U.S. NUCLEAR REGULATORY COMMISSION
REGION I

DOCKET/REPORT NOS. 50-277/93-21
50-278/93-21

LICENSE NOS. DPR-44
DPR-56

LICENSEE: Philadelphia Electric Company

FACILITY NAME: Peach Bottom Units Nos. 2 and 3

INSPECTION DATES: September 20, 1993 to November 8, 1993

INSPECTOR: John A. Calvert 1/31/94

John A. Calvert, Reactor Engineer
Electrical Section, EB, DRS

Date

APPROVED BY: William H. Ruland 2/2/94

William H. Ruland, Chief
Electrical Section, EB, DRS

Date

Inspection Summary: Inspection on September 20, 1993, to November 8, 1993. (Inspection Report Nos. 50-277/93-21 and 50-278/93-21)

Area Inspected: This was an announced inspection to review the licensee's 10 CFR 50.59 modification process and documentation for the digital aspects of the high pressure coolant injection system, the recirculation control system, and the feedwater control system.

Results: No violations or deviations were identified. One unresolved item and one open item were determined. These items are discussed in Section 2.0, Section 3.0, and Section 6.0.

The inspection found that the 10 CFR 50.59 process did not address the industry and NRC concerns regarding safety-related digital upgrades. This is an unresolved item.

For the safety-related HPCI digital upgrade, the licensee recognized the major issues involved in analog-to-digital retrofits, but was not effective in the application of procedures for design equivalent change. The direct relation of the quality of the software to the reliability of the application was not fully addressed. The EMI issues were addressed in the engineering stages. The dedication process was not comprehensive as far as consideration of software verification and validation issues and mild environment testing for the digital upgrades.

The system engineering translation of analog functions to digital showed very good comprehension of the vendor function block programming tools for the recirculation and feedwater upgrades.

For the feedwater upgrade, the selection of an appropriate computer system and software vendor was a major contributing factor for the good performance of the digital upgrade. The system functional specification was very good, although no software standards were specified. The system engineer interfaced with the vendor in a very effective manner, and this also was a direct contribution to the good performance of the system. The use of a system simulator for factory acceptance test allowed a realistic checkout of the system before installation. The participation of the operating and maintenance staff in the factory test along with formal classroom training was an excellent training method.

DETAILS

1.0 PURPOSE

The purpose of this inspection was to assess the safety and the engineering aspects of plant modifications, with special focus on the digital and software design, including electromagnetic interference (EMI) tests. The inspection included review of documents associated with the high pressure coolant injection system for Unit 3, the recirculation control system for Unit 3, and the feedwater control system for Units 2 and 3. The inspection was conducted at the Peach Bottom Atomic Power Station site in Delta, Pennsylvania.

2.0 DIGITAL UPGRADE 10 CFR 50.59 EVALUATION

The inspector audited the 10 CFR 50.59 process that was used for the analog-to-digital upgrade for the HPCI system. The licensee determined that the modification could proceed under their design equivalent change (DEC) method. The DEC is a type of modification that may be accomplished by a limited scope procedure and can be a permanent change that does not alter the plant design as described in the UFSAR, Technical Specifications and other portions of the SAR. The DEC allows replacements of two components with one, or vice versa, as long as the function of the system is not changed.

2.1 Design Equivalent Change Process for HPCI Digital Modification

The inspector determined that certain failure modes unique to digital products were not evaluated as part of the DEC. The licensee stated that the failure modes of the digital controller were identical with the analog controller; namely, fail high, fail low. The inspector pointed out that unlike an analog controller, a digital controller is subject to transient hardware/software failures that can cause internal transfer function errors and lead to different failure modes than just fail high or low. The evaluation of the digital failure modes focus on detection of failures and indications of failures to the operator so that action could be taken. The inspector examined an internal licensee letter entitled "Summary of Analog to Digital I&C Upgrade Practices and Recommendations," (R.D. Disandro to Distribution; August 31, 1993) that delineated some of the differences between analog and digital equipment, and documented NRC concerns on digital modifications, electromagnetic interference/radio frequency interference (EMI/RFI), and software verification and validation (V&V). The letter also included additional guidance on 10 CFR 50.59 evaluations, especially for digital upgrades. The inspector pointed out to licensee management that the DEC did not address the pertinent NRC and industry concerns expressed in the letter. Licensee management agreed to address the guidance in the digital I&C upgrades letter.

2.2 10 CFR 50.59 Evaluation for Generic Digital Upgrades

The inspector examined the licensee procedure "10 CFR 50.59 Reviews" (LR-C-13 Revision 0, effective April 12, 1993, w/attachments) and found that it also did not address the unique digital concerns outlined in the digital I&C upgrades letter discussed in paragraph 2.1 above. The licensee management agreed to evaluate the procedure to determine if the digital concerns of the memo would be, or are, adequately addressed.

2.3 Conclusions

The inspector concluded that the range of potential digital failure modes were not identified or evaluated to determine the possibility of an equipment malfunction of a different type as described in 10 CFR 50.59(a)(2). The NRC will inspect the completed licensee evaluations of the HPCI digital upgrade and the generic 10 CFR 50.59 review procedure (Unresolved Item 93-21-01).

3.0 HPCI DIGITAL UPGRADE (UNIT 3, ECR PB 93-01185)

The digital upgrade for the high pressure coolant injection system (HPCI) modification is concerned with the HPCI turbine control system. The modification will replace the existing analog square root module, the PID controller, and two signal converters with one programmable digital controller and one signal converter. Not all of the modification documents were completed at the time of the inspection. The inspector reviewed the areas below to assess the system, hardware and software aspects of the design.

3.1 Analog-to-Digital Requirements Translation

The HPCI system is capable of maintaining adequate core cooling for intermediate and small break LOCAs. Defense in depth is provided by the automatic depressurization system (ADS) and either the low pressure coolant injection (LPCI) modes of the residual heat removal (RHR) or the core spray (CS) systems.

The inspector determined that the functional requirements and parameters for the digital controller were translated from the elementary diagram and instrument data sheets. The design and performance requirements were formalized in the design input document, which the inspector reviewed. The inspector examined the loop diagram that depicted the programming symbology, data flow and control flow for the digital controller. The loop diagram is a controlled document that uses vendor programming symbols and serves as the requirement document for the controller programming. The vendor symbols are unique and do not conform to any programming standard.

3.2 Digital Cc.ntroller

The inspector accompanied the licensee on a QA pre-audit conference with the digital controller vendor, Moore Products. The digital controller is a 352 MYCRO series that is configured (programmed) to perform the square root translation, the PID algorithm, alarms, and the necessary input/output functions for a single loop. It is a microprocessor-based, stand-alone industrial grade unit. The design of the controller provides front panel configuration (programming) of the desired type of control strategy by using software interconnection of pre-coded function blocks. The same digital controller, with different configuration programming, is a!so used in the feedwater control and recirculation systems.

3.2.1 Hardware

The control program that the controller performs is configured by front panel selection of software function blocks that reside in the read only memory (EPROM) on the microprocessor board. When selected for inclusion into a particular control program, function block parameters are stored in nonvolatile random access memory (NVRAM).

Each NVRAM chip has a self-contained lithium energy source that will provide data retention in the event of power failure. The lithium batteries are an integral part of each memory chip package and do not discharge unless the power to the controller is removed; the shelf life of the batteries is 10 years. The inspector reviewed vendor test data that showed NVRAM data retention capability in excess of 10 years. The vendor stated that there is no limit on the number read/write cycles for the NVRAM.

The microprocessor is an 8-bit machine and runs at 2Mhz. A watchdog timer, independent of the microprocessor, will automatically reset the microprocessor in the event that the microprocessor does not complete program execution within a preset time. When the watchdog timer activates, the controller output is driven to the zero output, the licensee's preferred safe state output. The analog-to-digital (A/D) converter is the integration type, which has good noise immunity characteristics.

The inspector reviewed the vendor's list of performance specifications for the controller and found that hardware "type tests" applicable for digital equipment installed in a mild environment were performed, with one exception. The exception was for seismic tests; the licensee plans to do seismic tests as part of the qualification process. The exact determination of the suitability of the vendor tests for the HPCI application is planned to be completed by the licensee and is subject to NRC inspection.

The inspector walked down the control room location where the controller will be mounted and found it adequate.

3.2.2 Software

The generic software package consists of 40,000 lines of source code written in assembly language. The software does not contain an off-the-shelf operating system. The vendor stated that was a design goal, because quality levels of operating system documentatio.. and V&V make the design of deterministic code difficult. The system is partitioned into four major software components and 38 software units, which in turn contain 124 software modules, of which 99 modules contain the various function blocks. The code is documented in commented source listings. A purchased floating point math package is included in the code. The front panel display is updated only on data changes, and is not refreshed periodically.

Power-on diagnostics are included that perform the following:

a. verifies that each RAM memory location can be written to and read from;
b. verifies that factory-entered data is correct and can be read;
c. checks for software compatibility between boards;
d. checks for correct boaru installation.

When a power-on diagnostic error is detected, the analog and digital outputs are put in the safe-state value. On-line diagnostics are also performed that check for A/D errors, watch dog time outs. When a watch dog time out is detected, the processor executes power-up diagnostic routines.

All generic functional blocks are stored in EPROM, but only the blocks that have been assigned an execution sequence number in the configuration process will be performed. The execution number and other parameters for the configured function blocks are stored in NVRAM.

The control program documentation for HPCI had 8 function blocks before the addition of the output current loop feedback for display purposes as described in paragraph 3.2.3 below.

3.2.2.1 Software Verification and Validation (V&V)

The vendor had a V&V program that was covered in three procedures: "Product Design and Test Guidelines"; "Design Documentation Procedures"; and "Software Management." These procedures covered the rudiments of a V&V program, but did not reference any software standard. Structural tests of the generic code were performed by the vendor's individual programmers at the unit level during the software development process. Functional testing of the generic code was done using manual and automated methods. Test statistics were taken on the automated tests. The inspector audited a software metrics report, a block execution time report, and a regression test for an update to the generic software for the 352 controller and found them satisfactory. The suitability of the vendor's V&V program and methodology is planned to be determined by the licensee and is subject to inspection by the NRC.

3.2.2.2 Software Configuration Management

The inspector reviewed the documents that provide the basis of the vendor software configuration management program. The vendor configuration management is covered in the procedure "Software Management," which describes the process by which the development, documentation, release and maintenance of software is controlled. The procedure has five levels of software control graded in terms of the source of requirements, degree of functionality, deliverables, and criticality of a project. Each level has steps for architectural design, preliminary design, detailed design, reviews, integration testing, and final testing. Each level also has associated documents that must be generated at each phase. Metrics are specified that provide indicators of code size, maintainability, thoroughness of tests, and quality. There are also provisions for controls for release and changes through software change requests (SCR) and field incident reports.

The inspector reviewed a vendor report concerned with software upgrade tests. The software change requests (SCRs) included in the test were clearly indicated, along with a severity level, the source of the SCR, and the software revision level where the SCR was incorporated. The functional blocks that were affected by the SCRs were tested to ensure operational consistency and reliability.

The software configuration for the HPCI digital controller will be done by the vendor in accordance with the licensee's loop diagram. The loop diagram shows the sequence and interconnection of function blocks and is a controlled document. The vendor will provide the configuration documentation that shows the actual software configuration control blocks and their installed parameters in the delivered controller. The configuration documentation is equivalent to a program listing. The vendor configuration will be checked at bench calibration by the I&C department. Gain, bias, tuning constants, and other function block parameters can be adjusted or checked during operation. The access for adjustment purposes and documentation of parameters is controlled by plant procedures. The software level of a particular controller can be determined from the labels on the EPROMs on the circuit cards.

3.2.3 Human Machine Interface (HMI)

All displays and controls necessary for configuration are located on the front panel of the digital controller. The inspector observed that the process variable, setpoint, and the output variable are continuously displayed on the front panel with three LED segmented bargraphs calibrated in percent. The exact value of the process, setpoint and output variables are read on the digital display using a pushbutton stepping method. The inspector asked if any of the display controls could change the programming and was shown that the controls did not change the programming. The programming controls are behind an inspection plate, and do not change programming variables unless a digital switch behind the inspection plate is actuated. The inspector therefore determined that access to the controls necessary for programming is physically protected and administratively controlled to prevent inadvertent changes to the stored control program.

The inspector observed the configuration programming of a Moore digital controller and saw that when the output current loop was disconnected, the output variable displayed on the front panel did not indicate zero. The inspector questioned this and determined that system level failure modes of the analog and digital controllers were not examined critically. When the output of an analog current mode controller is disconnected, the output meter would indicate zero and this failure indication would be available to the operator. In the Moore digital controller, the output digital display meter is not in the output current loop, but is on the microprocessor data bus. For the digital controller to respond in the same manner as an analog controller, external circuitry must be added in the loop and used to develop an input for the controller. When this is done, the controller can then be programmed to display the actual output current loop, and show the safe state value of zero if the current loop is opened. The fact that this was not considered indicated that knowledge of the internal operation of the digital controller, along with knowledge of the programming, was not used effectively in deciding if the failure characteristics of analog and digital controllers were equivalent. The licensee system engineer said that the front panel indication should read the zero safe state when the output current is zero, and will add the necessary external circuitry and programming.

The HMI considerations and system/hardware/software factors involved in analog to digital modifications are discussed in the licensee's memo as found in Attachment 2 of this report.

3.2.4 **Commercial Dedication**

According to the 50.59 evaluation, the digital controller will be a fully qualified Class 1E component purchased from a 10 CFR 50 Appendix B supplier. The inspector reviewed the purchase order for the qualification and found that it covered testing for seismic, EMI, and electrostatic discharge (ESD).

The purchase order did not cover service environment temperature testing. The digital controller will be located in a mild environment and is not subject to the requirements of 10 CFR 50.49, environmental qualification for harsh environments; however, the controller is subject to the requirements of 10 CFR 50 Appendix B, Criterion III, design control. This criterion applies in that the controller must be verified for operation over the temperature and humidity ranges that will exist in the installed panel. The licensee agreed to address mild environment testing.

The Class 1E dedication purchase order did not cover software verification and validation (V&V) issues. Since the design is very dependent on the unique properties of software, the verification of the design control issues is important. The licensee agreed to address software V&V issues.

During the inspection, the licensee decided to evaluate the digital controller vendor for placement on the evaluated vendor list (EVL). This will involve a QA audit that will map the vendor's QA program to 10 CFR 50 Appendix B criteria. The results of this evaluation wil! be reviewed by NRC.

3.3 EMI Tests

3.3.1 Digital Controller EMI Tests

According to the 50.59 evaluation, the digital controller will be tested by Nutherm International in accordance with EPRI topical report TR-102323 for EMI susceptibility and emissions. At the time of this inspection, no data was available. The completed EMI evaluation will be reviewed by the NRC.

3.3.2 Plant EMI Mapping

The purpose of FMI mapping is to collect emissions data that can be used to verify that there is sufficient margin between the EMI qualification levels of equipment and the actual EMI levels at the point of installation. The plant EMI mapping data will be used by the licensee to establish conditions for future digital upgrades, as well as the HPCI digital upgrade. The licensee is a participant in the EPRI/Utility EMI working group on generic emissions testing and will make the data available to the EPRI statistical data base.

The inspector audited the conduct of the EMI mapping of the Unit 3 side of the control room during shutdown conditions for the following tests:

a. conducted emissions on power and signal lines, common mode and differential mode in the frequency band of 15KHz to 50 Mhz;

b. radiated emissions, DC magnetic field;

c. radiated emissions, AC magnetic field, 30Hz to 50KHz;

d. radiated emissions, electric field, 14KHz to 1GHz.

The tests were conducted to written procedures approved by the licensee. The test contractor personnel were experienced in the performance of the test methods and operation of the computer and graphic equipment. The computer-plotted graphs of signal strength versus frequency made trends readily apparent. The graphs will be part of the data to be analyzed by the licensee to determine that the HPCI digital controller has sufficient margin. The EMI evaluation is planned for completion by the licensee.

The inspector observed that for the conducted emissions common mode measurements on signal cables, the test contractor ensured that the current probe surrounded as many conductors as the diameter would allow. For the same type of measurement on power leads, the test contractor included the ground wire. The inspector also observed that for the conducted emissions differential mode measurements on signal cables, the test contractor worked with the licensee to select the longest conductors that break out of the bundle, or select signal leads that were close to power leads. These test contractor actions were in accordance with the test procedure and reduce the risk of invalid data.

3.4 Training

The inspector went to the I&C classroom area and observed the instruction on the digital controller. The controller is installed in an actual control loop. Instrument theory, programming, calibration were covered according to a written lesson plan. The inspector found that the training was adequate to convey the digital hardware system and configuration programming practices to the technicians and technical staff.

3.5 Conclusions

The HPCI controller is used in conjunction with other systems that provide defense in depth. The same digital controller is not used in the defense in depth systems, so that software common mode failure concerns can be ruled out. The digital controller will combine functions that were performed by the analog controller. This will enhance hardware reliability from strictly a parts count basis, but makes functional reliability very dependent on the quality of the software.

The failure modes of the digital controller were not completely addressed in the 50.59 evaluation. A set of potential faults internal to the processor will cause a corresponding set of failures at the controller boundaries, which then can be evaluated at the system level. The licensee's failure mode basis for modifying the HPCI control system under the design equivalent change (DEC) procedure will be clarified as written in Sections 2.1 and 2.2.

The function block programming tools allow the system engineer to understand the software programming at a system level, and allow for a common ground of interpretation between the vendor and the licensee. Therefore the accuracy of translation from the system requirements to the software is improved by using the tools of the function block programming.

The programming tool kit, while a benefit in requirements accuracy, places a premium on the quality of the software. This is because the underlying microprocessor considerations of processor utilization, timing margins, memory margins, and the extent of error processing is not available to the user for verification. The accuracy and reliability of the software can only be determined by audit of the vendor's software practices. The licensee recognized the importance of this, and will audit the vendor's QA practices.

The software V&V, qualification tests, and commercial dedication issues are yet to be completed. When they are completed, they will be reviewed by NRC.

4.0 RECIRCULATION SYSTEM DIGITAL UPGRADE (Unit 3 Modification 887)

This modification package for the reactor recirculation system was ın the final document approval stage and the inspector audited the documents that were completed. The licensee's objective for the reactor recirculation flow system digital upgrade was to change the system from closed loop automatic control to open loop manual control for the MG set generator speed and thereby the recirculation pump speed. This was done by removing the process signal from the generator tachometer and implementing analog functions in a manual station digital controller. The reason for the modification was that the system had a history of rapid core flow transients with resultant power excursions caused by erratic recirculation pump speed changes.

4.1 Analog-to-Digital Requirements Translation and Digital Controller Implementation

The functions implemented in the digital controller were the control, speed run backs, rate of speed limiters, and alarm functions that were performed by the corresponding analog devices as defined in the plant elementary diagrams and instrument data sheets. The licensee's engineering determined the software loop diagrams and the vendor did the configuration programming.

The digital controller basic hardware and software was the same as used for the digital controllers used in the feedwater and HPCI control systems. The vendor configuration programming for the recirculation flow digital controller was checked by the I&C modification group under procedural control.

The inspector audited the loop diagram and the configuration documentation for consistency using the vendor's programming instructions, and found no discrepancies. The control program used approximately 35 function blocks. The inspector observed that the output variable is read from the microprocessor bus and not the actual output current. The licensee's system engineer said that the plant operator will mainly watch the recirculation flow instrumentation for system trouble and not the MG set controls, so that strict analog emulation is not required. The inspector had no further questions in this area.

4.2 Conclusions

The digital controller is a small scale integration of analog functions that is now part of an open loop system, which should enhance operational reliability. The translation of system requirements using the function block tools reduced the chance for error. The audit of the configuration program was satisfactory.

5.0 FEEDWATER DIGITAL UPGRADE (Modification 1843, Units 2 and 3)

The analog feedwater control systems of both Unit 2 and 3 were replaced with digital control systems because of numerous plant trips caused by the analog systems.

5.1 Analog-to-Digital Requirements Translation

The system functions were those functions listed in the plant elementaries and instrument data sheets for the analog system as documented in a digital system specification. The vendor made software function block documents that showed how the high level software would implement the system. The licensee's engineering reviewed and commented on the function block implementation; three iterations of review occurred. The inspector did not audit the sampled data system aspects of the design.

5.2 Dual Redundant Computer Implementation

The dual redundant computer system was designed so that any single failure of the computers or of the input field transmitters will not result in loss of feedwater control. The two computers receive identical (but not separate) inputs, process the inputs using identical programs, and deliver identical, but separate outputs. The inputs from process variable field transmitters are redundant. The power sources are redundant.

The computer outputs are routed to a transfer switch that is controlled by separate watchdog timers. One computer is designated as the primary and one computer is designated the backup. The transfer switch normally provides the set of primary computer outputs to the control system. If an internal failure of the primary computer is sensed by the watchdog timer, then the transfer switch will select the backup computer set of outputs to control the system.

If a field transmitter fails the limit check or deviation check with an equivalent redundant transmitter, the computers will switch to the redundant input, or change to another method of control.

The inspector walked down the installation of the computer system in the relay room. The location was adequate from the maintenance and heat load aspects.

5.2.1 **Hardware**

The two computers are IBM 7552 industrial grade CPUs, which use the Intel 386 microprocessor chip. The input/output (I/O) consisted of boards from Computer Products (CPI). The I/O types were the following: 21 analog inputs; 23 analog outputs; 14 digital inputs; 12 digital outputs. The system has 4 control modes. Six digital controllers are also used on the control room operator panel.

5.2.2 **Software Development, V&V, and Configuration Management**

The software was developed by AECL using their PROTROL control block language, which the licensee said was written in Turbo Pascal, with assembly language as necessary for speed. The operating system was DOS 3.3.

The system specification did not specify any software standards, but the vendor had a software quality assurance program that used the following IEEE standards as a basis

a. IEEE Std 730-1984, "IEEE Standard for Software Quality Assurance Plans";

b. IEEE Std 1012-1986, "IEEE Standard for Software Verification and Validation Plans";

c. IEEE Std 828-1983, "IEEE Standard for Software Configuration Management Plans";

d. IEEE 829-1983, "IEEE Standard for Software Test Documentation."

In addition, AECL had software developers' handbooks that define internal coding document standards and procedures. Formal V&V plans are written for critical parts of the software.

The inspector reviewed the calculation document (PE-057, October 27, 1992) that determined the acceptable ranges of the software variables for setpoints and process tuning parameters for 128 types of control blocks. The bases for the calculations were clear and the calculations were referenced to the software version. The detailed analyses in the document showed that the system engineer understood the interface between the feedwater system and the control block software programming methodology.

The inspector reviewed the vendor software freeze document (Version 2.19, 17-69200-225-000, April 4, 1992) and samples of completed software change requests (SCR.) The freeze document included the title and closed status of 364 SCRs, along with the software module affected and a priority code. The inspector calculated the percentage of total SCRs involved in the priorities as: 23% critical; 28% important; 21% upgrades; 10% enhancements; 18% cosmetic or undefined. The inspector also calculated the percentage of critical and important SCRs completed at each major phase as: 62% baseline phase; 21% factory acceptance test phase; 17% site testing/final acceptance stage. The data showed that software errors were classified as to effect and that the critical/important errors were decreasing at each major phase, which is one indication of a well controlled software project. Also included in the configuration were the titles, document numbers and revision levels of the software documentation. The inspector audited the correlation of the SCR numbers and titles with the description on the configuration and found no conflicts. The inspector concluded that the vendor had an adequate software configuration management program to assure that inadvertent changes and uncoordinated revisions would not be introduced into the installed software.

5.2.3 Test Program

A system acceptance test was performed at the vendor's facility that involved the use of a feedwater system simulator, which was designed and built by the vendor. The licensee's operators, system engineer, and I&C technicians were involved in the factory test. Plant tests were conducted to show conformance to performance criteria and establish final tuning parameters. The inspector reviewed the requirements traceability matrix that listed the source of 159 system requirements and their acceptance or disposition criteria. The approximate percentage of requirements accepted at the initial vendor test was 87%, acceptance after further testing was 13%, and less than 1% required further resolution before acceptance.

5.2.4 Training

The system engineer had software training at AECL. The I&C technicians had hardware training at AECL.

5.3 Digital Controller

A total of six digital controllers from Moore Products were used: master level(1); reactor feed pump speed controls (3); and startup level control (2). The controllers were configured using the same control block configuration programming procedures as the digital controllers for the HPCI and recirculation system upgrades. The inspector reviewed the instrument calibration sheet and software programming document for master level digital controller and found that it was in agreement with the vendor's programming instructions.

5.4 Conclusion

The use of the function block tool kit for programming minimized the chance for functional errors. The system engineer showed excellent grasp of the tool kit and its application to the feedwater system. There were design reviews of the vendor translation of system requirements. These actions showed excellent licensee/vendor interaction.

The hot standby dual redundant computer system configuration provides good protection against random hardware failures. The independent, dual watchdog timers provide adequate protection for computer lock-up failure modes.

The vendor V&V program was based on industry standards and had software development handbooks. The software configuration management program was adequate to ensure change and version control. The test program, including factory acceptance test and site test, was done in a controlled manner and provided adequate coverage of the functional requirements.

6.0 UNRESOLVED ITEMS

Unresolved items are matters about which additional information is necessary to determine whether they are acceptable, a deviation, or a violation. One unresolved item is discussed in detail under Section 2.3. There is one open item subject to NRC inspection, in which the licensee agreed to complete certain HPCI details; these are discussed in Sections 3.2.1, 3.2.2.1, 3.2.3, 3.2.4, and 3.3.1 (Open Item 93-21-02).

7.0 EXIT MEETING

The inspector met with the licensee's personnel denoted in Attachment 1 of this report at the conclusion of the inspection period on October 8, 1993. At that time, the scope of the inspection and inspection results were summarized. Also at that time, a licensee document, inadvertently marked with comments by the inspector, was given to the licensee; the document is included as Attachment 2. An additional exit was conducted by telephone with the licensee's personnel on November 8, 1993, to summarize the inspection of a portion of the control room EMI tests.

ATTACHMENT 1

Persons Contacted

Philadelphia Electric Company

*	J. Armstrong	Senior Manager, Plant Engineering
	W. Bowers	ISEG
	T. Cabarey	System Engineer, Digital Feedwater
	J. Clupp	Manager, I&C
**	F. Cook	Senior Manager, Design Engineering, PBAPS0
*	W. Curry	Manager, NISD-PBAPS
**	K. Cutler	Engineer, I&C Design, PBAPS
**	R. DiSandro	Engineer, I&C Engineering, NED
*	G. Edwards	Plant Manager, PBAPS
	A. Fulvio	Manager, NQA
*	G. Gellrick	Senior Manager, Operations
**	K. Graff	Licensing Engineer
	G. Hager	Instructor
*	D. Keene	Manager, Design Engineering, I&C, PBAPS
*	M. Kray	Manager, Licensing PBAPS
*	D. Louie	Design Engineer, I&C
*	D. B. Miller	Vice President, PBAPS
	W. Nelle	Lead Assessor, NQA
*	T. Niessen	Director, Site Engineering
	C. Patrick	Engineer, NQA
	K. Schoenknecht	Engineer, NISD-PBAPS
	J. Schul	I&C Technician
**	R. Smith	Experience Assessment/Regulatory
	G. Termine	System Engineer, Recirculation Upgrade
	M. Thomas	Instructor

Atlantic Electric

*	H. Abendroth	Site Representative

Bechtel

	C. Yaegley	Modification Engineer, I&C (Bechtel)

Moore Products Company

V. Camuti	Sales Engineer
E. Krieg	Senior Software Engineer
B. Storer	Supervisor, Systems Test
W. Wright	Manager, Product marketing

National Technical Systems

I. Kaye	EMI Technician
M. Metcalf	EMC Manager, East Coast

PSEG

* J. Carey	Co-owner Site Representative

U.S. Nuclear Regulatory Commission

** J. A. Calvert	Reactor Engineer, Region 1
P. Bonnett	Resident Inspector

* denotes attendance at exit meeting 10/8/93

** denotes telephone exit conferees 11/8/93

ATTACHMENT 2

Report References

Section 3.2.3, Human Machine Interface (HMI), last paragraph

Section 7.0, Exit Meeting

Title: Lessons Learned from PECo/NRC Inspection of Moore Products, 10/05/93, w/enclosure titled, "Analog to Digital Retrofits." (Licensee document, marked)

ATTACHMENT 2

PHILADELPHIA ELECTRIC COMPANY
NUCLEAR ENGINEERING DIVISION
965 CHESTERBROOK BLVD.

October 5, 1993

FROM: R. D. DiSandro

TO: Distribution

SUBJECT: Lessons Learned from PECo/NRC Inspection of Moore Products - October 1, 1993

An NRC inspection of Peach Bottom digital retrofits[1] is being performed by John A. Clavert of Region 1 from September 20 through October 8, 1993. Part of this inspection reviewed the design packages for Feedwater (Mod. 1843), Recirc (Mod 887), and HPCI (ECR # 93-01186).

Design Engineering Change

Since the HPCI ECR involved a DEC replacement of an existing GEMAC controller with a Moore "Mycro 352" digital "equivalent", PECo and the inspector decided to visit Moore Products of Spring House, PA to determine the extent of Moore's design control process. The following design guidelines for digital devices were based on this visit:

1. Make sure there is a provision to protect for inadvertent ~~[illegible]~~ access to processes, operations, such as passwords or keyboard lockout.

2. There must be a positive check on device configuration when first configured. There must also be a periodic check of the device configuration to assure it has not changed. These checks can be by independent verification, or by review of file size, checksum or CRC check.

   measured in the scan cycle

3. In determining response time of the device, credit should not be taken for times faster than twice the scan cycle. For example, if the scan cycle is 50 msec., the fastest response time that can be credited is 100 msec. Be assure that the actual update time could exceed the scan cycle dependent on when the input change

   ~~include also update time could extend to 2X scan cycle~~

4. A through understanding of device display options is important. thorough Devices, such as controllers can indicate either the desired output (command value) the actual output (response value). Additionally, some devices do not continually update the display. A review of operator assumptions prior to device configuration will reduce the potential for inadvertent operator errors. Be ~~advised~~ aware that ~~[illegible]~~ external circuitry and/or additional configuration may have to be done if ~~the [illegible]~~ ~~the~~ only the command values are available and the response value is desired to be displayed.

[1] See analog to digital retrofit explanation (attached)

5. The device should be designed to present a positive acknowledgement for command entries (such as a beep or display flash or blink).

6. It is advisable to document the ROM chip Firmware version level (found on the circuit card) as part of the I&C data sheet information. Check with the manufacturer prior to loading new configurations into existing devices since there have been instances where manufacturer generic enhancements have not been backward compatible.

7. The watchdog timer should be electrically independent from the processor. Namely, the timer should be a discrete circuit. Software self diagnostics may be desirable but they are ineffective during a CPU halt.

8. When evaluating a vendor, the quality of sub-tier vendors should be considered. This consideration should also be extended to sub-tier suppliers of software. The software vendors' system for maintaining version control along with evidence of testing of sub-tier vendor supplied math packages, drivers, compilers and assemblers should be determined. Ask about what software development tools were used and extent of SQA on them.

9. If the device has a RAM battery, determine its expected life and assure that maintenance procedures have been updated to reflect periodic replacement.

10. When evaluating software module test results, assure yourself that all flow/signal and Control paths have been tested.

11. Does the vendor have a method for classifying software failures? The vendor should have a mechanism to evaluate their internal Software Change Reports for possible trends.

12. On devices that perform math functions, are some of the calculations dependant on internal clock accuracy? An example would be integrations. If the clock accuracy is a factor, to what degree will clock drift corrupt the calculation?

13. Has a determination of the effects of ~~concerning~~ EMI on power lines and I/O ~~signal~~ lines been made? Has ~~power factor~~ harmonic distortion, power factor of the new device been considered?

14. Explore the extent of the consequences of single bit errors on address/data/control busses. ~~Are~~ Find out if the errors are detected internally or externally. Cover transient and steady state errors. ~~[illegible]~~ ~~that~~ Determine ~~that~~ effect ~~[illegible]~~ is severe ~~or~~ benign if the probable or improbable.

The 50.59 documentation process should ~~[illegible]~~ be clear so that NRC inspectors can understand ~~[illegible]~~ the rationale used.

[illegible] Explicitly [illegible] failure modes and

ANALOG TO DIGITAL RETROFITS

The present PECo position concerning analog to digital upgrades is to evaluate each case on an individual basis. If a particular digital upgrade application constituted an unreviewed safety question by use of the 50.59 determination, then PECo would seek prior NRC approval. If the application does not constitute an unreviewed safety question, regardless of whether it went into a safety system or non-safety system, prior NRC approval would not be requested and the upgrade would be performed under the 50.59 process. The analog to digital issue revolves around establishing the extent the utility needs to understand the digital device in order to assure that any additional failure modes are captured and evaluated.

The Commission is concerned that the use of digital devices as replacements to analog I&C may introduce new plant failure modes which may not be appropriately captured by existing check lists and utility practices. There is also a question as to how much CRITICAL understanding of internal design detail is necessary for adequate bounding of these failure modes. The ideal is to have the critical errors be detected ~~and~~ in a form that is recognizable to a plant operator.

Retrofits of safety related systems require the highest scrutiny. The functional complexity of replacement digital devices may range from a one-for-one replacement item such as a signal converter to a programmable logic controller that could replace an entire bank of safety critical relays. Clearly, complex devices with multiple inputs and outputs will require a greater evaluation and understanding than that of a single function item. However, the engineer should not casually be misled by the outward simplicity of a single function device. It is important to understand that digital devices are time/~~domain~~ sequenced/state ~~state~~ sequential machines rather that continuous/linear time processing devices. Even the simplest devices may incorporate a microprocessor and an operating system. Unlike the continuous processing of an analog device, digital devices tend to take time samples of the input, perform the intended function, set an output value and then repeat the cycle.

linear time

When evaluating a retrofit for failure effects to the system, it is necessary to recognize the possibility of new failure modes and subtle system changes for digital devices and determine if they constitute an unreviewed safety question. Examples of these are namely:

- Since the device operates in ~~the~~ a time sequenced domain, delays in response between changes in input value and output response must be considered. The sampling or update rate should ~~match~~ MATCH the [illegible] criterion for the system.
- The bandwidth sensitivity to electro-magnetic interference (EMI) is different than analog. EMI susceptibility and compatibility testing may be necessary to assure proper operation in the intended environment. Switching supplies are commonly used as power supplies; these may introduce internal ~~of~~ external noise and introduce harmonic distortion on the power lines.

o There must be Reset to known states or safe on power failure, CPU halt, or other critical failures as a minimum,

[illegible]

- There must be a method for monitoring CPU activity that is not dependent on software. A resetable time delay drop out relay (watch dog timer) circuit pulsed every computer cycle can provide adequate assurance for a sensing CPU halt.

o There must be

Like analog, digital devices need to be qualified for use in a safety critical system. For a commercial device, this dedication involves evaluating for the critical parameters such as form, fit and function. For digital, the added requirement of EMI testing to assure compatibility to the expected environment will be necessary. Since device operation is dependent on both hardware and software design, it is important that both areas be evaluated when selecting a product. Software design may play a significant role in assuring expected operations in all modes of operation but, unlike analog designs, proper analysis of software structure may not be easily accomplished by bench testing. In such cases, vendor evaluation may be necessary.