEEE standards. New identification labels will be installed at the nest and rack level for all new

equipment. The licensee also stated that components with dedicated functions, not interchangeable with other components will be distinctly labeled to ensure configuration at the component level. Drawings, procedures, and references are to be updated to reflect new equipment at the rack, nest, and component level upon installation.

The new RPS cabinets were inspected by the staff in the plant shipping/receiving area prior to equipment installation. The plant identification labels and color coding on the cabinets and components were determined to be acceptable. The labels are clearly legible and consistent with plant documentation and drawings. Color coding was implemented on a channel level as well as train level, which is consistent with the original plant design, and is, therefore, acceptable to the staff.

5.10 Auxiliary Supporting Features

Section 5.12 of IEEE Standard 603-1980 has specific criteria regarding the use of auxiliary supporting features. IEEE Standard 603-1980 defines an auxiliary supporting feature as systems or components which provide services (such as cooling, lubrication, and energy supply) that are required for the safety systems to accomplish their safety functions. The RPS instrument racks at D. C. Cook have open mesh screening at the top of the cabinets and louvers in the rear door. These features support natural circulation of the control room air for component cooling by convection. The Foxboro RPS equipment used at D. C. Cook does not require forced circulation (cooling fans) or lubrication.

5.10.1 Lithium Batteries

One lithium battery is used in each SPEC 200 MICRO module. The sole function of each battery is to retain the RAM [random access memory] configuration of the associated microprocessor when the module is without normal power. The primary battery function is to retain the software configuration when the module is in transit from the RPS instrument racks to the Instrument Calibration Lab for configuration or maintenance and in transit back to the instrument racks. The battery also retains the software configuration when there is a momentary power loss, such as the few milliseconds involved during the transfer of power between the normal inverter-supplied power and the backup ac power source. Documentation provided by the licensee states the CMOS chip memory is guaranteed at supply voltages of 2 Vdc or higher.

Lithium batteries have an inherent long life in standby applications due to the chemical composition of the battery. The lithium electrolyte construction is ideal for memory backup power applications such as this where the battery is essentially unloaded for more than 99 percent of its life. In particular, the licensee stated that the three volt lithium battery cell used in this application is able to provide required memory retention for 15,000 hours if the cell is new. Memory is retained for a minimum of 1,000 hours when the cell reaches the low voltage threshold. This threshold is continuously monitored by the SPEC 200 MICRO module. A light emitting diode (LED) is illuminated when the battery has less voltage than the threshold being monitored. It was noted that the SPEC 200 MICRO modules are shipped with the batteries removed, and the batteries are shipped separately.

As each battery is installed, its serial number, lot number, and installation date are included in a database. Surveillance procedures call for monitoring the battery status and will direct replacement of the battery before the useful battery life expires. Additionally, routine preventive maintenance will replace the batteries before the end of useful battery life as necessary. Through the use of the database, trends in battery performance can be observed. The staff finds the procedures associated with the lithium batteries to be acceptable for maintenance and surveillance.

The batteries were tested using Foxboro test procedure BT-180A. The test demonstrated acceptable battery characteristics when the battery terminals were shorted or when the battery was installed in reverse polarity. The fresh battery had the same potential when loaded or unloaded. The SPEC 200 MICRO module performed as though the battery was not present when it was installed with reverse polarity. With the battery terminals short circuited, the battery temperature rose to 262°F [127.8°C] after 7 minutes. The voltage dropped significantly, but the battery holder was not damaged. However, the plastic coating of the battery was discolored and partially melted. With the short circuit removed, the battery voltage recovered. A second test obtained similar results.

The staff reviewed the test results and finds that the lithium battery does not pose a significant ignition or explosion hazard. The SPEC 200 MICRO module continued functioning as designed even when the backup battery was short circuited. The SPEC 200 MICRO module does not need the battery for operation, but only for transport memory retention. With no backup battery, the module represents a channel trip when power is restored. With no power, a channel trip occurs due to the output signal going to a fail-safe condition. Thus, the staff concludes that the lithium batteries are acceptable as an auxiliary supporting feature.

5.10.2 Power Supplies

Each D. C. Cook RPS protection set will be equipped with new Foxboro power supplies. The transmitter instrument current loops will have 75 Vdc supplies. Each protection set will have Foxboro Model PO300CQ power supplies. The output of each power supply is diode-auctioneered to a common transmitter power supply bus. Each protection set channel will have an installed, in-service, spare power supply. The failure of any one power supply does not affect the proper operation of the RPS protection set channels. Power to the power supplies is from the existing station 120 Vac power sources.

The signal processing rack mounted instrument modules have a similar power source arrangement. The power to these instrument modules is ±15 Vdc. Each RPS channel has Foxboro Model 2ARPS05 linear, series-pass ±15 Vdc power supplies that are diode auctioneered to the nest power distribution buses. Each protection set channel will have an installed, in-service, spare power supply. The failure of any one power supply does not affect the proper operation of the RPS channel. Power to the power supplies is from the existing station 120 Vac power sources.

The circuit breakers feeding the instrument (transmitter and rack mounted) power supplies will each be rated at 20 amperes, which is capable of powering all connected loads. However, due to the filter capacitors on the output of the power supplies, the inrush current may exceed 50 amperes if not controlled. This could cause nuisance tripping of the circuit breaker and transfer of the solid-state transfer switch or current limiting of the inverter. To address this possibility, the design incorporates a 2.5 ohm resistor in series with the power leads. A time delay-upon-energizing relay operates contacts that bypass the resistor after 2 seconds. These components were purchased as Class 1E. A control switch is manually operated, resetting the current limiting circuit, per operating procedures prior to energizing the channel to prevent a current inrush the next time the cabinet is energized. The staff reviewed the procedure entitled "Foxboro Protection Rack Inrush Current Control Function Verification," 12IHP6030.IMP.015 Rev 0 to verify functionality of the inrush current limiting circuits, and finds it acceptable. Performance of this procedure assures that the inrush current control circuit performs its function properly. The licensee is developing procedures which will require I&C personnel to reset the current limiter and perform the functionality checks each time power is restored to the RPS cabinets. This is acceptable to the staff.

The existing station 120 Vac power sources have adequate capacity to provide power to the new Foxboro power supplies. Should the solid-state transfer switch change from normal inverter power to the alternate regulated 120 Vac power, that transfer occurs in one-quarter cycle (less than 5 milliseconds). The cycle time of the microprocessor is 200 milliseconds. The filter capacitors in the dc power supplies will maintain power for this brief switching interval. No degradation of signals, configuration, or output occurs during this switching transient. For a longer power outage, such as when the alternate regulated 120 Vac is in service and there is a loss of offsite power, the lithium battery will maintain the configuration of the microprocessor. The clock cycle resumes when power is restored, and the outputs are driven to the state required by the configuration and the input signals. Loss of power to the solid-state protection system, where the individual channel trip signals are combined into reactor trip signals is already a postulated event and not affected by this modification. Any required reactor trip would occur. The staff finds the power supply systems acceptable auxiliary supporting features.

5.11 Configuration Management

The Configurator application (software used to create the configuration data that is downloaded to the SPEC 200 MICRO control cards to specify the functions performed and the input and outputs to each function), developed by the vendor, was reviewed by the staff. This configuration software is not considered by the vendor to be safety grade because it is utility-specific software that does not run on the RPS operating equipment. It runs under MS-DOS, and its only product is data that can be otherwise verified. Despite these assertions, the staff audited the Configurator software development process in the same way the operating system firmware residing in firmware modules was audited because of the importance of configuration data to proper system operation. No differences in the requirements and design

documentation, review, testing, or change control processes were noted. The only potential deficiency noted was a lack of regression testing. Specifically, when a new version of DOS is released, the configuration data should be evaluated to confirm that the new version of DOS does not affect the data. However, the licensee committed, in the September 1993 audit, to freeze DOS at Version 5.0, thus precluding the need for regression testing.

The purpose of the Configurator is to create configuration files that can be downloaded to the appropriate control cards. The engineering information driving the configuration data was derived systematically by the vendor from current plant drawings. The vendor analyzed the original use of H-Line analog equipment and designed a set of control cards using Control Blocks to produce the same functionality. The licensee then verified each of these new drawings to ensure that design equivalence was obtained.

Failure of the Configurator to properly store, verify, print, or archive data or the random occurrence of an undetected corruption of a data disk could lead to the downloading of incorrect configuration data to individual control units. To deal with this concern, the channel calibration parameters (configuration), including setpoints, are to be independently verified by periodic surveillance and post-maintenance testing following data downloading from the Configurator. A walkthrough of the procedures for using the Configurator was provided by the licensee. The staff reviewed the administrative controls to be placed on its use. Independent configurators are supplied for Unit 1 and Unit 2. Each unit has its own dedicated Configurator mounted in a lockable cabinet along with the applicable interface equipment and a printer. The Configurator cabinets are color coded and will be located in separate rooms near the I&C Maintenance Shop to ensure Unit 1 and Unit 2 integrity. A PC is installed in the cabinets for configuration use.

The cabinets are kept locked, except when in use. The keyboards are keyed separately and are also kept locked. The keys are in a locked key box with authorized access under administrative controls. When an Engineering Control Procedure dictates that a change should be made to a control card, the individual responsible for maintaining the configuration will first update the database on the PC Hard Drive using the Configurator, then print a hard copy of the changes on the printer installed in the cabinet. The exact same changes are then made on the other unit's Configurator PC Hardware Drive by accessing the backup database, implementing changes, and printing a hard copy of the changes. Also, two backup floppies are created after each configuration change is made. One floppy is sent to AEPSC Corporate Office and the other is stored at the plant under administrative control.

Two procedures govern the use of the Configurator for modifying the Foxboro control cards. The high level procedure (D. C. Cook Plant Procedure MHI-6030 "Administrative Control Policy For Instrument Configurators," September 1993, Rev. 0) covers aspects of the Configurator control packages and applies at the Configurator Cabinet level. The low level procedure for the Foxboro Configurator (D. C. Cook Draft Plant Procedure 12IHP6030.CFG.002, "Configuration of Foxboro Spec 200 Micro Control Card") provides step by step instructions for accessing the right program, making changes, and verifying

changes. The high level procedure has been approved but the low level procedure was in draft form during the audit. Both procedures contain the appropriate content and level of detail. Most importantly, both demonstrate the appropriate formality and commitment to control that is required. The staff finds that acceptable configuration management is provided.

5.12 Human Factors Considerations

Indications of the status of the Foxboro digital RPS are provided to the operator. The SPEC 200 MICRO control cards have three indicator LEDs. The indicator to the right of the battery is red when the battery is low. The other two LEDs are immediately below the battery. The STBY/CONT LED is normally steady green and indicates normal operating conditions. A blinking green indicates a STANDBY condition. The FAIL indicator, is a steady red in FAIL condition, and a blinking red in ERROR STANDBY condition. It is normally off. The control cards are mounted in racks with doors. During normal operations, these indicator LEDs are not observable and only the green LED is on. The STBY/CONT and FAIL LEDs are of particular use during the downloading of the configuration data from the Configurator and in diagnosing unanticipated behavior during plant operation or surveillance testing. During regular surveillance activities, the plant personnel will open the cabinets to observe the battery indicator LED as well as the STBY/CONT and FAIL LEDs.

Regarding the potential for mixing up the control cards, the plant representatives indicated that only one card would be configured at a time, and that all configuration activities would be done at a dedicated workbench. Before new or modified configuration data can be downloaded to a control card, that card will be removed from the nest and rack and placed on a workbench where the stand-alone PC used as the Configurator and the display module are placed. The control cards are labeled and will be properly returned to their nest and rack before another card is pulled for configuration. Post-maintenance testing procedures, and administrative controls such as component, rack and nest identification labeling are also in place. The staff finds that the above practice provides acceptable control of the configuration process.

5.13 Software Reliability

Software reliability, a measure of how well a software system provides the services expected by its users, is built into a product through use of quality assurance including V&V during the development process. Software metrics (methods of quantifying aspects of the process or products of software development) have been developed to aid in the measurement of software system characteristics (such as reliability, maintainability, and efficiency), processes, and documentation. Some key reliability metrics include mean time between failure, rate of fault occurrence, probability of failure on demand, and availability. Other metrics combine two or more of these basic metrics to model the reliability growth of a system. These metrics can be used to predict when a particular level of reliability is attainable.

The growth model used by the vendor to mathematically summarize the fault data collected regarding the SPEC 200 MICRO software was the Duane Growth - Error Rate of Change as summarized in a report dated February 18, 1987. The Duane

Growth model not only yields an estimate of the rate of change of errors, but estimates the time to nest error and the number of errors expected in the near future. It utilizes the cumulative detected software defect rate during testing and the accumulated central processing unit operational time. Two other reliability metrics were noted in the Qualification Compliance Report: the Software Error Discovery Rate and Software Error Pareto Profile. The results contained in this report indicate that the software is acceptably reliable.

Availability data, coupled with the fact that the last problem report was received in 1987, would also indicate that the SPEC 200 MICRO firmware constitutes a highly reliable software product. Vendor representatives presented data to the effect that over 30 nuclear facilities and 400 non-nuclear facilities have installed over 14,000 SPEC 200 MICRO modules. The staff finds that these data demonstrate that SPEC 200 MICRO modules are highly reliable, and are, therefore, acceptable.

5.14 Grounding

Electrical noise is an important consideration in analog and digital instrumentation as well as signal conversion systems. Proper grounding of instrumentation circuits and equipment minimizes the potential for electrical noise affecting system operation. The D. C. Cook Nuclear Plant grounding practices and equipment grounding methods were evaluated by Hurst Engineering in Report 2985-HEI-02, "Engineering Analysis of Grounding Issues," Revision 2, December 15, 1992. Redundant ground return paths using #4/0 copper conductors are provided for each RPS instrument rack to the plant grounding mat. The grounding mat provides a common ground reference point throughout the plant. Redundant connections to ground are used, with precautions taken against forming ground loops. The RPS power supplies will be connected to operate with the output power ungrounded. The power supplies are each grounded to the rack ground bus bar. The staff finds that acceptable grounding provisions are provided.

5.15 Electromagnetic and Radio Frequency Interference

Electromagnetic compatibility is the capability of an electronic system to operate at design levels of accuracy and efficiency in an environment where EMI or electrical noise exists. Similarly, RFI is any spurious voltage or current that appears in an instrument circuit due to a radio frequency signal in the instrument environment. EMI and RFI can either obscure valid signals or generate non-valid signals. Instrument design should negate any internally generated interference and be resistant to external EMI and RFI.

The replacement RPS equipment will be mounted in existing RPS instrumentation racks in both control rooms at the D. C. Cook Plant. The control room environment was tested for the presence of electromagnetic fields and radio frequency signals (Report 2985-HEI-03, Preliminary EMI/RFI Evaluation, AEPSC Reactor Protection and Control System Replacement Project, Hurst Engineering, Revision 0). EMI/RFI surveys were conducted in each control room. Sources of EMI/RFI were researched for areas within 50 miles of the plant. The evaluation of interference sources took credit for the shielding inherent in

the control room construction (grounded steel rebar in the concrete walls, floor, and ceiling). The actual field measurements validated that assumption.

Supplemental EMI/RFI testing was performed by the licensee. The site-specific requirements for this EMI/RFI testing were established consistent with the general guidance on test methodology in Military Standard 461C, "Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference," April 1, 1980, and Military Standard 462, "Electromagnetic Interference Characteristics, Measurements of," July 31, 1967, with later notices on applications. Surveys indicated slightly higher amplitude signals in the D. C. Cook, Unit 2 control room compared to the Unit 1 control room. Much of the EMI/RFI in the control rooms is generated and radiated from within the control room due to power supplies and lighting. Plant communication (radio) signals are attenuated by the control room structure. Use of radio transmitters inside the control room is prohibited and controlled by administrative procedures. The results of this supplemental testing were provided in Test Report 60214-94N, Rev. 1, "Main Control Room Mapping Data and Process Control System EMI." Satisfactory results for EMI were demonstrated.

Factory testing of the Foxboro SPEC 200 dual MICRO modules indicated that they emit RFI between 50 MHz and 200 MHz. At 1 meter from the surface of the control card, the field strength was less than or equal to 0.00316 volt/meter throughout the frequency range. The control room existing EMI/RFI field strength peak is at 1.5849 volts/meter at frequencies below 50 MHz. Between 50 MHz and 200 MHz, the measured field strength was between 0.0178 volt/meter and 0.0316 volt/meter. Because of these low noise values, the upgraded system is expected to have no undesired effects on the existing electronic equipment.

The factory test included both conducted and radiated susceptibility using test methods from MIL-STD-462. No anomalies were noted. The staff finds that the above described testing provided confidence in the capabilities of the installed configuration to be sufficiently immune to EMI/RFI, and, therefore, this issue has been acceptably addressed.

5.16 Testing

Functional testing of the completed RPS modification is necessary to ensure that the system is designed and will function as intended. The licensee's overall testing program is summarized in Report 2985-BJB-01, "Test Program Summary," December 10, 1992, Revision 0.

The licensee's overall testing program for the RPS upgrade includes factory acceptance tests, integration tests, installation tests, surveillance tests, and time response tests. All types of testing, except the surveillance tests, are discussed in the following paragraphs. Periodic surveillance testing is discussed in Section 5.6 of this report.

5.16.1 Factory Acceptance Tests

The staff examined the factory acceptance test procedure (TP-150 Revision 2, Foxboro Factory Acceptance Test Procedures for the Upgrade of the Reactor

Protection Process Instrumentation), witnessed portions of the test, and reviewed selected test data. System checkouts and tests are performed under Foxboro Engineering Operating Procedures (Foxboro Engineering Operating Procedure EOP-201 Revision D, "System Checkout and Test of Nuclear Orders with Commercial Grade Equipment," October 29, 1991, and Foxboro Engineering Operating Procedure EOP-202 Revision C, "System Checkout and Functional Test of Nuclear Orders with Qualified Equipment," October 29, 1991). Foxboro had completed its factory acceptance test, prior to the staff review. However, personnel from D. C. Cook were repeating the test while the staff review was underway. The licensee's tests were conducted on the factory assembled instrument racks with the same physical layout as that designed for the installation in the D. C. Cook control rooms. The instrument modules and power supplies tested were identified as the equipment to be shipped to D. C. Cook Nuclear Plant.

The factory acceptance test verified the equipment serial numbers, including power supplies, and verified equipment operability before packaging for shipment. The test procedures were sufficiently detailed to provide test history, notation of and resolution of anomalies, and a record of the test steps taken, test personnel, test instruments used, and the test configuration. Field inputs were simulated using current generators. The racks were wired to the design configuration for D. C. Cook. Testing verified the correctness of the test configuration, the time responses, and proper response to input stimuli. Verifications included workmanship and the physical condition of materials and wiring. The staff identified no unresolved anomalies as a result of the factory acceptance test.

5.16.2 Integration Tests

Integration tests are performed before installation, but after the equipment is delivered to the plant site. These tests ensure that the replacement RPS instrumentation will interface with the control system without adverse interaction. Portions of the control system are being upgraded concurrent with the upgrade of the RPS process instrumentation. The integrating tests call for wiring the upgraded portion of the RPS and the control systems together per design drawings. Anticipated interactions are then simulated, including power failures, ground faults, and instrument failures. The results are recorded and documented. Any anomalies are corrected before proceeding with installation.

Integration Test Procedure #2985-U21NT was reviewed and found acceptable by the staff. The test procedure was well written with clear instructions and detail. The licensee is required to provide a summary of any anomalies identified, and corrections made. This is acceptable to the staff.

5.16.3 Installation Tests

Installation tests provide, in an orderly fashion, verification of installation according to the engineering design package, instructions, and drawings. This testing includes continuity checks of the de-energized wiring, cable testing, and visual inspections and examinations versus the installation drawings. Power, grounding, field wiring, and instrument cable shielding are

verified before initial energization of the installed equipment. Trip, alarm, isolated digital outputs, and isolated analog outputs are verified to respond to input stimuli. Some instrument calibrations occur concurrent with the installation testing. Functional installation testing assures plant interfaces have been implemented properly. The licensee stated that any anomalies discovered during the installation testing will be corrected before proceeding.

5.16.4 Time Response Testing

Time response testing is part of the current technical-specification required surveillance testing. The time response is measured between a simulated perturbation in the process to the channel trip and includes all upgraded Foxboro instrumentation. The licensee indicated that the current time response surveillance procedures do not require change to accommodate the upgrade. Thus, the existing surveillance procedures are the control documents governing the time response testing of the newly installed RPS equipment.

Report 2985-HEI-01, "Summary Report for Response Time Evaluation," Hurst Engineering, November 9, 1992, Revision 0, described the results of the response time testing. The worst case published module response times for the resistance-to-current module used for OT/dT and OP/dT was 2 seconds with 400 milliseconds added as worst case for the associated SPEC 200 MICRO module. The staff reviewed the time response data recorded for the factory acceptance test using those modules. For the TBX-4116 channel, the response times were 600 milliseconds to de-energize and 900 milliseconds to energize. For the TBX-411C channel, the response times were 612.5 milliseconds to de-energize and 750 milliseconds to energize. For both cases, the response times were within the acceptance criteria.

The licensee committed, during the September 1993 audit, to continue to use the existing Channel Time Response Test Procedures to conduct periodic technical-specification required response time testing of the new RPS. Response time for the new equipment will be verified to meet the technical-specification allowable limits. The staff finds that the above described testing satisfactorily demonstrates the new RPS functional capability.

5.17 Defense-in-Depth

In order to establish an appropriate level of reliability, the protection system is to be designed using techniques such as (1) diversity in component design and function to the extent practical, (2) fail-safe configuration, and (3) simplification of design such that normal operating, maintenance, and postulated accident conditions do not result in the loss of the protection function.

Staff concerns regarding digital systems which are addressed by appropriate defense-in-depth include digital system susceptibilities to existing plant environments, the commercial dedication of digital hardware and software, onsite expertise for problem recognition and troubleshooting, the potential for common mode failures introduced by software errors and unintended functions, and software/hardware interaction problems. The staff review

verified that there is sufficient functional diversity to mitigate an accident or transient given a common mode failure of a component (hardware or software) due to these areas of concern. Therefore, the licensee was requested to provide an evaluation/analysis using the methodology described in NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection Systems," design basis to demonstrate that sufficient diversity exists to mitigate accidents and transients assuming a postulated common failure. If a safety function is disabled, then a diverse means, that is unlikely to be subject to the same common mode failure, is to be provided to perform either the same function or a different safety function. The diverse function may be performed by a non-safety system if a certain quality level is maintained. Manual actions from the control room are acceptable if the analysis shows that adequate time and information, not susceptible to RPS replacement hardware/software common mode failure, is available to the operator for diagnostics and plant shutdown.

By letter dated December 22, 1993, the licensee provided a response to the staff's concern regarding defense-in-depth and diversity in the digital system. The licensee performed a functional diversity assessment of each UFSAR event assuming a common mode failure of the software in the RPS upgrade modification. In this assessment, all the FSAR events for both Units 1 and 2 of the D. C. Cook Nuclear Plant were considered. A review was performed to divide the events into those that were potentially affected by the postulated common mode software failure and those that were not affected. The potentially affected events were then individually evaluated qualitatively in light of the FSAR analysis to ensure that adequate diverse mitigation capability is maintained.

In the licensee analysis, if the trip function is processed outside of the new digital RPS, then the trip is assumed to be available. If the trip is processed by a function that is a part of the new digital equipment, then the trip/ESF function is assumed to be lost. However, for some functions, alternate indications and/or diverse alarms are available. The alternate indications alarms that are available to the operator to mitigate the transient were given for the worst-case event. A discussion was also provided concerning the operator's response/impact on reactor safety.

As part of the defense-in-depth analysis performed by the licensee for the Foxboro digital RPS modification, the licensee evaluated diversity for the new system against the existing anticipated transient without scram (ATWS) mitigation system actuation circuitry (AMSAC) to ensure that the requirements of 10 CFR 50.62 for ATWS diversity continue to be met. The licensee's analysis indicated that diversity between the RPS modification and the AMSAC system could not be demonstrated since both consisted of digital equipment manufactured by Foxboro. Consequently, the licensee replaced the AMSAC system with a vendor-specific designed system consisting of Taylor-Mod 30 digital equipment. This modification was done to meet the equipment diversity requirement of 10 CFR 50.62. The staff finds the licensee's analysis and subsequent change to be consistent with 10 CFR 50.62 and, therefore, acceptable.

5.17.1 Common Mode Failure Analysis Results

The staff notes that various reactor trips are not affected by the installation of the new digital RPS equipment. Among these trips are neutron high flux and high rate trips, undervoltage and underfrequency trips, and reactor trip on turbine trip. For events that are affected by a postulated common mode failure in the new digital equipment, the operator will be alerted to the event by alarms and/or indication. The operator can then provide the appropriate manual action and enter into the emergency operating procedures.

The licensee's analysis indicated that for a locked rotor event, the consequences could be more severe than currently analyzed due to the longer response time assumed for the required mitigating actuation given the failure of the digital RPS. The FSAR analysis for this event assumes an instantaneous seizure of a reactor coolant pump rotor. For this event the reactor trips on low RCS flow. A common mode failure of the new digital RPS would result in the loss of the low flow reactor trip signal. As a result, manual action by the operator is the only method available for mitigating this event.

The locked rotor event evaluation indicated that the loss of reactor coolant flow will increase the coolant temperature and increase pressurizer pressure due to the reduction in heat removal. The wide range RCS pressure recorders will still be available to the operator. The pressurizer pressure will continue to rise, with the operator receiving a high pressurizer pressure deviation alarm at 2325 psia for Unit 2 and 2175 psia for Unit 1. The reactor trip on high pressure is also lost to the postulated RPS common mode failure. The licensee stated that diverse high pressure alarms will be available and will draw the operators' attention to trip the reactor manually.

The licensee stated that the locked rotor event is similar to the loss of forced reactor coolant flow in one loop but is more severe in that total core flow is reduced more rapidly to a lower value (approximately 70% in 2 seconds). As the coolant heats up, a significant increase in pressure will occur (2590 psia peak for both units). This peak is shown to occur 2 seconds after the reactor trip at 1 second. The licensee stated that this pressure is less than 110% of design pressure (2750 psia). However, if a reactor trip is delayed for approximately 60 seconds, the licensee indicated that the above design pressure may be exceeded. The licensee's analysis took no credit for operation of pressurizer spray or for the opening of the Power-Operated Relief Valves (PORVs). The licensee stated that as is the case with the loss of forced reactor coolant flow, the analysis was performed with a positive moderator temperature coefficient of +5 pcm/degrees F. This is more limiting than the technical specification limit of 100% reactor thermal power. The licensee stated that this assumption is conservative and provides substantial margin throughout core life.

As T_{avg} is increased in the analysis, power also increases. The licensee stated that a more realistic beginning of cycle Moderator Temperature Coefficient (MTC) would be -4 pcm/ degrees F. Throughout core life, the MTC would decrease to -20 pcm/degrees F. The licensee stated that the feedback from the MTC would, therefore, tend to shut the reactor down rather than increase power in an actual event. The possibility that automatic rod control could occur which would withdraw rods has no impact on the event because the rods are essentially already fully withdrawn at full power. On the basis of

the above, the licensee concluded that it is unlikely that pressurizer pressure would exceed 2750 psia and virtually impossible that it would exceed 3200 psig (the ASME Boiler and Pressure Vessel Code level C criterion).

In the licensee analysis, Departure from Nucleate Boiling (DNB) is expected to occur. In the event of a delay in reactor trip of 60 seconds, the number of fuel rods in DNB would increase. The licensee's analysis again did not assume operation of the pressurizer sprays, nor opening of the PORVs. The licensee stated that the available flow will prevent the core from degrading to a condition to where it cannot be adequately cooled after trip. The portion of the core that experiences DNB will heat up until the Doppler coefficient shuts it down. The licensee stated that it is not expected that fuel melt will occur, but cladding burst and oxidation are anticipated. The licensee stated that substantial core damage is acceptable for this postulated ANS Condition IV event with massive multiple failures.

As noted, in the evaluation of the locked rotor event, operator response to manually trip the reactor is assumed within 60 seconds. However, several pressurizer pressure alarms can be expected within seconds of event initiation including RCS acoustic monitor flow alarms since the pressurizer safety valves will lift. Therefore, the licensee indicated that operator response may occur in less than the 60 seconds assumed for this event.

The most likely cause of this event as indicated by the licensee is the failure of the reactor coolant pump or motor. The operator is provided with additional alarms of reactor coolant pump status, including bearing temperature high, lower bearing seal water temperature high, lower bearing cooling water flow low, upper oil pot level high or low, and lower oil pot level high or low. The licensee indicated that this additional information available to the operator will increase the likelihood that the operator will respond promptly to manually trip the reactor.

The calculated offsite dose for the locked rotor event for the D.C. Cook Vantage 5 fuel was 0.3 rem whole body and 3 rem thyroid. With a delay in operator response of 60 seconds core damage is increased significantly. The analysis indicated that 10 CFR Part 100 criteria will be met for this Condition IV event. In addition, the maximum hypothetical accident doses will substantially bound the locked rotor event doses.

In order to assess the adequacy of the licensee's defense-in-depth analysis, the staff weighed the safety implications of: (1) the diverse back-up actuation that will not meet the safety analysis timing requirements if a common mode failure of the digital RPS is assumed; (2) the credit that the licensee gives to diverse indication in the control room that would facilitate manual actions if a common mode failure is assumed; (3) the staff findings regarding the software V&V program; (4) the operating experiences with a similar RPS at the Haddam Neck Plant, and (5) a qualitative assessment for this application that it is unlikely an accident or transient coupled with a common mode software failure will result in an RPS failure into other than the preferred state. The postulated ANS Condition IV event with massive multiple failures exceeds the single failure criterion and is considered to be highly unlikely. Based on this assessment, the staff finds that there is reasonable assurance that if a software common mode failure occurs, there is a diverse means to safely shut down the reactor.

5.18 Reactor Trip and Engineered Safety Features (ESF) Trip Setpoints

All Trip Setpoints and Allowable Values for Reactor Trip and Engineered Safety Features Trip Setpoints other than those associated with Neutron Flux were evaluated to ensure values remained consistent with existing technical specifications. Neutron Flux setpoints were not evaluated because the nuclear instrumentation was not included in the upgrade; therefore, no new nuclear instrumentation uncertainties were introduced.

The new setpoint calculations provided by the licensee were based on Instrument Society of America (ISA) draft recommended practice ISA-dRP67.04, Part II, "Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation," (Draft 10) and the Westinghouse Menu Driven Setpoint Calculation Program, WCAP-12741 (STEPIT).

The calculations based on ISA-dRP67.04, Part II, methodology were performed on all upgraded instrument loops, and included uncertainties obtained from manufacturer published data, qualification test reports, plant-specific procedures, and plant-specific practices. The calculations included the uncertainties identified in ISA-dRP67.04, Part II. The staff finds the calculation methods to be consistent with the ISA recommended practice. The uncertainty values used in the calculations for the new Foxboro equipment were verified by the staff to be conservative by review of applicable reference documentation and test results, and, therefore, the setpoint methodology is acceptable.

6.0 SUMMARY

The staff has reviewed the proposed Foxboro digital RPS upgrade for D.C. Cook, Units 1 and 2 with particular attention focused on those aspects specific to ensuring safety in digital-based instrumentation and control systems including software quality and reliability, configuration management, environmental qualification of hardware, and defense-in-depth provisions in the event of postulated failures.

Based on its review, the staff concludes that the proposed modification to the RPS is consistent with the current plant licensing design basis and will provide appropriate RPS function as required. The staff, therefore, concludes that the Foxboro digital RPS modification at D.C. Cook is acceptable.

7.0 STATE CONSULTATION

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

8.0 ENVIRONMENTAL CONSIDERATION

The amendments change the requirements with respect to the installation or use of a facility component located within the restricted area as defined in 10 CFR Part 20. The staff has determined that the amendments involve no significant increase in the amounts, and no significant change in the types, of any effluents that may be released offsite, and that there is no significant increase in individual or cumulative occupational radiation

exposure. The Commission has previously issued a proposed finding that the amendments involve no significant hazards consideration and there has been no public comment on such finding (58 FR 12263). Accordingly, the amendments meet the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(9). Pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendments.

9.0 CONCLUSION

The staff has concluded, 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 amendments will not be inimical to the common defense and security or to the health and safety of the public.

Principal Contributor: S. Rhow

Revised: May 13, 1994

cc:

Regional Administrator, Region III
U.S. Nuclear Regulatory Commission
801 Warrenville Road
Lisle, Illinois 60532-4351

Attorney General
Department of Attorney General
525 West Ottawa Street
Lansing, Michigan 48913

Township Supervisor
Lake Township Hall
Post Office Box 818
Bridgman, Michigan 49106

Al Blind, Plant Manager
Donald C. Cook Nuclear Plant
Post Office Box 458
Bridgman, Michigan 49106

U.S. Nuclear Regulatory Commission
Resident Inspector Office
7700 Red Arrow Highway
Stevensville, Michigan 49127

Gerald Charnoff, Esquire
Shaw, Pittman, Potts and Trowbridge
2300 N Street, N. W.
Washington, DC 20037

Mayor, City of Bridgman
Post Office Box 366
Bridgman, Michigan 49106

Special Assistant to the Governor
Room 1 - State Capitol
Lansing, Michigan 48909

Nuclear Facilities and Environmental
Monitoring Section Office
Division of Radiological Health
Department of Public Health
3423 N. Logan Street
P. O. Box 30195
Lansing, Michigan 48909

Mr. S. Brewer
American Electric Power Service
Corporation
1 Riverside Plaza
Columbus, Ohio 43215