

Document 2

**Tennessee Valley Authority (TVA) Watts Bar Unit 2 (WBN2) – Post-Accident
Monitoring System (PAMS) Licensing Technical Report (Document Number
WNA-LI-00058-WBT- NP, Revision 0, June 2010) (Non Proprietary)**

WNA-LI-00058-WBT-NP

June 2010

**Tennessee Valley Authority (TVA)
Watts Bar Unit 2 (WBN2)
Post-Accident Monitoring System (PAMS)
Licensing Technical Report**

Revision 0

APPROVALS

Function	Name and Signature
Author	William J. Catullo Jr.* Fellow Engineer, Regulatory Compliance & Plant Licensing
Reviewer	Warren R. Odess-Gillett* Fellow Engineer, Safety Systems Platform Configuration Management
Approver	Mark J. Stofko* Manager, Safety Systems Platform Configuration Management

*Electronically approved records are authenticated in the electronic document management system.

Westinghouse Electric Company LLC
P.O. Box 355
Pittsburgh, PA 15230-0355

©2010 Westinghouse Electric Company LLC
All Rights Reserved

SECTION 1 INTRODUCTION

This report summarizes the following technical information in support of the licensing effort associated with the WBN2 PAMS:

- Common Q licensing background and a description of the PAMS system
- Hardware and software changes to the Generic Common Q Platform since issuance of the safety evaluation (SE)
- A description of the resolution of the 10 Generic Open Items (GOIs) associated with the U.S. Nuclear Regulatory Commission's (NRC) review of the Westinghouse Common Qualified (Common Q) Platform identified in the Approved Topical Report (ATR) (Reference 2)
- A description of the resolution of the 14 Plant Specific Action Items (PSAIs) associated with NRC review of the Westinghouse Common Q Platform identified in the ATR (Reference 2)
- Responses to the twenty criteria for bi-directional communications that are described in DI&C-ISG-04, Section 1, "Interdivisional Communications" (Reference 14)
- Codes and Standards update associated with the Common Q PAMS (SECTION 7)

SECTION 2 LICENSING BACKGROUND AND SUMMARY SYSTEM DESCRIPTION

2.1 Licensing Background

By letter dated June 5, 2000, Westinghouse (formerly CE Nuclear Power (CENP)) submitted a topical report (early version of Reference 1) to the NRC for review, describing the design of the Common Qualified (Common Q) platform for safety-related instrumentation and control (I&C) applications in nuclear power plants.

Reference 2 is the NRC safety evaluation (SE) report regarding the Common Q topical report. The SE provided the results of the NRC staff's review of the topical report, the accompanying appendices, and other supporting documents. Based on the information provided and the review conducted, the staff concluded that the design of the Common Q platform meets the relevant NRC regulatory requirements and is acceptable for safety-related instrumentation and control (I&C) applications in nuclear power plants, subject to the satisfactory resolution of ten vendor related generic open items (GOI) listed in Section 7.0 of the SE. Additionally, the NRC stipulated that fourteen plant-specific action items (PSAIs) listed in Section 6.0 of the SE be addressed by applicants requesting approval for installation of a Common Q system. These 14 PSAIs are addressed, in detail, in SECTION 4. All GOIs (except for GOI 7.8, Loop Controllers, which will not be used in the WBN2 PAMS) have already been addressed by the vendor (References 7 and 8) and are closed (See SECTION 3, Generic Open Items).

During subsequent meetings between Tennessee Valley Authority (TVA) and the NRC regarding the replacement of the Westinghouse inadequate core cooling monitoring system (ICCM-86) at WBN2 with the Common Q post-accident monitoring system (PAMS), licensing information in addition to the PSAI was requested including:

- A system description of Common Q PAMS
- A list of changes to the Generic Common Q Platform since issuance of the SE
- Resolution of the twenty criteria for interdivisional communications
- Codes and standards that will be included in the design basis for WBN2 specifically revised for the Common Q PAMS (in SECTION 7)

This information is provided in the subsequent sections of this report.

2.2 System Description

The Common Q platform is a computer system consisting of a set of commercial-grade hardware and previously developed software components dedicated and qualified for use in nuclear power plants. The Common Q platform was developed by Westinghouse from the standard AC160 computer system developed by ABB Automation Products, GmbH (ABB Products) of Europe. The Common Q platform is configured with plant-specific application software to implement various nuclear plant safety system applications. The hardware components of the platform are:

- Advant Controller 160 (AC160) with PM646A processor module (includes Watchdog Timer)

- S600 input and output (S600 I/O) modules
- AF100 Bus communication interface (CI631) modules
- External Network communications interface
- Power supply modules
- Flat-panel display system (FPDS)

The AC160 software, residing on flash PROM in the processor module, consists of a real-time operating system, task scheduler, diagnostic functions, communication interfaces and plant specific application programs. The application program is created using the Asea Brown Boveri (ABB) Master Programming Language (AMPL) Configuration Control (ACC) software development environment that includes a function block library for creating specific logic for the application.

The WBN2 PAMS, based on the application of the safety-grade Common Q platform, will replace the existing inadequate core cooling monitor system (ICCM-86). This digital-to-digital replacement will calculate subcooled margin and reactor vessel level, process core exit temperatures, and provide key data to the control room via the FPDS.

The purpose of the WBN2 PAMS is to provide safety grade processing of instruments used to detect the approach to, the existence of, and the recovery from, an Inadequate Core Cooling (ICC) event and display such information to the operator in the control room. The WBN2 PAMS is based on the requirements in the Common Q Topical Report PAMS Appendix, WCAP-16097-P-A, Appendix 1 (Reference 1) with one significant difference. The WBN2 PAMS is deploying a different design for reactor vessel level monitoring (reactor vessel level indication system, RVLIS) from that described in the Common Q Topical Report. The Common Q Topical Report describes a reactor vessel level monitoring system using heated junction thermocouple technology. The WBN2 PAMS will instead employ a reactor vessel level monitoring function based on the requirements and instrumentation used in Watts Bar Unit 1 (WBN1). The WBN2 PAMS will monitor three reactor vessel differential pressure inputs, upper range differential pressure, lower range differential pressure, and dynamic range differential pressure to measure reactor coolant level in the vessel.

Each PAMS train:

- Is mounted in a dedicated cabinet, with identical hardware. Figure 2.2-1 depicts the hardware architecture of the WBN2 PAMS.
- Has an AF100 communication bus that allows communication within a train between the Operators Module (OM), Maintenance and Test Panel (MTP) and the AC160 Controller rack.
- Has a Common Q 15" flat panel display (FPD) for its OM and MTP. Both the OM and MTP have a fiber-optic (FO) Ethernet interface. The MTP uses the FO Ethernet interface to communicate data to the plant computer and for performing print screen functions. The OM FO Ethernet interface is not connected when the system is in service. Access to this interface is controlled by design output drawings and maintenance procedures.

The MTP FO Ethernet datalink to the non-safety plant computer system is via a non-class 1E data diode device. The MTP transmits PAMS data to the plant computer on a cyclic basis. [

] ^{a,c}. The electrical side of the receiving fiber-optic modem is connected to a data diode device. The data link is [] ^{a,c} to the data diode. The data diode is [] ^{a,c}. The data diode is not credited for isolation in accordance with ISG-04, but does provide an additional level of assurance.

The MTP, located in each PAMS train, contains all of the OM pages, except for the default timeout selection page, and provides the human machine interface (HMI) that is used for maintenance and internal alarm functions. The MTP provides displays in support of the following activities:

- Maintenance displays to support corrective maintenance activities
- Displays for entering RVLIS Constants
- Displays for storing and retrieving addressable constants to/from external media.
- Display for allowing the MTP to reboot and load the AC160 tool to load software and run AC160 diagnostic programs.

There are two keylock switches at the MTP and one keylock switch at the OM. The Function Enable (FE) switch (at both the OM and MTP) is used as the permissive for bypassing of input signals, enabling PAMS channel testing, and for changing selected alarm setpoints.

The Software Load Enable (SLE) keylock switch (only on the MTP) is used to enable booting of the PC Node Box into Microsoft Windows for using the AC160 software load tools to load software and read diagnostic buffers.

Both the MTP and the OM will have the following PAMS status displays:

1. [
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.

9.

10.

J^{a,c}

The default page for the OM display is user selectable and has an auto restore feature. The time for auto restore is user selectable. The default display and auto restore time will be established by TVA Operations.

Trends can be generated independently at both the OM and MTP with a minimum of 30 minutes of data available.

In addition, both the MTP and the OM will have the following process displays:

Table 2.2-1 PAMS Process Displays

Group	First Level	Second Level
Core		
	Core Summary	
	ICC Summary	
	Saturation Margin	
	CET Summary	
	Core Map	
	Reactor Vessel Level	
	Level Bar Graphs	
	Level Sensors	
RCS		
	RCS	
Trends		
	Trends	
Selectable Trends		
		Trend 1 Parameter
		Trend 2 Parameters
		Trend 3 Parameters
Dedicated Trends		
		ICC Trend
		RVLMS Trend
		RCS Trend

The WBN2 PAMS is housed in a standard Westinghouse cabinet that is seismically qualified. A basic layout of the WBN2 PAMS cabinet is depicted in Figure 2.2-2. The WBN2 PAMS Common Q power supply is housed in the uppermost section of the PAMS cabinet. Top-mounting of the power supply assembly was chosen as this is the biggest heat producer in the cabinet and in this position; this heat will quickly exit the cabinet. The Common Q power supply assembly receives a 120 Vac input feed through a circuit breaker mounted on a breaker panel in the cabinet rear.

The PAMS process inputs are:

- Core exit thermocouples (CETs)
- Cold reference junction resistance temperature detector (RTD) temperature inputs
- RVLIS differential pressure signals
- RVLIS capillary RTD temperature signals
- RVLIS hydraulic isolation contact status
- Reactor coolant system (RCS) wide range pressure and wide range T_{hot}
- Core thermal power based on differential temperature (delta T power)
- Reactor coolant pump on/off contact status

The PAMS digital data outputs (digital data link to the plant computer) are:

- CET temperatures (individual, representative, highest, quadrant highest, quadrant next highest)
- CET reference junction temperature
- Reactor vessel level (dynamic, lower, upper, void fraction)
- Reactor vessel level operations setpoint
- RCS and CET subcooled margin (temperature, pressure)
- System status information and alarms
- Reactor coolant pump status
- Reactor vessel differential pressure inputs (dP1, dP2, dP3)
- Delta T core thermal power
- RVLIS RTD temperatures
- Reactor coolant system (RCS) wide range pressure and wide range T_{hot}

The PAMS available analog data outputs are:

- RCS and CET subcooled margin
- Representative CET temperature
- Reactor vessel level
- Three user selectable analog outputs

Note: Only the CET subcooled margin output is used for WBN2.

The PAMS available alarm contact and digital outputs are:

- Low RCS saturation margin alarm
- Low reactor vessel level alarm
- High representative CET temperature alarm
- Low RCS and CET saturation margin alarm
- System trouble alarm
- ICC trouble alarm

Note: Only the system trouble alarm contact output is used for WBN2. All alarm digital outputs are sent to the plant computer over the digital data link. All alarms are displayed on the OM (no audible alarm).

a,c

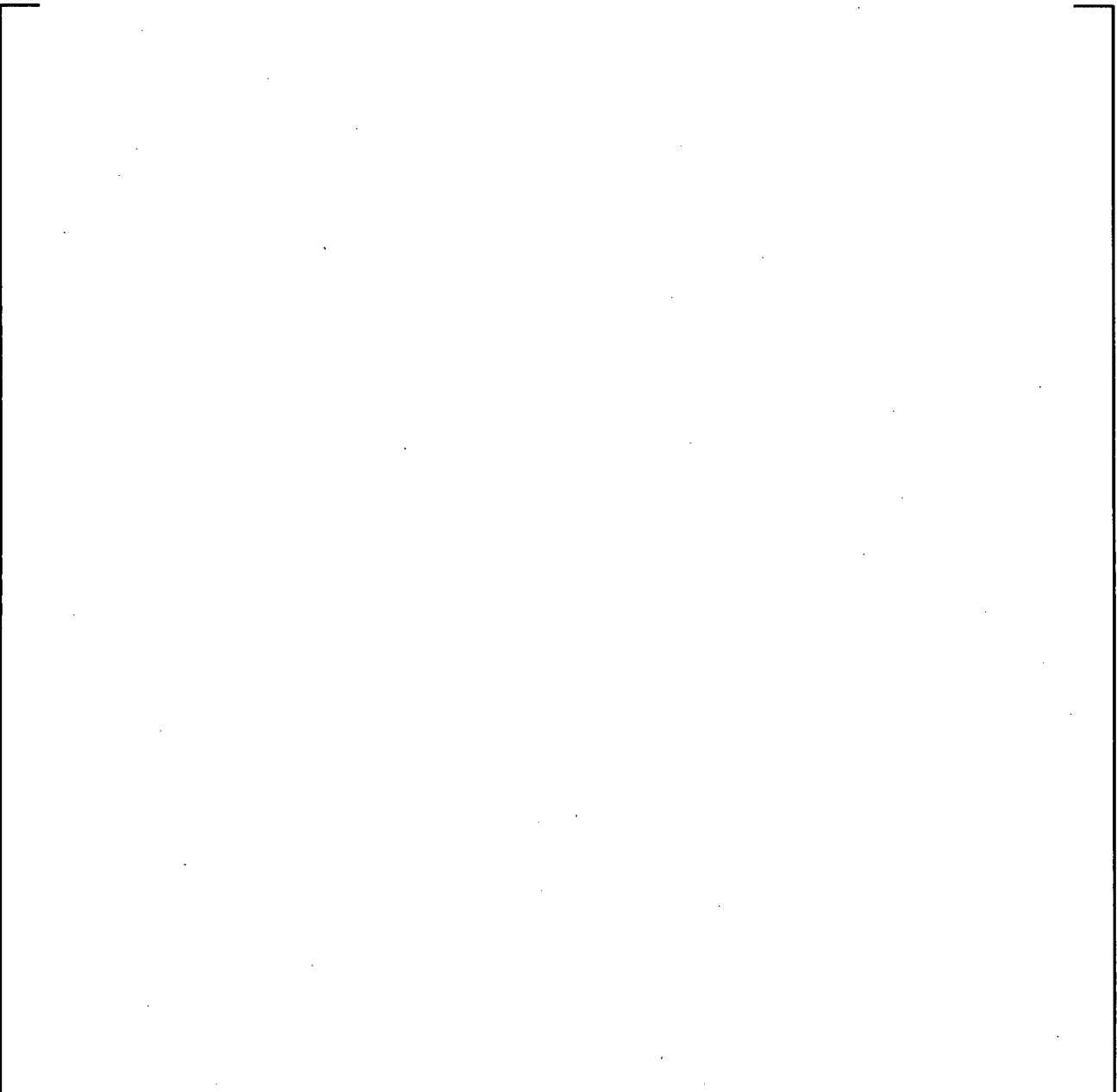
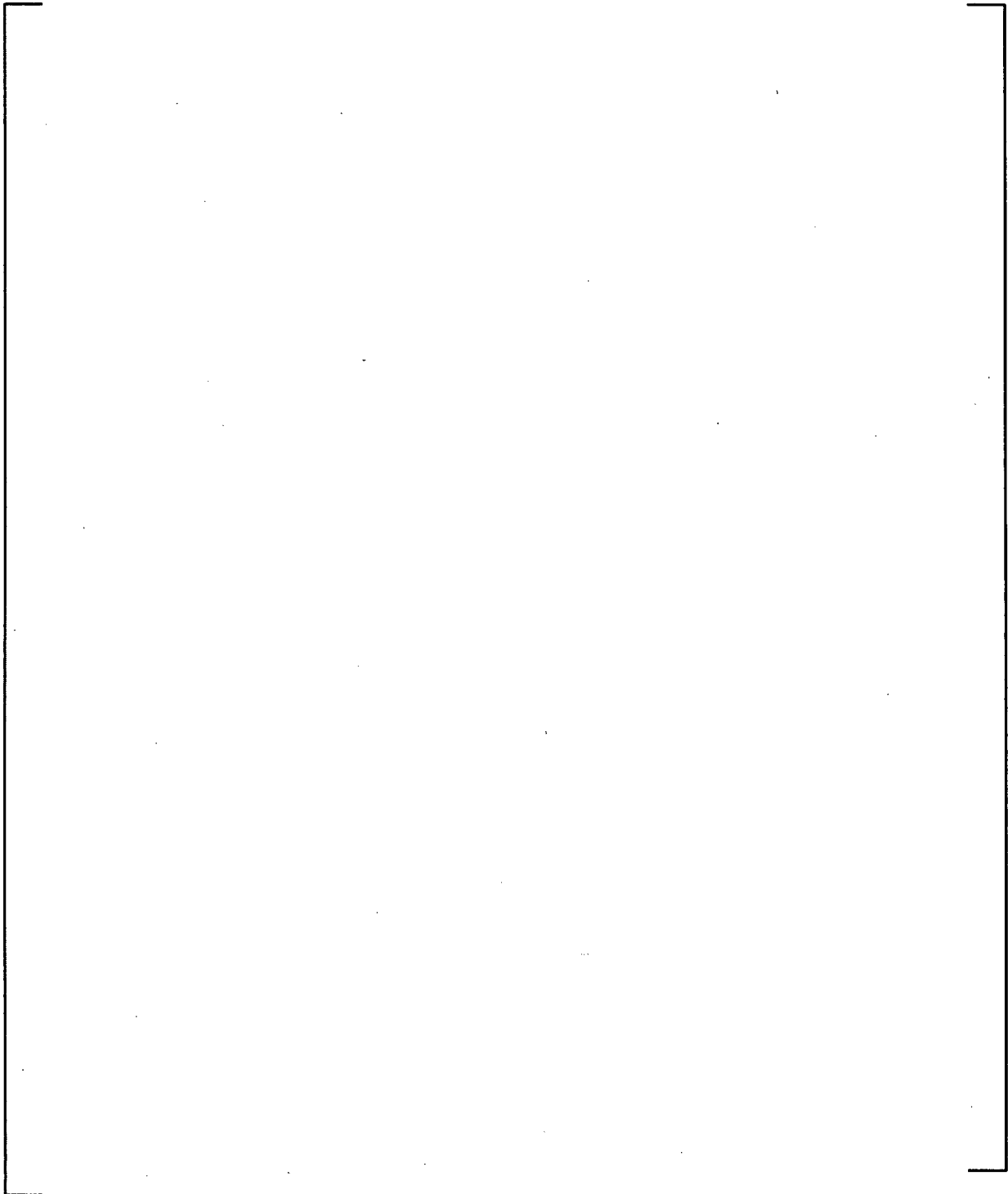


Figure 2.2-1
Watts Bar Unit 2 PAMS Hardware Architecture



a,c

Figure 2.2-2
Watts Bar Unit 2 PAMS Typical Cabinet Layout

2.2.1 Hardware/Software Changes

The following is a summary compilation of hardware and software related changes (from that which was approved in the generic Common Q design described in the NRC SERs) applicable to the WBN2 PAMS application:

2.2.2 Hardware

1. Common Q power supply (*Evolutionary Product Maintenance/Improvements*)
2. Common Q flat panel display system []^{a,c}
 - a. 15" flat panel display
 - b. PC node box
 - c. CI527 AF100 peripheral component interconnect (PCI) interface card
3. Common Q TC514 AF100 fiber optic modems (*Evolutionary Product Maintenance/Improvements*)
4. Common Q AC160 (*Evolutionary Product Maintenance/Improvements, except where noted*)
 - a. PM646A processor module
 - b. CI631 AF100 communication interface module
 - c. AI687 analog input card (RTDs and T/Cs) (*New Module*)
 - d. AI688 analog input card (voltage and current loops) (*New Module*)
 - e. DO620 digital output card

2.2.3 Software

1. Common Q AC160 (*Fix Errors, except where noted*)
 - a. 1.3/0: Revision level at time of SER
 - b. 1.3.1: Revision level to correct errors from Oskarshamn system testing
 - c. 1.3/2 - /4: Corrected minor field reported errors, many not applicable to Common Q applications
 - d. 1.3/5 - /8: (*Modifications to support the Dungeness project in the United Kingdom and inclusion of AI687/AI688 libraries*)
2. [
 - a.
 - b.
 - c.
 - d.
 - e.]^{a,c}

SECTION 3 GENERIC OPEN ITEMS

During its review, the NRC staff identified 10 generic open items (GOIs) in Section 7 of the Reference 2 safety evaluation of the Common Q platform. Resolution was provided by Westinghouse as part of the NRC review process. The NRC issued an SER that generically closed all of the GOIs, with the exception of GOI 7.8 (loop controllers), which will not be used for the WBN2 Common Q PAMS. The generic information provided in the NRC review of Common Q and the additional information provided in this report provides closure of all of the GOI items for WBN2 Common Q PAMS.

Each GOI and its resolution are presented below.

3.1 GOI 7.1

Westinghouse (formerly CENP) has committed to develop a new I/O module or re-design some of those already considered for use in the Common Q platform in order to meet the performance requirements of EPRI TR-107330.

GOI 7.1 Resolution

A new analog input (AI) module, the AI685, has been developed, and qualified per the requirements in EPRI TR-107330 (Reference 25). The previous S600 resistance-temperature detector (RTD) and thermocouple (T/C) modules did not have adequate sampling time for inputs required for protection. The AI685 can be configured for use as a voltage, RTD, or T/C analog input and has been qualified for environmental, seismic and EMC conditions. The AI685 design and qualification are documented in Reference 12. This report was submitted to the NRC in August 2002.

On February 24, 2003 the NRC issued Reference 4. This report states that the AI685 analog input module is acceptable for use in safety systems in nuclear power plants. Also, the staff reviewed the changes that incorporate the AI685 into Revision 2 of the main body of the topical report and concluded that these changes are appropriate and acceptable.

Item GOI 7.1 was previously closed by the NRC by the Common Q review process. The AI685 analog input module will not be used on the WBN2 Common Q PAMS. The WBN2 Common Q PAMS is using the AI687 and AI688 analog input modules. Therefore the resolution of GOI 7.1 is not applicable to the WBN2 PAMS.

3.2 GOI 7.2

Westinghouse (formerly CENP) has not yet finalized the selection of the Common Q power supplies.

GOI 7.2 Resolution

The Common Q power supply system has been developed and qualified for environmental, seismic, and EMC conditions. This is documented in Reference 12. This report was submitted to the NRC in August 2002.

On February 24, 2003 the NRC issued Reference 4. This report states that the staff has audited the development of the supplemental Common Q hardware and finds that Westinghouse has continued to

follow its prescribed procedures. The staff concluded on that basis that the Common Q power supplies, as well as the other supplemental Common Q hardware components included in the Summary Qualification Report, are manufactured and/or dedicated in accordance with the applicable regulatory 10CFR Part 50, Appendix B, quality assurance requirements.

Item GOI 7.2 was previously closed by the NRC by the Common Q review process.

3.3 GOI 7.3

Westinghouse (formerly CENP) has not submitted information on the design or dedication of the hardware watchdog timer and it has not yet been subjected to testing for environmental qualification.

GOI 7.3 Resolution

The internal PM646A watchdog timer meets the requirements for this on-line monitoring tool for Common Q system applications. Environmental qualification testing of the PM646A has been completed. This is documented in Reference 12. This report was submitted to the NRC in August 2002. A revision to the Common Q topical report was also submitted that describes the use of the internal PM646A watchdog timer.

On February 24, 2003 the NRC issued Reference 4. This report states that the staff has concluded that the internal PM646A watchdog timer has been qualified to meet the EMC, environmental, and seismic requirements for digital I&C safety systems in nuclear power plants to stated conditions. Westinghouse has acceptably addressed the staff's concerns regarding the qualification of the Common Q components. Also, the staff has reviewed the substitution of the built-in hardware watchdog timer function for the previously planned separate hardware watchdog timer module and concluded that the substitution of the built-in watchdog timer function in the design continues to meet the applicable regulatory requirements. The staff concluded, therefore, that these changes to the text in the topical report and appendices are appropriate and acceptable.

Item GOI 7.3 was previously closed by the NRC by the Common Q review process.

3.4 GOI 7.4

Westinghouse (formerly CENP) has committed to arrange a value-added reseller agreement with QSSL that is similar to BA AUT-99-ADVANT-00, the value-added reseller agreement it has with ABB products. A value-added reseller agreement is needed to satisfy the configuration control and incoming inspection requirements of EPRI TR-106439.

GOI 7.4 Resolution

On June 22, 2001 the NRC issued Reference 7. This report states that the staff has reviewed the value-added reseller agreement with QNX software systems limited (QSSL), the vendor for the flat panel display system (FPDS) operating system and display system, and concludes that it satisfies the configuration control and incoming inspection guidance of EPRI TR-106439 (Reference 24). The reseller agreement is, therefore, acceptable.

Item GOI 7.4 was previously closed by the NRC by the Common Q review process.

3.5 GOI 7.5

Westinghouse (formerly CENP) will perform additional EMC tests and measurements on the PM646.

GOI 7.5 Resolution

The PM646 processor module has been modified to the PM646A. This modification involved the removal of an internal terminating resistor for the High-Speed Data Links (HSLs). The link termination resistor is now external to the module, permitting high-speed data link output to multiple processors using a multi-drop configuration. Additional EMC tests and measurements were performed using the PM646A. These tests are documented in Reference 12. This report was submitted to the NRC in August 2002. A revision to the Common Q topical report was also submitted that describes the modification of the PM646 to the PM646A.

On February 24, 2003 the NRC issued Reference 4. This report states that the staff concluded that the internal PM646A processor module has been qualified to meet the EMC, environmental, and seismic requirements for digital I&C safety systems in nuclear power plants to stated conditions. Westinghouse has acceptably addressed the staff's concerns regarding the qualification of the Common Q components. Also, the staff has reviewed the change in resistor in the processor module and concurred that the resistor change is inconsequential and is, therefore, acceptable. The staff concluded that the PM646 and PM646A processor modules may be used interchangeably to suit the configuration requirements of the specific application.

Item GOI 7.5 was previously closed by the NRC by the Common Q review process.

3.6 GOI 7.6

Westinghouse (formerly CENP) has not yet conducted seismic and environmental qualification testing on the non-AC160 hardware components. Items not yet tested include the FPDS, watchdog timer, and power supply modules.

GOI 7.6 Resolution

Seismic and environmental qualification testing on the non-AC160 hardware components has been completed. These components include the FPDS and the power supply modules. The external watchdog timer is no longer required. The internal PM646A watchdog timer meets the requirements for this on-line monitoring tool for Common Q system applications (refer to resolution of GOI 7.3 above). The seismic and environmental testing is documented in Reference 12. This report was submitted to the NRC in August 2002. A revision to the Common Q topical report was also submitted that describes the use of the internal PM646A watchdog timer.

On February 24, 2003 the NRC issued Reference 4. This report states that the staff has audited the development of the supplemental Common Q hardware and finds that Westinghouse has continued to follow its prescribed procedures. The staff concluded on that basis that the supplemental Common Q hardware components included in the Summary Qualification Report are manufactured and/or dedicated in accordance with the applicable regulatory 10CFR Part 50, Appendix B, quality assurance requirements. The staff concluded that Westinghouse has acceptably addressed the staff's concerns regarding the qualification of the Common Q components, both AC160 and non-AC160.

Item GOI 7.6 was previously closed by the NRC by the Common Q review process.

3.7 GOI 7.7

The staff has reviewed the information in the SVVP about software module testing and finds that the information provided is not sufficient for the staff to arrive at a conclusion about the adequacy of the scope of the tests for validating a software module.

GOI 7.7 Resolution

On June 22, 2001 the NRC issued Reference 7. This report states that Westinghouse submitted additional information indicating in which sections of CE-CES-195, Rev. 01, "Software Program Manual for Common Q Systems", and topical report CENPD-396-P, Rev. 1, "Common Qualified Platform," the staff would find the Westinghouse procedures for performing software module testing. The staff has reviewed the indicated sections and concludes that the procedures specified therein satisfy the software verification and validation program (SVVP) requirements of IEEE Std 7-4.3.2-1993 with regard to testing of software modules and are, therefore, acceptable.

Item GOI 7.7 was previously closed by the NRC by the Common Q review process.

3.8 GOI 7.8

Westinghouse (formerly CENP) needs to provide in future submittals the design information for the loop controllers to support their diversity from the Common Q components.

GOI 7.8 Resolution

This GOI relates to the "level 3 loop controllers" referenced in the Common Q topical report integrated solution (Appendix 4). The level 3 loop controllers (LCs) provide component control based on signals from the ESFAS. The loop controllers (i.e., Component Interface Modules, CIMS) are not being used in the WBN2 PAMS, therefore the resolution of GOI 7.8 is not applicable to the WBN2 Common Q PAMS.

3.9 GOI 7.9

The staff has reviewed the approach for the integrated solution of using the ITPs and the AF100 buses to provide separation of safety and non-safety signals and finds that there is not sufficient detail to permit an evaluation against the independence requirements set forth in IEEE Std 7-4.3.2. This must be the subject of a future Westinghouse (formerly CENP) submittal.

GOI 7.9 Resolution

On June 22, 2001 the NRC issued a safety evaluation Report, Reference 7. This report states that Westinghouse has revised Appendix 4, "Common Qualified Platform Integrated Solution," to provide additional information on the use of the interface and test processors (ITPs) and the AF100 buses to provide separation of safety and non-safety signals. The staff has reviewed the revised information in Appendix 4, Rev. 2 on the use of the ITPs and the AF100 buses to provide separation of safety and non-safety signals and finds that the conceptual approach as presented therein is consistent with the independence requirements set forth in IEEE Std 7-4.3.2. The staff, therefore, concludes that this

conceptual approach may be used for guidance for the anticipated application-specific and plant-specific designs involving the integration of multiple Common Q digital instrumentation and control (I&C) upgrades. This closes GOI 7.9 as far as the conceptual approach is concerned, but the evaluation of each forthcoming design remains a plant-specific action item because the staff finds that the forthcoming details of the actual designs may require an evaluation against the independence requirements for safety systems in specific nuclear power plants.

The Common Q systems installed at WBN2 are the safety related PAMS and the non-safety-related computer enhanced rod position indication (CERPI) system. Neither the PAMS nor CERPI system architectures incorporate the ITP. While both systems utilize the AF100 bus design for communication, there is no connection between the CERPI and PAMS AF100 buses. Therefore, the resolution of GOI 7.9 is not applicable to the WBN2 Common Q PAMS.

3.10 GOI 7.10

The evaluation of the design for the multi-channel operator station control for the integrated solution requires detail beyond the scope of the present submittals.

GOI 7.10 Resolution

Common Q multi-channel operator stations (for control) are not used in the WBN2 design; therefore GOI 7.10 is not applicable to the WBN2 Common Q PAMS.

SECTION 4 PLANT SPECIFIC ACTION ITEMS

The following information describes TVA's response to the fourteen (14) plant specific action items that the NRC outlined in their SE for WCAP-16097-P-A (Reference 2).

4.1 Plant Specific Action Item 6.1

Each licensee implementing a specific application based upon the Common Q platform must assess the suitability of the S600 I/O modules to be used in the design against its plant-specific input/output requirements.

TVA Response to PSAI 6.1

The suitability of all new components is assessed to meet applicable requirements in accordance with the WBN2 Quality Assurance Program. Performance requirements for these components are assured, for example, by specifying them in purchase contracts, observing vendor testing and analysis, reviewing and commenting on vendor design requirements and specifications, performing design reviews by the engineering department, witnessing the vendor Factory Acceptance Tests (FAT), and by performing post modification and Site Acceptance tests after installation. All these activities are controlled by WBN2 administrative procedures and/or project quality plans.

The PAMS input/output categories and the S600 input/output module used to provide the interface are provided in Table 4.1-1 below.

Table 4.1-1 PAMS Input/Output Signals

Item	I/O Signal Type	S600 I/O Module
1.	Contact Inputs wetted by the PAMS auctioneered 24Vdc auxiliary power supplies.	DI620
2.	Type K Thermocouple, 100 Ω platinum RTD	AI687
3.	4 – 20 mA Analog Inputs	AI688
4.	24 Vdc logic level signals (to interposing relay panel)	DO620
5.	4 – 20 mA Analog Outputs	AO650

The S600 Input/Output modules are designed to fully meet the functional and signal interface requirements for the PAMS input sensors and output loads as required by TVA as clarified in the Westinghouse Compliance Matrix (Reference 9). The S600 Input/Output modules are demonstrated to be capable of performing their design function by successful completion of testing, culminating in a Factory Acceptance Test (FAT) to be performed by the vendor at the Westinghouse manufacturing/engineering facility. Acceptance criteria are based on the PAMS System Requirements Specification (Reference 10) and the PAMS System Design Specification (Reference 11).

4.2 Plant Specific Action Item 6.2

A hardware user interface that replicates existing plant capabilities for an application may be chosen by a licensee as an alternative to the FPDS. The review of the implementation of such a hardware user interface would be a plant-specific action item.

TVA Response to PSAI 6.2

The PAMS utilizes the flat panel display system (FPDS) as developed by Westinghouse for Common Q safety systems. An alternative hardware interface is not used. Therefore, PSAI 6.2 is not applicable.

4.3 Plant Specific Action Item 6.3

If a licensee installs a Common Q application that encompasses the implementation of FPDS, the licensee must verify that the FPDS is limited to performing display and maintenance functions only, and it is not to be used such that it is required to be operational when the Common Q system is called upon to initiate automatic safety functions. The use of the FPDS must be treated in the plant specific FMEAs.

TVA Response to PSAI 6.3

The FPDS purchased by TVA is limited to performing display and maintenance functions only. The plant-specific Failure Mode Effects Analysis (FMEA) prepared in accordance with PSAI 6.10 will address the loss of the FPDS. Additionally, the NRC in their safety evaluation for the closeout of several of the Common Qualified Platform Category 1 Open Items Related to Reports CENPD-396-P, Revision 1 and CE-CES-195, Revision 1, dated June 22, 2001 (Reference 7) has stated that this action item (PSAI 6.3) has been generically resolved and is considered closed. Therefore, no further evaluation is required.

4.4 Plant Specific Action Item 6.4

Each licensee implementing a Common Q application must verify that its plant environmental data (i.e., temperature, humidity, seismic, and electromagnetic compatibility) for the location(s) in which the Common Q equipment is to be installed are enveloped by the environment considered for the Common Q qualification testing, and that the specific equipment configuration to be installed is similar to that of the Common Q equipment used for the tests.

Westinghouse configured the Common Q test specimen for seismic testing using dummy modules to fill all the used rack slots. As part of the verification of its plant-specific equipment configuration the licensee must check that it does not have any unfilled rack slots.

TVA Response to PSAI 6.4 (Temperature & Humidity)

The PAMS equipment is located in the Auxiliary Instrument Room (AIR) and Main Control Room (MCR) in a mild environment. The PAMS equipment will be exposed to the following environmental conditions during the life of the plant.

Table 4.4-1 WBN2 PAMS Plant-Specific Operating Environment Parameters

Parameter	Abnormal		Duration
	Min	Max	
Temperature	60 °F	104 °F	12 Hours
Humidity	10 % RH*	90% RH*	12 Hours
Pressure	Atmospheric	Atmospheric	Continuous

*(non-condensing)

The environmental conditions described below are the abnormal conditions for which the Common Q system is generically qualified (Reference 12). No condensation formed on the test item during any phase of the testing.

Table 4.4-2 WBN2 PAMS Generic Qualification Environment Parameters

Parameter	Abnormal		Duration
	Min	Max	
Temperature	40 °F	140 °F	12 Hours
Humidity	20% RH	95% RH	12 Hours
Pressure	Atmospheric	Atmospheric	Continuous

During anticipated abnormal transients/accident conditions, the essential HVAC system maintains the essential areas that contain the PAMS equipment (cabinets at AIR Elevation 708', Operators' Module (OM) at MCR Elevation 755') within design ambient temperature, pressure and humidity conditions (References 20 and 21). Based on the above, the environment considered for the Common Q qualification testing envelopes the specific WBN2 temperature and humidity conditions.

TVA Response to PSAI 6.4 (Seismic)

The seismic qualification of the Common Q equipment for the WBN2 PAMS has been completed by Westinghouse for most of the components except for newly released components (AI687, AI688) and upgraded components (PC node box, Flat Panel Displays and Common Q power supply). All of the Common Q components being used in the WBN2 PAMS have been qualified, or will be qualified, to the Common Q Platform generic seismic envelope specified in Reference 12. Results of specific qualification testing for both new and existing components will be reported in the WBN2 Final EQ Summary Test Report. TVA has evaluated the Required Response Spectra (RRS) cited in the Westinghouse Seismic Test Plan for OBE, SSE, and Table Limits and has determined that they are higher than the WBN2 floor response spectra curves (Reference 13) for the area where the PAMS equipment will be installed (cabinets at AIR Elevation 708', Operators' Module (OM) at MCR Elevation 755') and therefore, envelopes the seismic criteria for WBN2.

The dummy modules populating the unused chassis slots during seismic testing are essentially the outer cases and front faces of modules similar in size and appearance to the active modules, but lacking the internal electronics and associated hardware.

Installation of the Common Q PAMS hardware at WBN2 will include dummy modules in unused chassis slots. Plant modification document EDCR 52351 used for implementing the Common Q PAMS at WBN2 will specify this requirement. WBN2 administrative procedures, which ensure equipment qualifications (e.g., seismic, etc) are maintained in the design change process, will control all future changes to the PAMS.

TVA Response to PSAI 6.4 (Electromagnetic Compatibility)

Westinghouse has performed specific electromagnetic compatibility tests on the Common Q equipment in accordance with EPRI TR-102323, Guidelines for Electromagnetic Interference Testing in Power Plants, Revision 1 (Reference 3). For newly released components (AI687, AI688) and upgraded components (PC node box, Flat Panel Displays and Common Q power supply), Westinghouse will provide a Common Q PAMS Equipment Qualification (EQ) summary report containing the electromagnetic compatibility test results. TVA will use the Westinghouse EQ summary report and compare the results to NUREG/CR-6431 (Reference 5) and TVA's EMI/RFI Design Standard (Reference 16). TVA will perform an EMI survey of the PAMS indication system.

4.5 Plant Specific Action Item 6.5

On the basis of its review of the Westinghouse software development process for application software, the staff concludes that the SPM specifies plans that will provide a quality software life cycle process, and that these plans commit to documentation of life cycle activities that will permit the staff or others to evaluate the quality of design features upon which the safety determination will be based. The staff will review the implementation of the life cycle process and the software life cycle process design outputs for specific applications on a plant specific basis.

TVA Response to PSAI 6.5

In accordance with the TVA Quality Assurance Program, TVA uses administrative control procedures to establish software quality assurance and configuration management for process computer software, firmware, software development computer systems, and associated documentation. They ensure that the integrity of a process software product is known and preserved throughout its life cycle from development to retirement. These controls also apply to the development tools and systems used to develop and test process software.

As required by administrative control procedures, TVA will maintain documentation of the Common Q PAMS Software Life Cycle Process provided by Westinghouse for both the Implementation Activities and the required Design Outputs. This documentation is for internal use and to allow for the NRC staff review. This documentation will include life cycle process documentation provided by Westinghouse (i.e., Safety Analysis Activities, V&V plans, V&V results, Testing Results) as well as installation test activities performed and documented by TVA in accordance with SPP 9.3, Plant Modifications and Engineering Change Control (Reference 17) and SPP 2.6, Computer Software Control (Reference 18).

Per procedural requirements, TVA also maintains the requirements documents provided by Westinghouse (i.e., Functional Design Requirements, System Requirements Specifications, Software Requirements Specifications), design output documents (i.e., Software Release Records, executable software on media, and Factory Acceptance Test reports) as well as Operations and Maintenance Manuals.

4.6 Plant Specific Action Item 6.6

When implementing a Common Q safety system (i.e. PAMS, CPCS, or DPPS), the licensee must review Westinghouse's timing analysis and validation tests for that Common Q system in order to verify that it satisfies its plant specific requirements for accuracy and response time presented in the accident analysis in Chapter 15 of the safety analysis report.

TVA Response to PSAI 6.6

The acceptable accuracy requirements associated with the Common Q PAMS are those given in the WBN2 Functional Requirements Document (FRD), Section 21 (Reference 15). TVA will review the WBN2 Common Q PAMS plant-specific system accuracy specifications provided by Westinghouse, and ensure that they are equal to or better than that of the WBN1 ICCM-86. In addition, accuracy verification testing will be performed as part of the PAMS Factory Acceptance Test (FAT) on each train to be installed at WBN2. TVA will review Westinghouse Final Factory Acceptance Test Report to ensure plant specific requirements for accuracy as specified in the WBN2 FRD have been met:

- Common Q PAMS Accuracy; WAT/WBT-300/21.3.3

In addition to the above activities, the following Calculation Notes to support the Setpoint and Scaling Documents to be developed for Common Q. These documents will be reviewed and approved by TVA.

- Core Exit Thermocouples
- Core Exit Thermocouples Reference Junction Temperature
- Reactor Vessel Level Transmitters
- Reactor Vessel Level
- Subcooled Margin Monitor

4.7 Plant Specific Action Item 6.7

The OM and the MTP provide the human machine interface for the Common Q platform. Both the OM and MTP will include display and diagnostic capabilities unavailable in the existing analog safety systems. The Common Q design provides means for access control to software and hardware such as key

switch control, control to software media, and door key locks. The human factors considerations for specific applications of the Common Q platform will be evaluated on a plant-specific basis.

TVA Response to PSAI 6.7

As required by WBN2 Plant Modification procedures and as described in Sections 7.5.1.5.1 and 7.5.1.6 of the UFSAR, the PAMS upgrade project undergoes a TVA Human Factors Engineering (HFE) Review in accordance with TVA Design Standard DS-E18.1.24, Human Factors Engineering (Reference 22), prior to the system being installed. The HFE Review will focus on design features and characteristics of the new PAMS to ensure that the system incorporates acceptable human factors engineering principles and that the system provides the necessary system information, control capabilities, feedback, and analytical aids necessary for control room operators to accomplish their functions effectively.

4.8 Plant Specific Action Item 6.8

If the licensee installs a Common Q PAMS, CPCS or DPPS, the licensee must verify on a plant-specific basis that the new system provides the same functionality as the system that is being replaced, and meets the functionality requirement applicable to those systems.

TVA Response to PSAI 6.8

As part of the normal design change process at WBN2, the suitability of all new and upgraded systems is assessed. This review covers the overall function of the system, as well as the design and licensing basis of the system. These design attributes were captured in Westinghouse Letter WBT-D-0088 (Reference 9) for the PAMS upgrade project and detail the conditions of service and general requirements that must be met in the Common Q PAMS. This reference defines the necessary performance requirements to assure functionality is maintained with the new system. Enhancements to the PAMS are occurring as part of the Common Q design evaluation process for WBN2. In every case, performance requirement factors are being taken into account to ensure that the new PAMS will provide, at a minimum, the same functionality as the system that is being replaced.

4.9 Plant Specific Action Item 6.9

Modifications to plant procedures and/or TS due to the installation of a Common Q safety system will be reviewed by the staff on a plant-specific basis. Each licensee installing a Common Q safety system shall submit its plant-specific request for license amendment with attendant justification.

TVA Response to PSAI 6.9

As part of the normal design change process at WBN2, the impact to plant procedures and Technical Specifications (TS) are evaluated for all design changes. TVA will ensure that any plant procedure and/or TS (Section 3.3.3) change associated with the PAMS is evaluated and dispositioned prior to initial fuel load.

4.10 Plant Specific Action Item 6.10

A licensee implementing any Common Q applications (i.e., PAMS, CPCS, or DPPS) must prepare its plant specific model for the design to be implemented and perform the FMEA for that application.

TVA Response to PSAI 6.10

A plant specific Failure Modes and Effects Analysis (FMEA) for the WBN2 PAMS will be completed by Westinghouse. In general there have been no changes in the way that the PAMS will respond to input failures. This FMEA will confirm that no single failure associated with the replacement PAMS will defeat more than one of the two safety divisions, assuring operability at the system level.

4.11 Plant Specific Action Item 6.11

If a licensee installs Common Q PAMS, CPCS, DPPS or Integrated Solution, the licensee shall demonstrate that the plant-specific Common Q application complies with the criteria for defense against common-mode failure in digital instrumentation and control system and meets the requirements of HICB BTP-19.

TVA Response to PSAI 6.11

The level of Diversity and Defense-in-Depth (D3) for the WBN2 PAMS digital-to-digital replacement is equal to or greater than that provided by the ICCM-86 system. The PAMS supports the monitoring and indicator system echelon of defense that affords the operators accurate plant information to enable them to react to unexpected events.

BTP 7-19 Rev. 5 (Reference 6) requires "A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions. The displays and controls should be independent and diverse from the computer-based safety systems identified in Points 1 and 3". The Eagle 21 system is the only computer based safety system installed at WBN2 that is within the engineered safety features actuation system echelon as defined in BTP 7-19 Rev. 5.

The Common Q PAMS receives wide range RCS pressure, wide range T_{hot} and delta T power inputs from the Eagle 21 system. These inputs are used in the subcooled margin monitor (SMM) and RVLIS functions. A failure of one of the Eagle 21 channels would result in a loss of the SMM and RVLIS functions in the associated PAMS train, however, the SMM and RVLIS functions in the other PAMS train would remain operational.

The CET function is diverse at the transmitter and loop level. The CET function is credited as a diverse function for the Eagle 21 T_{hot} indication in the WBN2 licensing basis.

While the Common Q PAMS receives previously identified inputs from the Eagle 21 system for the SMM and RVLIS, it is diverse from the Eagle 21 digital process protection system in the following areas:

- Human Diversity – The Common Q Platform was originally developed by designers in different companies than the Eagle 21 protection system, which results in a high level of functional diversity in the systems. This reduces the possibility of similar design errors.
- Software Diversity – The Common Q PAMS uses different programs designed and implemented by different development groups with different key personnel than that utilized by the Eagle 21 protection system.
- Equipment Diversity – The Common Q PAMS utilizes a different computer architecture and diverse computer equipment than the Eagle 21 protection system. This has resulted in the use of diverse microprocessors, compilers, linkers, and other support software.

The communications between the Eagle 21 and Common Q systems are analog 4-20ma signals. The 4-20ma output channels are isolated by hardware within the Eagle 21 system to prevent any faults from affecting the Eagle 21 safety function processors. Therefore, a common cause failure of the Common Q system software cannot cause a failure of the Eagle 21 safety related functions. This provides the necessary isolation between these echelons.

The control echelon at WBN2 is a digital Foxboro intelligent automation (IA) system. There are no shared functions or communications between the Foxboro IA system and the Common Q PAMS system. Therefore, there is no diversity requirement between these echelons.

4.12 Plant Specific Action Item 6.12

A licensee implementing a Common Q DPPS shall define a formal methodology for overall response time testing.

TVA Response to PSAI 6.12

The WBN2 licensing bases documents do not contain any specific response time requirements for the Common Q PAMS. WBN2 Emergency Operating Procedures do not require continuous monitoring of RVLIS, Subcooled Margin or Core Exit Temperatures. These parameters are checked on a periodic basis to determine the effectiveness of operator actions in restoring core cooling. The refresh rate of the OM display []^{a,c} ensures that updated data is available to the operator to make accurate assessments more frequently than required by the procedures. Therefore, PSAI 6.12 is not applicable.

4.13 Plant Specific Action Item 6.13

The analysis of the capacity of the shared resources to accommodate the load increase due to sharing.

TVA Response to PSAI 6.13

The shared resource issue relates to multiple Common Q based systems using the same resources, such as the AF100 bus or an Operator Module. The replacement PAMS and CERPI are the only Common Q hardware at WBN2. As previously stated, there is no interaction between and no communications path between the PAMS and CERPI. Therefore, PSAI 6.13 is not applicable.

4.14 Plant Specific Action Item 6.14

The licensee must ascertain that the implementation of the Common Q does not render invalid any of the previously accomplished TMI action items.

TVA Response to PSAI 6.14

TMI action items from 50.34(f)(2) that are relevant to the WBN2 implementation of a new PAMS are as follows:

- ***50.34(f)(2)(i) – Provide simulator capability that correctly models the control room and includes the capability to simulate small-break LOCA's (I.A.4.2)***

The Simulator used to train WBN2 Licensed Operators is designed to model the Unit 1 control room including the capability to simulate small-break LOCAs. TVA will address the Unit 1/Unit 2 differences, including the Common Q displays, with operator training.

- ***50.34(f)(2)(iii) – Provide, for Commission review, a control room design that reflects state-of-the-art human factor principles prior to committing to fabrication or revision of fabricated control room panels and layouts. (I.D.1)***

As stated above, the PAMS replacement project, as required by FSAR and plant procedures, undergoes a TVA Human Factors Engineering (HFE) review in accordance TVA Design Standard DS-E18.1.24, Human Factors Engineering (Reference 22), prior to the system being installed. The HFE review will focus on design features and characteristics of the PAMS to ensure that the system incorporates acceptable human factors engineering principles and that the system provides the necessary information, operator navigation capabilities, feedback, and analytical aids necessary for control room operators to accomplish their functions effectively.

- ***50.34(f)(2)(xviii) – Provide instruments that provide in the control room an unambiguous indication of inadequate core cooling, such as primary coolant saturation meters in PWR's, and a suitable combination of signals from indicators of coolant level in the reactor vessel and in-core thermocouples in PWR's and BWR's. (II.F.2)***

The Common Q PAMS digital-to-digital system replacement is a functionally equivalent replacement of the ICCM-86 system. As such, it is a direct replacement for a system that accomplished the aforementioned safety functions.

Therefore, the Common Q PAMS implementation at WBN2 does not render invalid any of the previously accomplished TMI action items.

SECTION 5 INTERDIVISIONAL COMMUNICATIONS

5.1 System Function

The WBN2 PAMS monitors a subset of the variables listed in Table 2 of Regulatory Guide 1.97, Revision 2 (RG 1.97) in support of the following functions:

- Core exit thermocouple (CET) monitoring
- Reactor vessel level monitoring
- Subcooled margin monitoring

The RG 1.97 variables are displayed on the Operator's Module (OM) and Maintenance and Test Panel (MTP). The algorithms that support the CET Monitoring, Reactor Vessel Level Monitoring, and the Subcooled Margin Monitoring are executed exclusively in the AC160's PM646A processor. The AC160 rack also contains various IO modules to support analog inputs, analog outputs, digital inputs, and digital outputs. Any alarm conditions resulting from these algorithms actuate one or more Digital Outputs that drive relays in the CQ PAMS cabinet. These relays are available for annunciation in the control room. The five relay outputs that annunciate these alarms are:

- 1.) System trouble alarm (for detectable hardware failures and for the manual disabling of the safety function under keyswitch control)
- 2.) Low reactor vessel level alarm
- 3.) Low saturation margin alarm
- 4.) High core exit temperature alarm
- 5.) ICC trouble alarm (the logical OR of the previous 3 annunciators).

5.2 Safety Classification

The WBN2 PAMS is classified as safety-grade and is implemented on the Common Q safety platform since it is required to remain operable during and following a design basis event as described in TVA Design Criteria WB-DC-30-7, Rev. 22, Post-Accident Monitoring Instrumentation (Reference 19).

The SCOPE section of DI&C-ISG-04 (Reference 14), 2nd paragraph, 2nd sentence, states "*This guidance is not applicable to interactions among equipment that are all in the same safety division or that do not involve anything that is safety-related.*" All of the communications channels (the AF100 bus, the field inputs, the signals sent from the Eagle 21 safety computers, and the Ethernet communications to plant computer) are evaluated with respect to this scope statement.

The two PAMS trains, A and B, are outfitted with identical controllers and display equipment. Each train's equipment is independent and electrically isolated from the other train. Field cabling and input signal transducers used by each train are independent and isolated from the opposite train. Signals received on the analog input cards by either PAMS train from the Eagle 21 safety system are divisionally

separated. Additionally, the AF100 bus communications for each train are entirely within the same safety division. Power is provided by the corresponding divisional vital instrumentation bus.

Due to the divisional isolation of the field input signals and the AF100 bus communications, and considering the SCOPE statement above, the 20 DI&C-ISG-04 criteria do not apply to these aspects of the WBN2 PAMS design.

Thus, the only communications interface that the DI&C-ISG-04 guidance applies to is the Ethernet (TCP/IP) communications to the plant computer. [

Additionally, the Ethernet TCP/IP communications between the MTP and the non-safety plant computer are not vital to the performance of any safety function. Ethernet communications may be allowed to fail without impacting the PM646A processing or the OM/MTP display processing. [

Relating to the terms used in DI&C-ISG-04, in the Common Q design of the Watts Bar 2 PAMS, the [

The AC160 High Speed Link (HSL) interface as described in the Common Q Topical Report is not used in the WBN2 PAMS designs and therefore is not considered in this evaluation.

5.3 Response to Individual Criteria in DI&C-ISG-04

The WBN2 PAMS design meets each of the 20 criteria listed in the Section 1, Interdivisional Communications, of Revision 1 of DI&C-ISG-04 as explained below.

Criterion 1. A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE-603. It is recognized that division voting logic must receive inputs from multiple safety divisions.

The WBN2 PAMS design satisfies this criterion. The WBT PAMS does not receive any information from outside of its own safety division to perform its safety function.

Criterion 2. The safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.

The WBN2 PAMS design satisfies this criterion. [

All signals are contained within each safety division and no data information from outside the safety division is received by either the PM646A controller or the OM.

The MTP display system has an Ethernet port with TCP/IP communications to support printing to the plant computer via a one-way datalink from the MTP. The plant computer is non-safety equipment. The plant computer datalink is a custom protocol designed specifically to broadcast data to the plant computer. [

] a.c

No action over this Ethernet port from outside the safety boundary can affect the AC160 PM646A controller. In addition, no actions over this Ethernet port from outside the safety boundary can affect the display of the RG 1.97 variables on the OM.

Criterion 3. A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system. For example, comparison of readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (for example, On-Line Monitoring). Such a function executed within a safety system, however, could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and should not be executed within the safety system.

Receipt of information from outside the division, and the performance of functions not directly related to the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division. The applicant should justify the definition of "significantly" used in the demonstration.

The WBN2 PAMS design satisfies this criterion. All signals are contained within each safety division and no data information from outside the safety division is received by the PM646A controller or the OM.

The WBN2 PAMS processor performs only the functions necessary for the calculation and monitoring of the RG 1.97 variables allocated to this system.

Criterion 4. The communication process itself should be carried out by a communications processor separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with 10 C.F.R. Part 50, Appendix A and B. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is

accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.

The WBN2 PAMS design satisfies this criterion. [

] ^{a,c} The processor and memory of the MTP are physically separate from the PM646A controller and the OM, and thus are not shared. [^{a,c}]

The PAMS Safety Function does not depend on data received from outside the train to perform its safety function.

Criterion 5. The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.

The WBN2 PAMS design satisfies this criterion. The cycle time for the safety function processors takes into account the worst case timing constraints. The system load is monitored and an alarm limit applied to insure that the processor has sufficient resources to perform its safety function. There is no shared memory that is used by both the [

] ^{a,c} as they are physically separate.

Criterion 6. The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.

The WBN2 PAMS design satisfies this criterion. Communications to systems outside of the safety division are handled by a separate [^{a,c}]

Criterion 7. Only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the same locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.

The WBN2 PAMS design satisfies this criterion. The [

] ^{a,c}

Criterion 8. Data exchanged between redundant safety divisions or between safety and non-safety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.

The WBN2 PAMS design satisfies this criterion. No data is exchanged between safety divisions in this system.

[

It is not possible to adversely affect the safety function of the WBN2 PAMS from the non-safety side by way of the MTP Ethernet interface.

Criterion 9. Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.

The WBN2 PAMS design satisfies this criterion. The WBN2 PAMS has no incoming message data from outside of its safety channel to be used in the safety function processors. Therefore there is no storage of the incoming messages in the safety function processors.

Criterion 10. Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g., engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor/shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. "Hardwired logic" as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a "TRUE" or "1" at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.

The WBN2 PAMS design satisfies this criterion. Each PAMS division has its own MTP and OM that can only access the PM646A processor within its division. The PAMS design precludes any interconnection of the workstations between the PAMS trains.

Only setpoints can be changed while the system is in operation. Application software can only be changed when the system is offline.

Online changes (i.e., setpoints changes) can be made from the OM or the MTP in the same division as the safety function processor. Thus it is not possible to change a setpoint on the opposite train.

- Setpoint changes are prohibited by software unless that train is first taken out-of-service using the function enable (FE) keyswitch.
- Enabling the FE keyswitch causes the PAMS' "System Trouble" overhead annunciator to be activated in the main control room (via software control).
- A dedicated OM and MTP are permanently installed on each train. Since there are no inter-divisional connections, setpoints can only be changed by the associated train's OM and MTP.
- Access to the key to the FE keyswitch is administratively controlled by TVA in accordance with TI-12.09, Plant Key Control (Reference 23).

Application software (i.e., software loads) changes can only be made with a PAMS train inoperable.

- The PAMS must be taken out of service to load software.
- Software can only be loaded via the MTP. This feature is not available on the OM.
- [

]a,c

- The MTP is a permanently connected maintenance workstation used to modify that train's software.
- Each train's MTP and SLE keyswitch is installed in a separate locked cabinet. Access to these cabinets is controlled administratively by TVA via cabinet locks in accordance with TI-12.09, Plant Key Control.
- Enabling the SLE keyswitch causes the PAMS' "System Trouble" overhead annunciator to be activated in the main control room. []a,c
- [

]a,c

- Access to the key to the SLE keyswitch is administratively controlled by TVA in accordance with TI-12.09, Plant Key Control.

In addition to the above controls, the OM and MTP are located in vital areas which restrict access to only authorized personnel.

Criterion 11. Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.

The WBN2 PAMS design satisfies this criterion. As stated previously, the WBN2 PAMS has no incoming message data from outside of its safety channel to be used in the safety function processors. Therefore the progress of the safety function processors through its instruction sequence will not be affected.

Criterion 12. Communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in non-safety equipment, do not constitute "single failures" as described in the single failure criterion of 10 C.F.R. Part 50, Appendix A. Examples of credible communication faults include, but are not limited to, the following:

- *Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.*
- *Messages may be repeated at an incorrect point in time.*
- *Messages may be sent in the incorrect sequence.*
- *Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.*
- *Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.*
- *Messages may be inserted into the communication medium from unexpected or unknown sources.*
- *Messages may be sent to the wrong destination, which could treat the message as a valid message.*
- *Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.*
- *Messages may contain data that is outside the expected range.*
- *Messages may appear valid, but data may be placed in incorrect locations within the message.*
- *Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).*
- *Message headers or addresses may be corrupted.*

The WBN2 PAMS design satisfies this criterion. The signal data acquisition, the algorithms execution, and the setting of the annunciator output relays by the PM646A controller, cannot be impacted by any postulated communications failure at the Ethernet controller in the MTP. Ethernet communications failures in the MTP cannot impact the PM646A processor or the OM displays.

Criterion 13. Vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting methods, if used, should be shown to always reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor.

The WBN2 PAMS design satisfies this criterion. "Vital" communications is defined to be communications that are needed to support a safety function and the failure of vital communications could inhibit the performance of a safety function.

Ethernet communications between the MTP and the non-safety equipment (plant computer) are not vital to the performance of any safety function.

Criterion 14. Vital communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, "point-to-point" means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.

The WBN2 PAMS design satisfies this criterion. "Vital" communications is defined to be communications that are needed to support a safety function and the failure of vital communications could inhibit the performance of a safety function. The WBT PAMS system has no such vital communication interfaces. Ethernet communications between the MTP and the non-safety equipment (plant computer) are not vital to the performance of any safety function.

Criterion 15. Communication for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.

The WBN2 PAMS satisfies this criterion. No data is received from outside the safety division.

Criterion 16. Network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of: (1) 10 C.F.R. Part 50, Appendix A, General Design Criteria ("GDC") 24, which states, "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."; and (2) IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.) (Source: NUREG/CR-6082, 3.4.3)

Per BTP 7-19 Rev. 5 (Reference 6), the WBN2 Common Q PAMS is within the monitoring and indication echelon. It does not connect to or communicate with the control echelon (Foxboro IA). The connection to the ESFAS (Eagle 21) is the receipt of 4-20ma analog signals from Eagle 21. As previously described the Eagle 21 output is isolated electrically within the Eagle 21 system. Since there is no communications protocol in the receipt of an analog signal, a failure of the Common Q PAMS cannot cause a deadlock or livelock of the ESFAS. Therefore this criterion does not apply to the Common Q PAMS.

Criterion 17. Pursuant to 10 C.F.R. § 50.49, the medium used in a vital communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.

The WBN2 PAMS satisfies this criterion. The WBT PAMS system does not receive any vital communications from outside its own safety division. The MTP out-bound TCP/IP communication is not vital to any PAMS safety function. The WBN2 PAMS is installed in a mild environment. Qualification testing of the equipment for continuous use exceeds the environmental conditions for the installation (see Section 4.4). EMI/RFI testing is performed to industry standards (Reference 3) to insure acceptable performance.

Criterion 18. Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

The WBN2 PAMS satisfies this criterion. All MTP TCP/IP communications is out-bound only and is not vital. A failure modes and effect analysis (FMEA) will be prepared for this system and the TCP/IP interface will be included in this analysis.

Criterion 19. If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.

The WBN2 PAMS satisfies this criterion. The PM646A controller and the OM do not receive any vital communications from outside their own safety division. A data storm test is required as part of the Factory Acceptance Test in accordance with WBN2 Common Q purchase specification.

Criterion 20. The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.

There are no response time criteria in the WBN2 licensing basis for the post-accident monitoring system (see Section 4.12). Therefore, this criterion is not applicable

The WBN2 PAMS does not perform any actuation functions. Therefore Section 2, Command Prioritization, of Revision 1 of DI&C-ISG-04 is not applicable.

The WBN2 PAMS OM and MTP do not have the ability to control plant equipment and are physically separate and electrically independent of the other PAMS division. Therefore, Section 3, Multidivisional Control and Display Stations, of Revision 1 of DI&C-ISG-04 (Reference 14) is not applicable.

SECTION 6 REFERENCES

1. WCAP-16097-P-A, "Common Qualified Platform Topical Report," May 2003, including Appendices 1, 2, 3, 4, Rev. 0 and WCAP-16096-NP-A, "Software Program Manual for Common Q Systems," Rev. 1A, Westinghouse Electric Company LLC.
2. NRC Safety Evaluation Report, "Acceptance for Referencing of Topical Report CENPD-396-P, Rev. 01, 'Common Qualified Platform' and Appendices 1, 2, 3 and 4, Rev. 01 (TAC No. MA1677)," U.S. Nuclear Regulatory Commission, August 11, 2000.
3. EPRI Topical Report TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," Rev. 1, Electric Power Research Institute.
4. NRC Safety Evaluation Report, "Safety Evaluation by the Office of Nuclear Reactor Regulation Related to the Westinghouse Common Qualified Platform Closeout of Generic Open Items and Approve Changes to Topical Report CENPD-396-P, Rev. 01, Common Qualified Platform," February 24, 2003.
5. NUREG/CR-6431, "Recommended Electromagnet Operating Envelopes for Safety Related I&C Systems in Nuclear Power Plants," U.S. Nuclear Regulatory Commission.
6. NUREG-0800, Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-based Instrumentation and Control Systems", Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.
7. ML011690170, "Safety Evaluation for the Closeout of Several of the Common Qualified Platform Category 1 Open Items related to Reports CENPD-396-P, Revision 1, and CE-CES-195, Rev. 1 (TAC NO. MB0780)", U.S. Nuclear Regulatory Commission, June 22, 2001.
8. ML030550776, "Acceptance of the Changes to Topical Report CENPD-396-P; Rev. 01, "Common Qualified Platform", and Closeout of Category 2 Open Items (TAC NO. MB2553)," U.S. Nuclear Regulatory Commission.
9. WBT-D-0088, "Transmittal of Westinghouse Comments on TVA Specification EDCR52351", Westinghouse Electric Company LLC, July 10, 2008.
10. WNA-DS-01617-WBT, "Post Accident Monitoring System - System Requirements Specification," Rev. 1, Westinghouse Electric Company LLC.
11. WNA-DS-01667-WBT, "Post Accident Monitoring System – System Design Specification," Rev. 1, Westinghouse Electric Company LLC.
12. 00000-ICE-37764, "Summary Qualification Report of Hardware Testing for Common Q Applications," Westinghouse Electric Company LLC, August 2002.

13. TVA Design Criteria WB-DC-40-31.2, Attachment A Rev. 12 “Seismic Qualification of Category I Fluid System Components and Electrical or Mechanical Equipment,” Tennessee Valley Authority.
14. DI&C-ISG-04, “Task Working Group #4: Highly-Integrated Control Rooms – Communications Issues (HICRe) Interim Staff Guidance”, U.S. Nuclear Regulatory Commission, Rev. 1 (ML083310185)
15. WAT/WBT-300/21, “Inadequate Core Cooling Monitoring System”, Westinghouse Electric Company LLC, Rev. 7.
16. TVA Purchase Specification “WBN Unit 2 Post Accident Core Monitoring System”. Supplement to PEG package EDCR52351M0, Tennessee Valley Authority.
17. TVA Procedure SPP 9.3 Rev. 21, Plant Modifications and Engineering Change Control, Tennessee Valley Authority.
18. TVA Procedure SPP 2.6 Rev. 12, Computer Software Control, Tennessee Valley Authority.
19. TVA Design Criteria WB-DC-30-7 Rev. 22, Post Accident Monitoring Instrumentation, Tennessee Valley Authority.
20. TVA Drawing 47E235-16 Rev. 4, Environmental Data (Main Control Room elevation 755), Tennessee Valley Authority.
21. TVA Drawing 2-47E235-17 Rev. 0, Environmental Data Environment - Mild EL 708.0 (Auxiliary Instrument Room), Tennessee Valley Authority.
22. TVA Design Standard DS-E18.1.24 Rev. 0, Human Factors Engineering, Tennessee Valley Authority.
23. TVA Technical Instruction TI-12.09 Rev. 4, Plant Key Control, Tennessee Valley Authority.
24. EPRI Topical Report TR-106439, “Guidelines on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” Electric Power Research Institute, October 1996.
25. EPRI Topical Report TR-107330, “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants,” Electric Power Research Institute, December 1996.

SECTION 7 CODES AND STANDARDS APPLICABLE TO THE COMMON Q PAMS

The applicable NRC regulatory guides, IEEE and EPRI industry standards for the Common Q PAMS are shown below. Compliance to these codes and standards are stated in Section 4 of Reference 1.

1. Regulatory Guide 1.22, February 1972, "Periodic Testing of Protection System Actuation Functions"
2. Regulatory Guide 1.29, September 1978, "Seismic Design Classification."
3. Regulatory Guide 1.53, June 1973, "Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems."
4. Regulatory Guide 1.75, September 1978, "Physical Independence of Electric Systems."
5. Regulatory Guide 1.89 June 1984, "Environmental Qualification of Certain Electrical Equipment Important to Safety for Nuclear Power Plants."
6. Regulatory Guide 1.97, December 1980 "Instrumentation for Light-Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident."
7. Regulatory Guide 1.100, June 1988 "Seismic Qualification of Electrical and Mechanical Equipment for Nuclear Power Plants."
8. Regulatory Guide 1.118, April 1995 "Periodic Testing of Electric Power and Protection Systems."
9. Regulatory Guide 1.153, June 1996 "Criteria For Safety Systems."
10. ANSI/IEEE-ANS-7-4.3.2-1993 "IEEE Standard Criteria for Digital Computer in Safety Systems of Nuclear Power Generating Stations."
11. Regulatory Guide 1.152, January 1996, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants."
12. Regulatory Guide 1.168, September 1997, "Verification, Validation, Reviews, and Audits for Digital Computer Software used in Safety Systems of Nuclear Power Plants."
13. IEEE Standard 1012-1986, "IEEE Standard for Software Verification and Validation."

14. IEEE Standard 1028-1988, "IEEE Standard for Software Reviews and Audits."
15. IEEE Standard 279-1971, "Protection Systems for Nuclear Power Generating Stations."
16. IEEE Standard 323-1983, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."
17. IEEE Standard 338-1987, "IEEE Standard Criteria for the Periodic Testing of Nuclear Power Generating Station Safety Systems."
18. IEEE Standard 344-1987, "IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations."
19. IEEE Standard 379-1994, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."
20. IEEE Standard 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits."
21. IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
22. EPRI Topical Report TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," Revision 1.
23. EPRI Topical Report TR-106439, "Guidelines on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," Electric Power Research Institute, October 1996.
24. EPRI Topical Report TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," Electric Power Research Institute, December 1996.

Document 3

**Application For Withholding Proprietary Information
From Public Disclosure CAW-10-2866**

dated December 2009 (Proprietary)



Westinghouse Electric Company
Nuclear Services
P.O. Box 355
Pittsburgh, Pennsylvania 15230-0355
USA

U.S. Nuclear Regulatory Commission
Document Control Desk
Washington, DC 20555-0001

Direct tel: (412) 374-4643
Direct fax: (412) 374-3846
e-mail: greshaja@westinghouse.com
Proj letter: WBT-D-2085

CAW-10-2866

June 23, 2010

APPLICATION FOR WITHHOLDING PROPRIETARY
INFORMATION FROM PUBLIC DISCLOSURE

Subject: WNA-LI-00058-WBT-P, Revision 0, "Tennessee Valley Authority (TVA) Watts Bar Unit 2 (WBN2) Post-Accident Monitoring System (PAMS) Licensing Technical Report," (Proprietary)

The proprietary information for which withholding is being requested in the above-referenced report is further identified in Affidavit CAW-10-2866 signed by the owner of the proprietary information, Westinghouse Electric Company LLC. The affidavit, which accompanies this letter, sets forth the basis on which the information may be withheld from public disclosure by the Commission and addresses with specificity the considerations listed in paragraph (b)(4) of 10 CFR Section 2.390 of the Commission's regulations.

Accordingly, this letter authorizes the utilization of the accompanying affidavit by Tennessee Valley Authority (TVA).

Correspondence with respect to the proprietary aspects of the application for withholding or the Westinghouse affidavit should reference this letter, CAW-10-2866 and should be addressed to J. A. Gresham, Manager, Regulatory Compliance and Plant Licensing, Westinghouse Electric Company LLC, P.O. Box 355, Pittsburgh, Pennsylvania 15230-0355.

Very truly yours,

A handwritten signature in black ink, appearing to read 'J. A. Gresham', written over a horizontal line.

J. A. Gresham, Manager
Regulatory Compliance and Plant Licensing

Enclosures

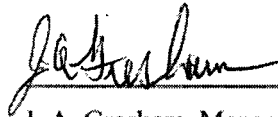
AFFIDAVIT

COMMONWEALTH OF PENNSYLVANIA:

SS

COUNTY OF ALLEGHENY:

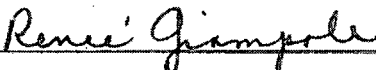
Before me, the undersigned authority, personally appeared J. A. Gresham, who, being by me duly sworn according to law, deposes and says that he is authorized to execute this Affidavit on behalf of Westinghouse Electric Company LLC (Westinghouse), and that the averments of fact set forth in this Affidavit are true and correct to the best of his knowledge, information, and belief:



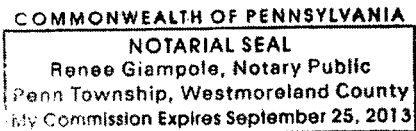
J. A. Gresham, Manager

Regulatory Compliance and Plant Licensing

Sworn to and subscribed before me
this 23rd day of June 2010



Notary Public



- (1) I am Manager, Regulatory Compliance and Plant Licensing, in Nuclear Services, Westinghouse Electric Company LLC (Westinghouse), and as such, I have been specifically delegated the function of reviewing the proprietary information sought to be withheld from public disclosure in connection with nuclear power plant licensing and rule making proceedings, and am authorized to apply for its withholding on behalf of Westinghouse.
- (2) I am making this Affidavit in conformance with the provisions of 10 CFR Section 2.390 of the Commission's regulations and in conjunction with the Westinghouse Application for Withholding Proprietary Information from Public Disclosure accompanying this Affidavit.
- (3) I have personal knowledge of the criteria and procedures utilized by Westinghouse in designating information as a trade secret, privileged or as confidential commercial or financial information.
- (4) Pursuant to the provisions of paragraph (b)(4) of Section 2.390 of the Commission's regulations, the following is furnished for consideration by the Commission in determining whether the information sought to be withheld from public disclosure should be withheld.
 - (i) The information sought to be withheld from public disclosure is owned and has been held in confidence by Westinghouse.
 - (ii) The information is of a type customarily held in confidence by Westinghouse and not customarily disclosed to the public. Westinghouse has a rational basis for determining the types of information customarily held in confidence by it and, in that connection, utilizes a system to determine when and whether to hold certain types of information in confidence. The application of that system and the substance of that system constitutes Westinghouse policy and provides the rational basis required.

Under that system, information is held in confidence if it falls in one or more of several types, the release of which might result in the loss of an existing or potential competitive advantage, as follows:

 - (a) The information reveals the distinguishing aspects of a process (or component, structure, tool, method, etc.) where prevention of its use by any of

Westinghouse's competitors without license from Westinghouse constitutes a competitive economic advantage over other companies.

- (b) It consists of supporting data, including test data, relative to a process (or component, structure, tool, method, etc.), the application of which data secures a competitive economic advantage, e.g., by optimization or improved marketability.
- (c) Its use by a competitor would reduce his expenditure of resources or improve his competitive position in the design, manufacture, shipment, installation, assurance of quality, or licensing a similar product.
- (d) It reveals cost or price information, production capacities, budget levels, or commercial strategies of Westinghouse, its customers or suppliers.
- (e) It reveals aspects of past, present, or future Westinghouse or customer funded development plans and programs of potential commercial value to Westinghouse.
- (f) It contains patentable ideas, for which patent protection may be desirable.

There are sound policy reasons behind the Westinghouse system which include the following:

- (a) The use of such information by Westinghouse gives Westinghouse a competitive advantage over its competitors. It is, therefore, withheld from disclosure to protect the Westinghouse competitive position.
- (b) It is information that is marketable in many ways. The extent to which such information is available to competitors diminishes the Westinghouse ability to sell products and services involving the use of the information.
- (c) Use by our competitor would put Westinghouse at a competitive disadvantage by reducing his expenditure of resources at our expense.

- (d) Each component of proprietary information pertinent to a particular competitive advantage is potentially as valuable as the total competitive advantage. If competitors acquire components of proprietary information, any one component may be the key to the entire puzzle, thereby depriving Westinghouse of a competitive advantage.
 - (e) Unrestricted disclosure would jeopardize the position of prominence of Westinghouse in the world market, and thereby give a market advantage to the competition of those countries.
 - (f) The Westinghouse capacity to invest corporate assets in research and development depends upon the success in obtaining and maintaining a competitive advantage.
- (iii) The information is being transmitted to the Commission in confidence and, under the provisions of 10 CFR Section 2.390, it is to be received in confidence by the Commission.
- (iv) The information sought to be protected is not available in public sources or available information has not been previously employed in the same original manner or method to the best of our knowledge and belief.
- (v) The proprietary information sought to be withheld in this submittal is that which is appropriately marked in WNA-LI-00058-WBT-P, Revision 0, "Tennessee Valley Authority (TVA) Watts Bar Unit 2 (WBN2) Post-Accident Monitoring System (PAMS) Licensing Technical Report," dated June 2010, for submittal to the Commission, being transmitted by Tennessee Valley Authority letter and Application for Withholding Proprietary Information from Public Disclosure, to the Document Control Desk. The proprietary information as submitted by Westinghouse is that associated with the NRC review of the Post-Accident Monitoring System (PAMS) being designed for Watts Bar Unit 2, and may be used only for that purpose.

This information is part of that which will enable Westinghouse to:

- (a) Assist the customer in providing requested technical licensing information to the NRC that is required for approval of the Common Q Post-Accident Monitoring System (PAMS).

Further this information has substantial commercial value as follows:

- (a) Westinghouse plans to sell the use of similar information to its customers for purpose of other plant-specific applications.
- (b) Its use by a competitor would improve his competitive position in the design and licensing of a similar product.
- (c) The information requested to be withheld reveals the distinguishing aspects of a design methodology which was developed by Westinghouse.

Public disclosure of this proprietary information is likely to cause substantial harm to the competitive position of Westinghouse because it would enhance the ability of competitors to provide similar instrumentation and control systems and licensing defense services for commercial power reactors without commensurate expenses. Also, public disclosure of the information would enable others to use the information to meet NRC requirements for licensing documentation without purchasing the right to use the information.

The development of the technology described in part by the information is the result of applying the results of many years of experience in an intensive Westinghouse effort and the expenditure of a considerable sum of money.

In order for competitors of Westinghouse to duplicate this information, similar technical programs would have to be performed and a significant manpower effort, having the requisite talent and experience, would have to be expended.

Further the deponent sayeth not.

PROPRIETARY INFORMATION NOTICE

Transmitted herewith are proprietary and/or non-proprietary versions of documents furnished to the NRC in connection with requests for generic and/or plant-specific review and approval.

In order to conform to the requirements of 10 CFR 2.390 of the Commission's regulations concerning the protection of proprietary information so submitted to the NRC, the information which is proprietary in the proprietary versions is contained within brackets, and where the proprietary information has been deleted in the non-proprietary versions, only the brackets remain (the information that was contained within the brackets in the proprietary versions having been deleted). The justification for claiming the information so designated as proprietary is indicated in both versions by means of lower case letters (a) through (f) located as a superscript immediately following the brackets enclosing each item of information being identified as proprietary or in the margin opposite such information. These lower case letters refer to the types of information Westinghouse customarily holds in confidence identified in Sections (4)(ii)(a) through (4)(ii)(f) of the affidavit accompanying this transmittal pursuant to 10 CFR 2.390(b)(1).

COPYRIGHT NOTICE

The reports transmitted herewith each bear a Westinghouse copyright notice. The NRC is permitted to make the number of copies of the information contained in these reports which are necessary for its internal use in connection with generic and plant-specific reviews and approvals as well as the issuance, denial, amendment, transfer, renewal, modification, suspension, revocation, or violation of a license, permit, order, or regulation subject to the requirements of 10 CFR 2.390 regarding restrictions on public disclosure to the extent such information has been identified as proprietary by Westinghouse, copyright protection notwithstanding. With respect to the non-proprietary versions of these reports, the NRC is permitted to make the number of copies beyond those necessary for its internal use which are necessary in order to have one copy available for public viewing in the appropriate docket files in the public document room in Washington, DC and in local public document rooms as may be required by NRC regulations if the number of copies submitted is insufficient for this purpose. Copies made by the NRC must include the copyright notice in all instances and the proprietary notice if the original was identified as proprietary.