October 30, 1996

Mr. Kevin P. Donovan, Chairman
Boiling Water Reactor Owners' Group
Centerior Energy
Perry Power Plant
MC A210
P. O. Box 97
Perry, OH 44081

SUBJECT: SOFTWARE AUDIT OF THE DYNAMIC CONTROLS HAMILTON STANDARD OSCILLATION POWER RANGE MONITOR

Dear Mr. Donovan:

On September 16, 17, and 18, 1996, the staff conducted an audit of the Dynamic Controls Hamilton Standard oscillation power range monitor developed by ABB-CE for the BWR Owners' Group at the Dynamic Controls offices in Windsor, CT. A report of this audit is attached. Two discrepancies were identified: (1) the requirements traceability matrix did not contain all of the software life cycle phases, and (2) the documentation indicates that the verification activities were not acceptable. These deficiencies are identified as open items in the audit report and must be corrected before the oscillation power range monitor can be connected to the reactor trip system. A follow-up audit is scheduled for later this year.

If you have any questions concerning this audit report, please contact the project manager, Jim Wilson, at (301) 415-1108.

Sincerely,

Original Signed By:
David B. Matthews, Chief
Generic Issues and Environmental
Projects Branch
Division of Reactor Program Management
Office of Nuclear Reactor Regulation

Project No. 691

cc: see attached list

DISTRIBUTION:

Central File	OGC	DMatthews
PUBLIC	ACRS	RArchitzel
PGEB r/f	JWermiel	MWaterman
TMartin	JMauck	BBoger

Document Name:BWRAUDIT.I&C

OFC	PGEB	SC:PGEB	C:HICB	C:PGEB
NAME	JWilson:sw	RArchitzel	JWermiel	DMatthews
DATE	10/29/96	10/29/96	10/29/96	10/30/96

OFFICIAL RECORD COPY

DF03 1/1

9611040232 961030
PDR PROJ
691 PDR

96-139 PROJ 691

PROJ

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

October 30, 1996

Mr. Kevin P. Donovan, Chairman
Boiling Water Reactor Owners' Group
Centerior Energy
Perry Power Plant
MC A210
P. O. Box 97
Perry, OH 44081

SUBJECT: SOFTWARE AUDIT OF THE DYNAMIC CONTROLS HAMILTON STANDARD OSCILLATION POWER RANGE MONITOR

Dear Mr. Donovan:

On September 16, 17, and 18, 1996, the staff conducted an audit of the Dynamic Controls Hamilton Standard oscillation power range monitor developed by ABB-CE for the BWR Owners' Group at the Dynamic Controls offices in Windsor, CT. A report of this audit is attached. Two discrepancies were identified: (1) the requirements traceability matrix did not contain all of the software life cycle phases, and (2) the documentation indicates that the verification activities were not acceptable. These deficiencies are identified as open items in the audit report and must be corrected before the oscillation power range monitor is connected to the reactor trip system. A follow-up audit is scheduled for later this year.

If you have any questions concerning this audit report, please contact the project manager, Jim Wilson, at (301) 415-1108.

Sincerely,

David B. Matthews, Chief
Generic Issues and Environmental
Projects Branch
Division of Reactor Program Management
Office of Nuclear Reactor Regulation

Project No. 691

cc: see attached list

Boiling Water Reactor Owners Group

cc: C. D. Terry
Vice President, Nuclear Engineering
Niagara Mohawk Power Corporation
Nine Mile Point-2
PO Box 63
Lycoming, NY 13093

D. B. Fetters
PECO Energy
Nuclear Group Headquarters
MC 62C-3
965 Chesterbrook Blvd.
Wayne, PA 19087

R. A. Pinelli
GPU Nuclear
MCC Building E
One Upper Pond Road
Parsippany, NJ 07054

S. J. Stark
GE Nuclear Energy
175 Curtner Ave, M/C 165
San Jose, CA 95125

T. J. Rausch
Commonwealth Edison Company
Nuclear Fuel Services
1400 Opus Place, 4th Floor ETWIII
Downers Grove, IL 60515

D. B. Bockstanz
Pennsylvania Power and Light Co.
Two North 9th St.
Allentown, PA 18101-1179

SOFTWARE AUDIT OF THE DYNAMIC CONTROLS HAMILTON STANDARD (DCHS)/ABB-CE OSCILLATION POWER RANGE MONITOR (OPRM)

1.0 INTRODUCTION

The BWR Owners' Group contracted ABB-CE to develop an OPRM system for use in BWR plants to detect and suppress reactor power oscillations, as required by GDC 12. ABB-CE contracted Dynamic Controls Hamilton Standard (DCHS) to develop the hardware and software, and assumed the role as the independent verification and validation (IV&V) organization.

To ensure the OPRM system conforms to 10CFR50 Appendix B criteria for quality, NRC staff conducted an audit of the OPRM system development. Mike Waterman, the NRC auditor, conducted the entrance meeting on 9/16; and summarized the audit results at the exit meeting on 9/18.

2.0 EVALUATION

The Period Based Algorithm (PBA) system requirement was selected for the software thread audit because this requirement is used in the licensing bases for the plants. As such, the PBA represents a critical requirement that must meet 10CFR50 Appendix B requirements.

2.1 Description of the PBA Function

The PBA detects peaks and valleys in neutron flux signal levels from selected groups (cells) of local power range monitors (LPRMs). When a sufficient number of consecutive neutron flux oscillations occur (Cell_Confirmation Count) within the frequency range that characterizes the onset of unstable reactor power fluctuations, the PBA provides alarm and trip signals to the RPS. A peak is defined as an increase in the neutron flux level followed by one decreasing sample. A valley is defined as a decrease in the neutron flux level followed by one increasing sample.

For each detected peak or valley, the confirmation count value will be cleared if the peak with valley is outside the area of interest, or the count will be incremented if it is inside the area of interest. Consecutive confirmation counts of peaks with valleys that occur within the required time limits (Tmin and Tmax) are compared to an alarm setpoint (N1) and a trip setpoint (N2). Exceeding the alarm setpoint for confirmation counts results in an alarm signal for the operator. If the neutron flux oscillation normalized amplitude or the peak value exceeds the setpoint (Sp), and the number of consecutive confirmation counts exceeds the trip setpoint (N2), the reactor is tripped.

The amount of required increase or decrease necessary to result in an indication of a peak or valley is the noise floor. Because each plant has its own characteristic noise levels, and these levels may change over time as LPRMs age, the noise floor value is an input variable value (MT_Noise_Floor) entered by the operator.

2.2 Audit Results

The thread audit followed the evolution of the PBA requirement from the ABB-CE system requirements document (Ref. 1) through the DCHS Software Requirements Specification (SRS, Ref. 2), the DCHS Software Design Description (SDD, Ref. 3), the source code (Ref. 4), to the DCHS factory acceptance test plan, procedure, and report (FAT, Refs. 5, 6, and 7). Supporting documents describing project management requirements were also referenced (e.g., the Software Development Plan, Ref 8, the Software Configuration Management Plan, Ref. 9, and the ABB-CE Requirements Traceability Matrix (RTM), Ref. 10). The software lifecycle is comparable to the waterfall lifecycle described in IEEE Std 7-4.3.2-1982, as endorsed by RG 1.152 (1985). DCHS developed the software using the Ada 83 programming language. The software was compiled on a DACS VAX/VMS for an Intel 80186 microprocessor, using a Bare Ada Cross Compiler, Release 4.6.2. The Computer Software Unit (CSU) number group for the set of subprograms comprising the PBA was 3400.

The PBA functional requirement was found in the OPRM Module SRS (¶3.1.23); the OPRM SDD (¶3.2.4.3, ¶4.4.3.1, and the bubble diagram in ¶3.2.4); the source code listing (CSU 3410) and the Test/Validation Test of MT-Noise-Floor (¶C3.1.23.1-3, TM1-2.1.14). The staff verified that the requirement is correctly stated in the applicable documents. The staff noted that the Requirements Traceability Matrix (RTM), which was maintained by the ABB-CE Independent Verification and Validation (IV&V) team, does not include the Computer Program Code Listing (Implementation Phase). ABB-CE was requested to provide information regarding the IV&V of this phase of the software lifecycle. This documentation will be provided at a later date. This is an open item.

Tables 1 and 2 list PBA input and output variables, as described in the System Spec, SRS, SDD, and source code listing. Table 3 provides definitions and comments for the input variables listed in SDD Volume 1.

As shown in Table 1, the input variables were not consistent between the lifecycle phase documents. For example, LTSSS_Time, which is used to define Cell(c).Tpeak, Cell(c).Previous_Peak, Cell(c).Tvalley, and Cell(c)_Previous_Valley, and is used as the clock for comparison with Tmin and Tmax, was not listed as an input variable requirement prior to SDD Volume 1, although this variable is included as a requirement in SDD Volume 2. Since LTSSS_Time was added to Volume 2, it should also have been added to Volume 1, and the documentation of previous lifecycle phases. Another example is the input variable, DR3, which is listed as a required input variable only in the System Specification and SDD Volume 1. As described in Table 3, DR3 is required only in the Amplitude and Growth Rate algorithms, not in the PBA. These major discrepancies in the documentation led the staff to conclude that the V&V and IV&V efforts did not sufficiently verify the lifecycle phase products for the input variable requirements. The staff requested that DCHS and ABB-CE complete the verification of the PBA function and correct these discrepancies in the input variable requirements. This is an open item.

The staff noted that the PBA functional requirements and the output variable requirements were consistent throughout the lifecycle phases. Based upon its review of the software code listings and the factory acceptance test (FAT) results, the staff verified that the discrepancies between the input variable lists of the lifecycle phase documents were not carried over into the PBA pseudocode description, and did not affect the number or type of the output variables.

Output variables are generally defined by the pseudocode for each requirement, and should not change unless the pseudocode is also changed. Since the PBA logic remained unchanged throughout the lifecycle phases, while the documentation describing the input variable requirements did change, the staff concluded that verification effort may have concentrated on ensuring consistent pseudocode descriptions throughout the lifecycle. Less effort is evident for the supporting documentation of the pseudocode.

As shown in Table 2, the output variable names remained essentially unchanged throughout the lifecycle from System Requirements through the Implementation phase. Inspection of the source code listing revealed three additional output variables that were not described in the SDD (Cell(c).Detecting_Peak, Cell(c).Previous_Peak, and Cell(c).Previous_Valley). These three variables were defined in the source code, and are output variables only by virtue of being defined in the variable type, Cell. Their inclusion in the source code for the PBA does not affect the PBA function, and are therefore acceptable.

The staff reviewed the Factory Acceptance Test (FAT) Plan (Ref. 5), FAT Procedure (Ref. 6), and FAT Report (Ref. 7). The purpose of the review was to verify the PBA tests acceptably address all the PBA requirements.

The FAT Plan (Ref. 5) objectives were to define the following:

1. Activities required for preparation and conduct of the FAT
2. The tasks to be performed and the schedule to be followed
3. Sources of information used to prepare the FAT plan
4. Test tools and the environment needed to conduct the FAT.

The scope of the FAT Plan was to ensure testing of all requirements imposed by SRS 0320-01. Testing includes simulating all OPRM inputs simultaneously. The test input signals simulated typical reactor core regional and core-wide oscillations and normal noise conditions. ABB provided the test data input signals, which were obtained from the BWROG and verified prior to delivery to the system developer. The tests were designed to validate requirements for detecting instabilities and not causing spurious trips.

The FAT Plan (Ref. 5) is acceptable. The PBA was test feature 'v' in the FAT Plan. The staff attended the FAT and verified that conduct of the testing conformed to the FAT Plan requirements.

The staff reviewed the FAT Procedure (Ref. 6). The main body of the FAT Procedure provides general test information, including test definition, and assumptions and constraints considered in the test development process. The remainder of the FAT Procedure consists of appendices describing the test setup and equipment, the procedures for creating the standard setpoint and configuration files for the two OPRM units in the test setup, the step-by-step test procedures with test inputs and expected results, additional testing requirements necessary to complete Maintenance Terminal (MT) software functional verification, analog waveform descriptions and procedures for recreating each waveform, and the FAT Test Data Log Sheets necessary for the OPRM FAT.

The staff reviewed the PBA test paragraph, C3.1.23, ODA Period Based Algorithm. The System Requirement states that the PBA will generate a trip output when a periodic oscillation occurs in any LPRM cell with a period between Tmin and Tmax, a cell peak greater than Sp, and a duration equal to or greater than N2. An alarm is generated when the duration of the oscillation is greater than or equal to N1, regardless of the oscillation amplitude in relation to Sp. These values are set with the maintenance terminal (MT); the resulting counting and trip status are reported on the MT and transmitted to the personal computer (PC) workstation that was set up to monitor the test results. The staff reviewed the input data and the test coverage and found the procedure to be acceptable.

The staff reviewed the PBA test results (Ref. 7) and witnessed the FAT initiated on August 2, 1996, and completed on August 6, 1996. One Failure Report was created (FR 111084) during the PBA testing when the setpoint and configuration files were not reset to 000 prior to the test initiation. The files were corrected and the tests were successfully completed. The test results validated correct implementation of the PBA requirements.

The FAT documentation states that the FAT was conducted to verify compliance with the LTSSS Requirements Specification (Ref. 1) and the OPRM SRS (Ref. 2). As noted in this report, the documentation is not consistent throughout the lifecycle phases with respect to input variable requirements. Based on the discrepancies concerning the input variables listed in the documentation, which changed between the System Requirements phase and the Implementation (Source Code) phase, the staff concluded that tests to validate the system requirements and the software requirements may have been written based on the algorithm requirement, and not on the listed input variable requirements. The staff noted that the test requirements acceptably addressed the functional requirements of the PBA; regardless of the errors in the input variable documentation. Consequently, the validation tests were acceptable.

3.0 CONCLUSIONS

The staff reviewed the PBA function in the LTSSS OPRM developed by DCHS and ABB-CE for the BWROG. The staff found input variable requirement inconsistencies within and between the documentation for the lifecycle phases. However, the output variable requirements remained consistent throughout the lifecycle, as did the algorithms for detecting and initiating an alarm and trip signal. The staff concluded that the backward traceability of the source code to the system requirements was not maintained. There is no immediate safety impact from this deficiency; however, revisions to the PBA, which also

must conform to Appendix B criteria for safety-related systems, will become increasingly more difficult without a fully consistent set of documentation for the entire lifecycle.

Based on inconsistencies in the documentation, the staff concluded that the software verification activities were not acceptably implemented with regard to revising the supporting life cycle documentation. Consequently, over the lifetime of the OPRM system, revisions may become correspondingly more difficult to correctly implement because incomplete documentation describing the system will be the only source of information regarding the structure of the code.

The ABB/DCHS OPRM system will be installed in Clinton, Cooper, Dresden 1 and 2, Hope Creek, La Salle 1 and 2, Quad Cities 1 and 2, and Susquehanna 1 and 2. As stated in the approved Topical Report (Ref. 12), each plant will monitor the performance of the OPRM for one fuel cycle before connecting the OPRM system trip output relays to the Reactor Protection System. Based on successful completion of the FAT, which was witnessed by the staff, the OPRM system may be installed in nuclear power plants in this system test configuration.

However, as stated by the staff in the Exit Meeting on 9/18/96, since Appendix B to 10CFR50 requires acceptable quality in both documentation and product, the OPRM software lifecycle verification must be completed and the documentation corrected, reviewed by the staff, and approved prior to final staff approval of the OPRM system as a safety-related component of the Reactor Protection System. None of the plants has installed the system for their current fuel cycle. Consequently, ABB and DCHS have at least one fuel cycle (approximately 24 months) to correct the existing documentation and receive final NRC staff approval. Additionally, ABB-CE must provide the staff with the IV&V results for the source code development phase of the software lifecycle. These two items will remain open pending final staff review and acceptance.

4.0 REFERENCES

1. "LTS Stability System Design Service Project for the Boiling Water Reactor Owners Group of Participating Utilities, LTSSS Requirements Specification," 00000-ICE-3230 Rev 3, ABB-CE, dated 5/29/96

2. "Software Requirements Specification for the Long Term Solution Stability System Module (LTSSS)," SRS 0320-01, Rev C, Data Item 005A, DCHS, dated 9/10/96

3. "Software Design Description for the Long Term Solution Stability System Module (LTSSS)," SDD 0320-01.02, Rev B, Data Item 006A, (Volumes 1 and 2), Preliminary (final version not through the ABB-CE review process), DCHS

4. "Computer Program Listing for the Long Term Solution Stability System (LTSSS)," Data Item No. 017A, CPL 0320-01.02, Rev A, DCHS, dated 8/14/96

5. "Factory Acceptance Test Plan (FAT) for the Oscillation Power Range Monitor (OPRM)," Data Item 013, R1471, Rev B, DCHS, dated 5/25/95

6. "Factory Acceptance Test Procedure for the Long Term Solution Stability System (LTSSS) Oscillation Power Range Monitor (OPRM) Module, PN 11426-1,-2", Data Item 014A, R1495, Rev B, DCHS, 8/5/96

7. "Factory Acceptance Test Report for the Long Term Solution Stability System (LTSSS) Oscillation Power Range Monitor (OPRM)", Data Item 015A, R1618, Rev A, DCHS, 8/28/96

8. "Software Development Plan for the Long Term Solution Stability System Module (LTSSS)," SDP 0320-01, Rev D, Data Item 007, DCHS, dated 8/15/96

9. "LTS Stability System Design Service Project for the Boiling Water Reactor Owners Group of Participating Utilities, Software Configuration Management Plan," 00000-ICE-15143, Rev 01, ABB-CE, dated 8/3/94

10. ABB Requirements Traceability Matrix

11. "Long Term Stability Solution System Project Plan," R1452, Rev B, Data Item 002A, DCHS, dated 10/21/94

12. "Generic topical Report for the ABB Option III Oscillation Power Range Monitor (OPRM)," CENPD-400-P-A, Rev 01, ABB-CE, May 1995.

13. "Self Test Requirements for the Oscillation Power Range Monitor (OPRM)," DCC PN 11426-1/-2, Data Item 005A, DCC1713, dated 5/5/95

14. "Software Programmers Manual for the Long Term Solution Stability System Module (LTSSS)," Data Item 112A, SPM 0320-01, Rev B, DCHS, dated 8/26/96

15. "Computer Resources Integrated Support Document for the Long Term Solution Stability System Module (LTSSS)," Data Item 008, CRISD 0320-01, Rev B, DCHS, dated 9/4/96

16. "Interface Design Document for the Long Term Solution Stability System Module (LTSSS)," IDD 0320-01, Rev B, DCHS, dated 8/27/96

17. "Version Description Document for the Long Term Solution Stability System Module (LTSSS)," VDD 0320-01.02, Rev B, Data Item 111A, DCHS, dated 8/15/96

18. Problem Tracking Forms, DCHS

Table 1. Period-Based Algorithm Input Variables

System Specification	SRS	SDD Volume 1	SDD Volume 2	Source Code Listing
				Cell_Range
		Algorithm_Initializing		
			Cell(c).Detecting_Peak	Cell(c).Detecting_Peak
		Cell(c).First_Peak_Found		
Cell_Norm_Amplitude[c]	Cell_Norm_Amplitude[c]	Cell(c).Norm_Amplitude	Cell(c).Norm_Amplitude	Cell(c).Norm_Amplitude
			Cell(c).Previous_Peak	Cell(c).Previous_Peak
			Cell(c)_Previous_Valley	Cell(c)_Previous_Valley
		Cell(c).Tbase_Established		Cell(c).Tbase (Undefined)
			LTSSS_Time	LTSSS_Time
DR3		DR3		
		MT_Noise_Floor	MT_Noise_Floor	MT_Noise_Floor
	N1	N1	N1	N1
	N2	N2	N2	N2
	Sp	Sp	Sp	Sp
Tmax	Tmax	Tmax	Tmax	Tmax
Tmin	Tmin	Tmin	Tmin	Tmin
TOL	TOL	TOL	TOL	TOL

Table 2. Period-Based Algorithm Output Variables				
System Specification	SRS	SDD Volume 1	SDD Volume 2	Source Code Listing
Cell_Confirmation_Count[c]	Cell_Confirmation_Count[c]	Cell(c).Confirmation_Count	Cell(c).Confirmation_Count	Cell(c).Confirmation_Count
			Cell(c).Detecting_Peak	Cell(c).Detecting_Peak
Cell_Peak[c]	Cell_Peak[c]	Cell(c).Peak	Cell(c).Peak	Cell(c).Peak
			Cell(c).Previous_Peak	Cell(c).Previous_Peak
			Cell(c).Previous_Valley	Cell(c).Previous_Valley
Cell_Period_Alarm[c]	Cell_Period_Alarm[c]	Cell(c).Period_Alarm	Cell(c)Status.Period_Alarm	Cell(c)Status.Period_Alarm
Cell_Period[c]	Cell_Period[c]	Cell(c).Period_Trip	Cell(c).Status.Period_Trip	Cell(c).Status.Period_Trip
Cell_Tbase[c]	Cell_Tbase[c]	Cell(c).Tbase	Cell(c).Tbase	Cell(c).Tbase
Cell_Tpeak[c]	Cell_Tpeak[c]	Cell(c).Tpeak	Cell(c).Tpeak	Cell(c).Tpeak
Cell_Tvalley[c]	Cell_Tvalley[c]	Cell(c).Tvalley	Cell(c).Tvalley	Cell(c).Tvalley
Cell_Valley[c]	Cell_Valley[c]	Cell(c).Valley	Cell(c).Valley	Cell(c).Valley

Table 3. Period-Based Algorithm Input Variable Definitions				
Variable Name	Type	Description	Notes	References
Algorithm-Initializing	Flag	Flag used to indicate completion of Initialization	Not an Input variable in SRS 3.1.23.2 (ODA Priod Based Algorithm Inputs) Not included in SRS Table 1, LTSSS Variable List Listed as an input in SDD 3.2.1.1.2 Defined via Set in SDD 3.2.1.1.3 (Initialization and Executive Processing) Defined in SDD 4.2.1.2.3 (MAIN Logic Flow - CSU No. 1002)	R02 Item 45 SRS 3.1.15 SDD 3.2.1.1, 3.2.4.5.1, 4.1, and 4.1.2
Cell(c).First_Peak_Found	?		Not defined in the SRS 3.1.23, not included in the LTSSS Variable Lists	pg 49
Cell(c).Norm_Amplitude	Analog	Cell amplitude after filtering and normalization by the DC value	shown as Cell_Norm_Amplitude[c] in DCHS SRS and ABB LTSSS Resquirements Spec, shown as Cell(c).Norm_Amplitude in the SDD,	

Table 3. Period-Based Algorithm Input Variable Definitions				
Variable Name	Type	Description	Notes	References
Cell(c).Tbase_ Established	?		Not defined in the LTSSS Variable Lists. Not used in SDD Volume 1. May be Cell(c).Tbase	
DR3	Integer	Growth rate factor SP for Amplitude and Growth Rate algorithms	Shown as an input to the PBA in the ABB LTSSS Requirements Spec 3.1.23.2, SDD 3.2.4.3.2, not shown as an input in SRS 3.1.23.2	
MT_Noise_Floor	Analog	A representation of the lowest detectable change at the analog input terminals. Used to verify detction of peaks and valleys in ODA Cell value. May be a function of APRM Power or Cell average value.	Not an Input in ABB Req. Spec, DCC SRS, shown as an input in DCHS SDD.	ABB Req 3.1.23, SRS 3.1.23, SDD 3.2.4.3
N1	Integer	Period confirmation alarm SP	Not an input in LTSSS Req Spec; shown as an input in SRS 3.1.23 and SDD 3.2.4.3. However, N1 used in LTSSS pseudo code	
N2	Integer	Period confirmation trip SP	Not an input in LTSSS Req Spec; shown as an input in SRS 3.1.23 and SDD 3.2.4.3. However, N2 used in LTSSS pseudo code	
Sp	Analog	Priod based trip amplitude	Not an input in LTSSS Req Spec; shown as an input in SRS 3.1.23 and SDD 3.2.4.3. However, Sp used in LTSSS pseudo code	
Tmax	Time	Maximum oscillation period		
Tmin	Time	Minimum oscillation period		
TOL	Analog	Period tolerance		