

Attachment 7

**Westinghouse Electric Company WCAP-17427-NP, Revision 1,
"Watts Bar Nuclear Plant Unit 2 Common Q Post Accident Monitoring System
Computer Security Assessment," (Non-Proprietary)**

**Watts Bar Nuclear Plant Unit 2 Common Q Post Accident
 Monitoring System Computer Security Assessment (Non-Proprietary)**

Westinghouse Non-Proprietary Class 3

WCAP-17427-NP
 Revision 1

August 2011

Watts Bar Nuclear Plant Unit 2 Common Q Post Accident Monitoring System Computer Security Assessment

BECHTEL POWER CORPORATION							Job Number: 25402					
SUPPLIER DOCUMENT REVIEW STATUS												
STATUS CODE:												
1	<input type="checkbox"/>	Work may proceed.					3	<input type="checkbox"/>	Rejected. Revise and resubmit.			
1C	<input type="checkbox"/>	Work may proceed. Editorial comments need only be incorporated if revised for other purposes.					4	<input checked="" type="checkbox"/>	Review not required. Work may proceed.			
2	<input type="checkbox"/>	Revise and resubmit. Work may proceed subject to incorporation of changes indicated.					Contract Number # 65717 WBT-D- <u>3438</u>					
Permission to proceed does not constitute acceptance or approval of design details, calculations, analysis, test methods, or materials developed or selected by the Supplier and does not relieve the Supplier from full compliance with contractual obligations.												
Reviewed by	Arch	Civil	CS	Elect	Mech	MET	PD	Constr	Startup	STE		
	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	
Status By:	M.S. Clark <i>M. S. Clark</i>						DATE	9/1/11				



WCAP-17427-NP

Revision 1

Watts Bar Nuclear Plant Unit 2 Common Q Post Accident Monitoring System Computer Security Assessment

Warren R. Odess-Gillett*
Nuclear Automation Licensing

August 2011

Verifier: Shawn M. Downey*
Nuclear Automation Safety System Support & Upgrades

Reviewer: Stephanie L. Smith*
Nuclear Automation Licensing

Approved: Mark J. Stofko*, Manager
Nuclear Automation Licensing

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

Westinghouse Electric Company LLC
1000 Westinghouse Drive
Cranberry Township, PA 16066, USA

© 2011 Westinghouse Electric Company LLC
All Rights Reserved

LIST OF CONTRIBUTORS

Revision	Name and Title
0	Ipek Tetikoglu Principal Engineer
1	Jonathan D. Vanase Senior Engineer, Safety Systems Platforms Engineering
1	Jenna L. Tyger Technical Editor, Technical Communications

REVISION HISTORY**RECORD OF CHANGES**

Revision	Author	Description	Completed
0	Warren R. Odess-Gillett	Original Issue	05/2011
1	Warren R. Odess-Gillett	Added section for Secure Development Environment	See EDMS

DOCUMENT TRACEABILITY & COMPLIANCE

Created to Support the Following Document(s)	Document Number	Revision
N/A		

OPEN ITEMS

Item	Description	Status
None.		

TABLE OF CONTENTS

LIST OF CONTRIBUTORS.....		ii
REVISION HISTORY		iii
LIST OF ACRONYMS AND ABBREVIATIONS.....		v
GLOSSARY OF TERMS		vi
1 INTRODUCTION		1-1
1.1 OVERVIEW		1-1
1.2 POST ACCIDENT MONITORING SYSTEM		1-1
2 DESIGN PHASES.....		2-1
2.1 PAMS SECURITY CAPABILITIES		2-1
2.1.1 PAMS Security Requirements		2-1
2.1.2 PAMS Cyber Security Assessment.....		2-1
2.2 CONCEPTS PHASE		2-1
2.2.1 PAMS Independence Features		2-1
2.2.2 Compliance with Clause 5.9 of IEEE Std. 603.....		2-1
2.2.3 Identification of Lifecycle Vulnerabilities.....		2-3
2.2.4 Remote Access.....		2-6
2.3 REQUIREMENTS PHASE.....		2-6
2.3.1 System Features – Security Functional Performance Requirements.....		2-6
2.3.2 Development System Requirements.....		2-8
2.3.3 Requirements Phase Outputs		2-8
2.4 DESIGN PHASE		2-8
2.4.1 System Features.....		2-8
2.4.2 Development Activities for the Design Phase		2-8
2.4.3 Design Phase Outputs.....		2-9
2.5 IMPLEMENTATION PHASE.....		2-9
2.5.1 Systems Features		2-9
2.5.2 Development Activities for the Implementation Phase		2-9
2.5.3 Implementation Phase Outputs.....		2-10
2.6 TESTING PHASE		2-10
2.6.1 System Features.....		2-10
2.6.2 Development Activities for the Testing Phase		2-10
2.6.3 Testing Phase Outputs		2-11
3 SECURE DEVELOPMENT ENVIRONMENT.....		3-1
3.1 AC160 SOFTWARE DEVELOPMENT		3-1
3.1.1 Reusable Software Elements		3-1
3.2 FLAT PANEL DISPLAY SOFTWARE DEVELOPMENT		3-4
3.2.1 QNX Operating System.....		3-4
3.2.2 QNX Development Environment		3-5
3.2.3 FPD Application		3-5
4 REFERENCES		4-1

LIST OF ACRONYMS AND ABBREVIATIONS

Acronyms used in the document are defined below to ensure unambiguous understanding of their use within this document.

Acronym	Definition
CIT	Channel Integration Test
CRC	Cyclic Redundancy Check
EDMS	Enterprise Document Management System
FCB	Function Chart Builder
FPD	Flat Panel Display
FPDS	Flat Panel Display System
IV&V	Independent Verification & Validation
MCR	Main Control Room
MTP	Maintenance and Test Panel
PAMS	Post Accident Monitoring System
RSED	Reusable Software Element Document
SDE	Secure Development Environment
SPM	Software Program Manual
SQAP	Software Quality Assurance Plan
WBN2	Watts Bar Nuclear Plant Unit 2

Advant, Photon, and QNX are trademarks or registered trademarks of their respective owner(s). Other names may be trademarks of their respective owners.

All other product and corporate names used in this document may be trademarks or registered trademarks of other companies, and are used only for explanation and to the owners' benefit, without intent to infringe.

GLOSSARY OF TERMS

Access Control

The physical or electronic mechanisms for permitting or limiting entry to a computer network. Access control restricts user access by requiring user identity or membership authentication of the predefined group. System administrators typically use access control to control access to servers, directories, or other network resources.

Authentication

Verifying the identity of a user who is logging onto a computer system or verifying the origin of a transmitted message. Authentication depends on four classes of data, generally summarized as “what you know,” “what you have,” “what you are,” and “what you do.” Passwords and digital signatures are forms of authentication.

Communication Flow Control

Used to restrict the flow of information and services between digital devices or systems. A communication flow control protects one system or network from another by blocking unauthorized traffic. The quality of communication flow control strongly depends on the configuration, implementation, operation, and maintenance of communication flow control equipment (for example, firewalls) by qualified personnel. It also heavily depends on the use of quality authentication measures and restrictions on ports.

Confidentiality

The ability of (or assurance that) information will remain secret or be otherwise prevented from unauthorized disclosure.

Configuration

The way a system is set up, or the assortment of components that make up the system. Configuration can refer to hardware or software or the combination of both.

Critical Digital Asset (CDA)

A subcomponent of a critical system that consists of or contains a digital device, and a computer or communication system or network.

Critical System (CS)

An analog or digital technology based system that performs or is associated with any of the following functions: safety-related, important-to-safety, security, emergency preparedness, or continuity of power.

GLOSSARY OF TERMS (cont.)

Development System

[]^{a,c,e}

Remote Access

The ability to access a safety system that is physically located in a less secure area.

RSED

Individual Type Circuit or Custom PC Element document that defines the requirements and describes the design and implementation of the Type Circuit or Custom PC Element.

Risk

“A combination of the probability of an adverse event and the nature and severity of the event” (Presidential/Congressional Commission on Risk Assessment and Risk Management 1997). In the security assessment method, risk is defined as the combination of the susceptibility of a CDA to cyber exploitation and consequences to the plant from that exploitation.

Safety System

The aggregate of electrical and mechanical equipment necessary to mitigate the consequences of design bases events.

Susceptibility

A relative measure of the likelihood that a CDA could be exploited. It is based on the number of identified vulnerabilities, the severity of the vulnerabilities, and the effectiveness of existing protection measures to reduce or eliminate these vulnerabilities. Susceptibility is used in the security assessment method’s determination of risk.

Test Bed System

[]^{a,c,e}

Target System

[

] ^{a,c,e}

Vulnerability

A weakness in the CDA's physical or electronic configuration that could allow an action that compromises the asset.

1 INTRODUCTION

1.1 OVERVIEW

This report reviews the digital safety system lifecycle phases of the Watts Bar Nuclear Plant Unit 2 (WBN2) Post Accident Monitoring System (PAMS) and summarizes the quality standards and design control measures implemented that provide computer security and ensure that the PAMS is designed for high functional reliability commensurate with the safety functions to be performed throughout the development phases of digital safety system lifecycle (see Reference 1, regulatory positions 2.1 through 2.5). The development phases reviewed include the concepts, requirements, design, implementation and testing phases. This report is structured such that each major section of the report addresses the system features and development activities for one lifecycle phase. Section 3 provides a description of the secure development environment (SDE) for the WBN2 Common Q PAMS.

1.2 POST ACCIDENT MONITORING SYSTEM

The WBN2 Common Q PAMS, replaces the existing inadequate core cooling monitor system (ICCM-86) that is in WBN1. PAMS calculates subcooled margin and reactor vessel level, process core exit temperatures, and provide key data to the control room via the Flat Panel Display System (FPDS).

The purpose of the WBN2 PAMS is to provide safety-related 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 2) 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 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.

2 DESIGN PHASES

2.1 PAMS SECURITY CAPABILITIES

2.1.1 PAMS Security Requirements

The security requirements for the WBN2 PAMS can be found in References 3 – 5.

2.1.2 PAMS Cyber Security Assessment

As part of Watts Bar Unit 2 Nuclear Security Program as mandated by 10 CFR 73.54, TVA will perform an assessment of the PAMS.

2.2 CONCEPTS PHASE

2.2.1 PAMS Independence Features

[

]a.c.e

2.2.2 Compliance with Clause 5.9 of IEEE Std. 603

[

]a.c.e

[

|

]a,c,e

[

]a,c,e

2.2.3 Identification of Lifecycle Vulnerabilities

2.2.3.1 Lifecycle Vulnerabilities for Conceptual, Requirements, and Design Phases

[

|

]a,c,e

[

]a,c,e

[

|

]a.c.e

2.2.3.2 Lifecycle Vulnerabilities for the Implementation Phase and the Testing Phase

[

]a,c,e

2.2.4 Remote Access

[

]a,c,e

2.3 REQUIREMENTS PHASE

2.3.1 System Features – Security Functional Performance Requirements

[

]a,c,e

2.3.1.1 Requirements for PAMS Independence Features

Refer to subsection 2.2.1.

2.3.1.2 Requirements to Enforce Access Control Security Attributes

Refer to subsection 2.2.2.

2.3.1.3 Human Factors

[

] ^{a,c,e}

2.3.1.4 Requirements Associated with Lifecycle Vulnerabilities

Refer to subsection 2.2.3.1.

2.3.1.5 PAMS Requirements Independent Verification & Validation (IV&V)

[

] ^{a,c,e}

2.3.1.6 Use of Pre-Developed Software and Systems

See discussion in item 2 on page 2-4 for pre-developed software.

2.3.2 Development System Requirements

See development processes discussed in subsection 2.2.3.

2.3.3 Requirements Phase Outputs

[

] ^{a,c,e}

2.4 DESIGN PHASE

[

|

] ^{a,c,e}

2.4.1 System Features

2.4.1.1 Security Functional Performance Designed to Meet Requirements

[

] ^{a,c,e}

2.4.1.1.1 PAMS System Design

The design of PAMS system shall meet the requirements of subsection 2.3.1.

2.4.2 Development Activities for the Design Phase

2.4.2.1 Documentation shall be controlled per subsection 2.2.3.1.

2.4.2.2 Design documentation shall be developed per subsection 2.2.3.1.

2.4.3 Design Phase Outputs

2.4.3.1 Design documentation complete.

2.4.3.2 IV&V Phase Summary Report.

2.5 IMPLEMENTATION PHASE

[

] ^{a,c,e}

2.5.1 Systems Features

2.5.1.1 Security Functional Performance Designed to meet Requirements

[

] ^{a,c,e}

2.5.1.1.1 PAMS System Implementation

The PAMS system shall be built to meet the security design captured in subsection 2.3.

2.5.1.1.2 PAMS Specific Application Software

The PAMS specific application software shall be implemented to meet the design captured in subsection 2.4.

2.5.2 Development Activities for the Implementation Phase

2.5.2.1 Documentation shall be controlled per subsection 2.2.3.1.

2.5.2.2 Software design documentation shall be developed per subsection 2.2.3.1.

[

] ^{a,c,e}

[

] ^{a,c,e}

2.5.2.3 Software implementation activities shall be performed as described in Section 3.

2.5.3 Implementation Phase Outputs

2.5.3.1 IV&V Phase Summary Report documenting module and unit tests, and code reviews.

2.5.3.2 Software Release Records for type circuits and custom PC elements.

2.5.3.3 Code is in a “locked” area of the configuration control system only available to IV&V for modification. This is the code approved by IV&V for the test phase.

2.6 TESTING PHASE

In this phase, completed cabinets containing the applications software are connected together as an integrated system. Validation testing (described in the PAMS test plan) is performed to test the system.

2.6.1 System Features

2.6.1.1 Security Functional Performance is tested against the Requirements

[

] ^{a,c,e}

2.6.2 Development Activities for the Testing Phase

[

] ^{a,c,e}

2.6.3 Testing Phase Outputs

2.6.3.1 Software Release Records with an IV&V approval stamp.

2.6.3.2 IV&V Phase Summary Report

2.6.3.3 Test Report(s)

3 SECURE DEVELOPMENT ENVIRONMENT

3.1 AC160 SOFTWARE DEVELOPMENT

3.1.1 Reusable Software Elements

The lowest AC160 software development is the reusable software element. A reusable software element is either a type circuit or a custom PC element.

3.1.1.1 Type Circuit

A type circuit is a group of PC elements that are then encapsulated into an entity that can be referenced in the Function Chart Tool. A type circuit is developed similarly to an AC160 application using the Function Chart Builder (FCB). [

] ^{a,c,e}

Once a developer has completed the RSED, coding for the type circuit, and performed preliminary tests on the type circuit, the software engineer checks the type circuit components into the software configuration control system. [

] ^{a,c,e}

The software engineer issues a software release record for that type circuit documenting [

] ^{a,c,e} the software configuration control system.

IV&V then performs a code review on the released type circuit comparing the implementation to the requirements in the RSED. IV&V uses the same set of AC160 tools used by the design team when conducting code reviews of the AC160 type circuit code. This tool set resides on a desktop (or laptop) PC with ABB Application Builder. The purpose of the type circuit code review is to verify that the function chart, created by the ABB FCB, contains logic as described by the RSED. Also, the logic functionality must be traced to the requirements defined in the RSED. Any non-traceable logic would be considered extraneous and/or undocumented code and would need to be removed. This would be reported as an IV&V anomaly.

IV&V also performs a module test on the released type circuit on a test bed and produces a test report. After the reviews and testing are completed satisfactorily, IV&V updates the software release record [

] ^{a,c,e}. IV&V then releases the code [

] ^{a,c,e}

To use the type circuit, the application developer will create a standard application directory structure using the FCB. Then the application engineer will copy the type circuit files from the production area of the software configuration management system into the type circuit folder in the application directory structure within the ABB Application Builder. The engineer then builds the Function Chart application

using PC elements and these type circuits to create an application. See the description regarding Function Chart application programming (subection 3.1.1.3) for how the application program is checked into the software configuration management system along with the type circuit files, and how IV&V ensures that the same type circuit files that are in the application Function Chart are the same as identified in the release record for the type circuit.

3.1.1.2 Custom PC Element

A custom PC element is a custom function block that is developed in the C programming language and can be used similarly to any other standard PC element that comes with the tool. [

instructions govern how the custom PC element is created. Once a developer has completed the RSED, coding for the custom PC element, []^{a,c,e} Internal work
 engineer checks the custom PC element components into []^{a,c,e} the software
 configuration management system. []^{a,c,e} the software

]^{a,c,e}

IV&V then performs a code review on the released []^{a,c,e} custom PC elements []^{a,c,e} comparing the implementation to the requirements in the RSED for each element. IV&V independently compiles and links the source code and independently generates a library for test. [

]^{a,c,e} IV&V then releases the code [

]^{a,c,e}

[

]^{a,c,e}

See the description regarding Function Chart application programming (subection 3.1.1.3) for how the application program is checked into the software configuration management system with a release record documenting the custom PC element library that is used with the application.

3.1.1.3 Application Programming

The Function Chart application programming, like the Type Circuit programming, is done using the Function Chart tool. The requirements for the Function Chart application comes from the Functional Specifications and Functional Logic Diagrams produced by the Functional Design Team, the System Design Specification, the Software Requirements Specification, and finally by the Preliminary Software Design Description. The documents go through an independent review.

As described earlier, to use the type circuits []^{a,c,e} will copy the type circuit files []^{a,c,e} into the type circuit folder in the ABB Application Builder standard application directory structure using the FCB. The engineer then builds the Function Chart application using PC elements and these type circuits to create an application.

[

] ^{a,c,e} After checking the node structure into the software configuration management system and prior to producing the software release record for the Function Chart application, the developer will check out the Function Chart application and load it into the test bed controller using internal work instructions.

[

] ^{a,c,e}

After loading the test bed controller with the required custom PC element libraries and the compiled Function Chart application program, the engineer then captures the calculated CRC for the Function Chart application and the CRC for the system software, which comprises the controller operating system, any standard controller libraries that are loaded, []^{a,c,e}.

[

] ^{a,c,e}

Once the Function Chart application is released, IV&V will check out the node structure from the software configuration management system. They will perform a code review on the Function Chart

application. Part of this review is to verify that the type circuits in the Function Chart application node structure are the same type circuits released for use in Function Chart applications. IV&V will load the Function Chart application into a test bed. [

] ^{a,c,e} Once the library images and Function Chart application are loaded into the test bed controller, IV&V validates the CRC for the Function Chart application and the CRC for the system software against what is published in the Function Chart application software release record. Additionally, the Function Chart application continuously validates the CRC values and reports any changes to the CRC for alarm. IV&V then performs the Processor Module Software Test on this configuration. IV&V issues the test report and releases the application [

] ^{a,c,e} of the software configuration management system [

] ^{a,c,e}

When it is time to load the target system with the Function Chart application software, the same process is followed. [

] ^{a,c,e}

The test team or development team will load the Function Chart application onto the target controller. Part of the test for the target system is to record the calculated CRCs for the Function Chart application and system, [

] ^{a,c,e}. The test procedure will include a validation step that the displayed calculated CRCs are consistent [

] ^{a,c,e}

3.2 FLAT PANEL DISPLAY SOFTWARE DEVELOPMENT

The Flat Panel Display (FPD) is the graphical user interface portion of the safety system.

3.2.1 QNX Operating System

[

] ^{a,c,e} The PC node box is tested according to a procedure as part of receipt inspection (called a Commercial Dedication Instruction). [

]a,c,e

3.2.2 QNX Development Environment

[

]a,c,e

3.2.3 FPD Application

[

]a,c,e

[

]a,c,e

Once released, the []a,c,e FPD application software goes through a test program and IV&V. An IV&V report on the []a,c,e FPD software is produced indicating that it is acceptable for use on projects.

[

] ^{a,c,e}

The [^{a,c,e} FPD application program consists of the displays and other processes [^{a,c,e}. Once the developer is ready to release the [^{a,c,e} FPD software, the developer checks the software into the software configuration management system. Once checked in, the developer will load the FPD controlled application software on a test bed PC node box. [

] ^{a,c,e}

IV&V will check FPD application [^{a,c,e} out of the software configuration management system. They will perform a code review on the FPD application [

] ^{a,c,e}

A Channel Integration Test (CIT) is conducted on the target safety system. The FPD application is checked out of the software configuration management system [

is loaded onto the PC node box [^{a,c,e} following internal work instructions. ^{a,c,e} The FPD application

[

] ^{a,c,e}

4 REFERENCES

1. Regulatory Guide 1.152, Rev. 3, "Criteria For Use Of Computers In Safety Systems Of Nuclear Power Plants," U.S. Nuclear Regulatory Commission, July 2011.
2. WCAP-16097-P-A, Rev. 0, "Common Qualified Platform Topical Report," Westinghouse Electric Company LLC.
3. WNA-DS-01617-WBT-P, Rev. 4, "Post Accident Monitoring System- System Requirements Specification," Westinghouse Electric Company LLC.
4. WNA-DS-01667-WBT-P, Rev. 4, "Post Accident Monitoring System- System Design Specification," Westinghouse Electric Company LLC.
5. WNA-SD-00239-WBT-P, Rev. 4, "Software Requirements Specification for the Post Accident Monitoring System," Westinghouse Electric Company LLC.
6. WNA-LI-00058-WBT-P, Rev. 3, "Post-Accident Monitoring System (PAMS) Licensing Technical Report," Westinghouse Electric Company LLC.
7. WCAP-16096-NP-A, Rev. 1A, "Software Program Manual for Common Q Systems," Westinghouse Electric Company LLC.
8. WNA-DS-01070-GEN, Rev. 6, "Application Restrictions for Generic Common Q Qualification," Westinghouse Electric Company LLC.
9. WCAP-7211, Rev. 5, "Proprietary Information and Intellectual Property Management Policies and Procedures," Westinghouse Electric Company LLC.
10. MOD 00-0577, Rev. 1, "Oskarshamn 1 – Project O1 Mod Qualification of Category A I&C Report on Software Static Analysis Advant Controller 160 for RPS."
11. MOD 97-7770, Rev. 3, "Oskarshamn 1 – Project O1 Mod Qualification of Category A I&C Tools Evaluation Report."
12. BA AUT-99-ADVANT-00, "Agreement for the Supply of Advant Hardware and Software Components," dated February 2, 1999."
13. WNA-CD-00018-GEN, Rev. 3, "Commercial Dedication Report For QNX 4.25G for Common Q Applications," Westinghouse Electric Company LLC.

Attachment 8

**Westinghouse Electric Company CAW-11-3241,
Application for Withholding Proprietary Information from Public Disclosure,
WCAP-17427-P, Revision 1, "Watts Bar Nuclear Plant Unit 2 Common Q Post Accident
Monitoring System Computer Security Assessment," (Proprietary)**



Westinghouse Electric Company
 Nuclear Services
 1000 Westinghouse Drive
 Cranberry Township, Pennsylvania 16066
 USA

U.S. Nuclear Regulatory Commission
 Document Control Desk
 11555 Rockville Pike
 Rockville, MD 20852

Direct tel: (412) 374-4643
 Direct fax: (724) 720-0754
 e-mail: greshaja@westinghouse.com
 Proj letter: WBT-D-3438

CAW-11-3241
 August 30, 2011

APPLICATION FOR WITHHOLDING PROPRIETARY
 INFORMATION FROM PUBLIC DISCLOSURE

Subject: WCAP-17427-P, Revision 1, "Watts Bar Nuclear Plant Unit 2 Common Q Post Accident
 Monitoring System Computer Security Assessment" (Proprietary)

The proprietary information for which withholding is being requested in the above-referenced report is further identified in Affidavit CAW-11-3241 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.

Correspondence with respect to the proprietary aspects of the application for withholding or the Westinghouse affidavit should reference this letter, CAW-11-3241, and should be addressed to J. A. Gresham, Manager, Regulatory Compliance, Westinghouse Electric Company LLC, Suite 428, 1000 Westinghouse Drive, Cranberry Township, Pennsylvania 16066.

Very truly yours,


 J. A. Gresham, Manager
 Regulatory Compliance

Enclosures

BECHTEL POWER CORPORATION							Job Number: 25402				
SUPPLIER DOCUMENT REVIEW STATUS											
STATUS CODE:											
1	<input type="checkbox"/>	Work may proceed.					3	<input type="checkbox"/>	Rejected. Revise and resubmit.		
1C	<input type="checkbox"/>	Work may proceed. Editorial comments need only be incorporated if revised for other purposes.					4	<input checked="" type="checkbox"/>	Review not required. Work may proceed.		
2	<input type="checkbox"/>	Revise and resubmit. Work may proceed subject to incorporation of changes indicated.					Contract Number # 65717 WBT-D-3438				
Permission to proceed does not constitute acceptance or approval of design details, calculations, analysis, test methods, or materials developed or selected by the Supplier and does not relieve the Supplier from full compliance with contractual obligations.											
Reviewed by	Arch	Civil	CS	Elect	Mech	MET	PD	Constr	Startup	STE	
	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	
Status By:	M.S. Clark						DATE	9/1/11			

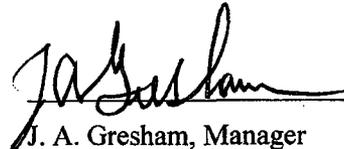
AFFIDAVIT

COMMONWEALTH OF PENNSYLVANIA:

SS

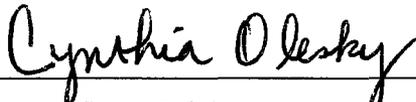
COUNTY OF BUTLER:

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:

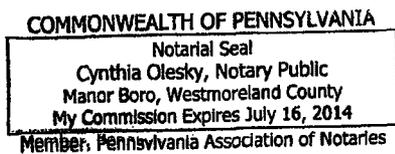


J. A. Gresham, Manager
Regulatory Compliance

Sworn to and subscribed before me
this 30th day of August 2011



Notary Public



- (1) I am Manager, Regulatory Compliance, 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 WCAP-17427-P, Revision 1, "Watts Bar Nuclear Plant Unit 2 Common Q Post Accident Monitoring System Computer Security Assessment" (Proprietary), dated August 2011, 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 Post Accident Monitoring System and may be used only for that purpose.

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

- (a) Continue to provide technical support for verification and validation services for the Post Accident Monitoring System.
- (b) Remain competitive in the marketplace for support services.

Further this information has substantial commercial value as follows:

- (a) Westinghouse plans to sell the use of similar information to its customers for the purpose of design verification and validation.
- (b) Westinghouse can sell support and defense of licensing activities.
- (c) The information requested to be withheld reveals the distinguishing aspects of a 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 calculations, analysis 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.

Tennessee Valley Authority

Letter for Transmittal to the NRC

The following paragraphs should be included in your letter to the NRC:

Enclosed are:

1. ___ copies of WCAP-17427-P, Revision 1, "Watts Bar Nuclear Plant Unit 2 Common Q Post Accident Monitoring System Computer Security Assessment" (Proprietary)
2. ___ copies of WCAP-17427-NP, Revision 1, "Watts Bar Nuclear Plant Unit 2 Common Q Post Accident Monitoring System Computer Security Assessment" (Non-Proprietary)

Also enclosed is the Westinghouse Application for Withholding Proprietary Information from Public Disclosure CAW-11-3241, accompanying Affidavit, Proprietary Information Notice, and Copyright Notice.

As Item 1 contains information proprietary to Westinghouse Electric Company LLC, it is supported by an affidavit signed by Westinghouse, the owner of the information. The affidavit 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 Section 2.390 of the Commission's regulations.

Accordingly, it is respectfully requested that the information which is proprietary to Westinghouse be withheld from public disclosure in accordance with 10 CFR Section 2.390 of the Commission's regulations.

Correspondence with respect to the copyright or proprietary aspects of the items listed above or the supporting Westinghouse affidavit should reference CAW-11-3241 and should be addressed to J. A. Gresham, Manager, Regulatory Compliance, Westinghouse Electric Company LLC, Suite 428, 1000 Westinghouse Drive, Cranberry Township, Pennsylvania 16066.

Attachment 9

**TVA Document Titled "Common Q PAMS Secure Operational Environment
Per Regulatory Guide 1.152, Revision 3"**

Watts Bar Nuclear Unit 2
Common Q Post Accident Monitoring System
Conformance to the Secure Development and Operational Environment Requirements of
Regulatory Guide 1.152 Revision 3
Page 1 of 12
September 1, 2011

Acronyms and Abbreviations

The following acronyms/abbreviations are used in this document

CCM	Contract Compliance Matrix
CIT	Channel Integration Test
CFR	Code of Federal Regulation
COTS	Commercial off-the-shelf
FAT	Factory Acceptance Test
FE	Function Enable
ICCM-86	Inadequate Core Cooling Monitor
ICS	Integrated Computer System
MCR	Main Control Room
MTP	Maintenance and Test Panel
NRC	Nuclear Regulatory Commission
OM	Operators Module
PAMS	Post Accident Monitoring System
PC	Personal Computer
RTM	Requirements Traceability Matrix
RSED	Reusable Software Element Document
SAT	Site Acceptance Test
SDS	System Design Specification
SDOE	Secure Design and Operational Environment
SLE	Software Load Enable
SM	Shift Manager
SPM	Software Program Manual
SRO	Senior Reactor Operator
SRS	Software Requirements Specification
STA	Shift Technical Advisor
SysRS	System Requirements Specification
TCP/IP	Transmission Control Protocol/Internet Protocol
TVA	Tennessee Valley Authority
US	Unit Supervisor
WBN	Watts Bar Nuclear
WCC	Work Control Center

1. Secure Development Environment

Per Regulatory Guide 1.152 Revision 3, a Secure Development Environment is defined as the condition of having appropriate physical, logical and programmatic controls during the system development phases (i.e., concepts, requirements, design, implementation, testing) to ensure that unwanted, unneeded and undocumented functionality (e.g., superfluous code) is not introduced into digital safety systems.

a. Concept Phase:

Regulatory Position:

In the concepts phase, the licensee should identify digital safety system design features required to establish a secure operational environment for the system. A licensee should describe these design features as part of its application.

The licensee should assess the digital safety system's potential susceptibility to inadvertent access and undesirable behavior from connected systems over the course of the system's life cycle that could degrade its reliable operation. This assessment should identify the potential challenges to maintaining a secure operational environment for the digital safety system and a secure development environment for development life cycle phases. The results of the analysis should be used to establish design feature requirements (for both hardware and software) to establish a secure operational environment and protective measures to maintain it.

The licensee should not allow remote access to the safety system. For the purposes of this guidance, remote access is defined as the ability to access a computer, node, or network resource that performs a safety function or that can affect the safety function from a computer or node that is located in an area with less physical security than the safety system (e.g., outside the protected area).

Other NRC staff positions and guidance govern unidirectional and bidirectional data communications between safety and non-safety digital systems.

WBN Unit 2 Post Accident Monitoring System (PAMS) Concept

The concept for the Watts Bar Nuclear (WBN) Unit 2 design was to duplicate the WBN Unit 1 design. However, the WBN Unit 1 Inadequate Core Cooling Monitor (ICCM-86) PAMS was no longer available. In order to minimize operator impact, the concept for the WBN Unit 2 PAMS was to duplicate as closely as possible the functionality, features and look of the WBN Unit 1 ICCM-86 system. This included:

- Locating the equipment inside the control building with restricted access.
- Use of the same type of RVLIS system as used in WBN Unit 1
- No remote access to the system
- Screen Look and Navigation

Watts Bar Nuclear Unit 2
Common Q Post Accident Monitoring System
Conformance to the Secure Development and Operational Environment Requirements of
Regulatory Guide 1.152 Revision 3
Page 3 of 12
September 1, 2011

The basic requirements were then translated into a detailed set of contract requirements which were supplied to the equipment vendor for use in design of the system.

b. Requirements Phase:

Regulatory Position

System Features

The licensee should define the functional performance requirements and system configuration for a secure operational environment; interfaces external to the system; and requirements for qualification, human factors engineering, data definitions, documentation for the software and hardware, installation and acceptance, operation and execution, and maintenance.

The design feature requirements intended to maintain a secure operating environment and ensure reliable system operation should be part of the overall system requirements. Therefore, the verification process of the requirements phase should ensure the correctness, completeness, accuracy, testability, and consistency of the system's SDOE feature.

Requirements specifying the use of pre-developed software and systems (e.g., reused software and commercial off-the-shelf (COTS) systems) should address the reliability of the safety system (e.g., by using pre-developed software functions that have been tested and are supported by operating experience).

Development Activities

During the requirements phase, the licensee should prevent the introduction of unnecessary or extraneous requirements that may result in inclusion of unwanted or unnecessary code.

WBN Unit 2 Post Accident Monitoring System (PAMS) Requirements Phase

The concept for the PAMS was translated into a set of technical and business contract requirements. A preliminary contract compliance matrix (CCM) was developed by the design engineer to ensure the vendor met the contract requirements. This document was later expanded and incorporated as Section 12 of the Licensing Technical Report WNA-LI-00058-WBT. As the system design progressed changes were made to the matrix and to the requirements/design documents to reflect changes necessary to ensure a secure operational environment i.e. not installing the Operators Module (OM) Function Enable (FE) keyswitch and eliminating the permanent OM connection to a printer.

Watts Bar Nuclear Unit 2
Common Q Post Accident Monitoring System
Conformance to the Secure Development and Operational Environment Requirements of
Regulatory Guide 1.152 Revision 3
Page 4 of 12
September 1, 2011

The Common Qualified Platform (Common Q) system used for the WBN Unit 2 PAMS is based on COTS hardware and software that has been dedicated for use in safety-related applications. Application specific software is based on Westinghouse Reusable Software Element Documents (RSEDs). RSEDs are developed, tested, verified and validated in accordance with the Westinghouse WCAP-16096-NP-A, "Software Program Manual for Common Q Systems," (SPM) which was previously approved by the Nuclear Regulatory Commission (NRC).

The requirements for the WBN Unit 2 PAMS were translated from the CCM into WNA-DS-01617-WBT-P, "Post Accident Monitoring System-System Requirements Specification" (SysRS). WBN Unit 2 engineering review and approval of the SysRS against the requirements of the CCM is the measure taken to prevent the introduction of unnecessary design features or functions that may result in the inclusion of unwanted or unnecessary code.

c. Design Phase:

Regulatory Position

System Features

The safety system design features for a secure operational environment identified in the system requirements specification should be translated into specific design configuration items in the system design description.

Licensees should be aware that digital safety systems will be considered Critical Digital Assets and must adhere to the requirements of 10 CFR 73.54. Regulatory Guide 5.71 describes an acceptable defensive architecture to comply with 10 CFR 73.54. The architecture described in the guidance would have licensees place all digital safety systems in the highest level of their defensive architecture and only permit one-way communication (if any communication is desired) from the digital safety system to other systems in lower levels of the defensive architecture. Licensees should be aware that Section B.1.4 of Appendix B to Regulatory Guide 5.71 notes that one-way communications should be enforced using hardware mechanisms. A licensee's adherence to the provisions of 10 CFR 73.54 will be evaluated per regulatory programs specific to that regulation.

The safety system design configuration items for a secure operational environment intended to ensure reliable system operation should address control over (1) physical and logical access to the system functions, (2) use of safety system services, and (3) data communication with other systems. Design configuration items that incorporate pre-developed software into the safety system should address how this software will not challenge the secure operational environment for the safety system.

Watts Bar Nuclear Unit 2
Common Q Post Accident Monitoring System
Conformance to the Secure Development and Operational Environment Requirements of
Regulatory Guide 1.152 Revision 3
Page 5 of 12
September 1, 2011

Physical and logical access control features should be based on the results of the assessment performed in the concepts phase of the life cycle. The results of this assessment may identify the need for more complex access control measures, such as a combination of knowledge (e.g., password), property (e.g., key and smart card), or personal features (e.g., fingerprints), rather than just a password.

Development Activities

During the design phase, measures should be taken to prevent the introduction of unnecessary design features or functions that may result in the inclusion of unwanted or unnecessary code.

WBN Unit 2 Post Accident Monitoring System (PAMS) Design

The SysRS requirements were used to develop the following lower tier design documents:

- WNA-DS-01667-WBT-P, Revision 4, "Post Accident Monitoring System-System Design Specification" (SDS) (Hardware)
- WNA-SD-00239-WBT-P, Revision 4, "Software Requirements Specification for the Post Accident Monitoring System" (SRS) (Software)

The relationship between the requirements is documented in WNA-VR-00279-WBT, "Requirements Traceability Matrix for the Post-Accident Monitoring System."

Westinghouse and WBN Unit 2 Engineering worked together to ensure that the requirements from the CCM and SysRS were correctly transferred to the SDS and SRS. This ensured that the design configuration items of the secure operational environment in these documents was correct, accurate, and complete. These documents then served as the basis for the design phase. Refer to WCAP-17427-P, "Watts Bar Nuclear Plant Unit 2 Common Q Post Accident Monitoring System Computer Security Assessment," section 2.4 "Design Phase" for additional information.

WBN Unit 2 engineering review and approval of the lower tier documents and RTM, against the requirements of the SysRS and CCM is the measure taken to prevent the introduction of unnecessary design features or functions that may result in the inclusion of unwanted or unnecessary code. Related design output documents (drawings etc.) are likewise reviewed and approved by WBN Unit 2 Engineering.

The hardware and software design features selected to ensure a secure operational environment are documented in section 2.a below. These include the use of both a software and a hardware data diode as recommended by Regulatory Guide 5.71.

Cyber security of the WBN Unit 2 PAMS is in accordance with the Tennessee Valley Authority (TVA) corporate cyber security program which is designed in accordance with 10 CFR 73.54.

Watts Bar Nuclear Unit 2
Common Q Post Accident Monitoring System
Conformance to the Secure Development and Operational Environment Requirements of
Regulatory Guide 1.152 Revision 3
Page 6 of 12
September 1, 2011

d. Implementation Phase:

Regulatory Position

In the system (integrated hardware and software) implementation phase, the system design is transformed into code, database structures, and related machine executable representations.

The implementation activity addresses hardware configuration and setup, software coding and testing, and communication configuration and setup (including the incorporation of reused software and COTS products).

System Features

The developer should ensure that the transformation from the system design specification to the design configuration items of the secure operational environment is correct, accurate, and complete.

Development Activities

The developer should implement secure development environment procedures and standards to minimize and mitigate any inadvertent or inappropriate alterations of the developed system. The developer's standards and procedures should include testing, (such as scanning), as appropriate, to address undocumented codes or functions that might (1) allow unauthorized access or use of the system or (2) cause systems to behave outside of the system requirements or in an unreliable manner.

The developer should account for hidden functions and vulnerable features embedded in the code, their purpose and their impact on the integrity and reliability of the safety system. These functions should be removed or (as a minimum) addressed (e.g., as part of the failure modes and effects analysis of the application code) to prevent any unauthorized access or degradation of the reliability of the safety system.

COTS systems are likely to be proprietary and generally unavailable for review. In addition, a reliable method may not exist for determining the complete set of system behaviors inherent in a given operating system (e.g., operating system suppliers often do not provide access to the source code for operating systems and callable code libraries). In such cases, unless the application developer can modify these systems, the developer should ensure that the features within the operating system do not compromise the required design features of the secure operational environment so as to degrade the reliability of the digital safety system.

WBN Unit 2 Post Accident Monitoring System (PAMS) Implementation

The secure development environment for the implementation phase is described in Westinghouse WCAP-17427-P, Revision 1, "Watts Bar Nuclear Plant Unit 2 Common Q Post Accident Monitoring System Computer Security Assessment." Hardware secure development is described in Section 2.5 and software secure development is described in Section 3.

Watts Bar Nuclear Unit 2
Common Q Post Accident Monitoring System
Conformance to the Secure Development and Operational Environment Requirements of
Regulatory Guide 1.152 Revision 3
Page 7 of 12
September 1, 2011

e. Test Phase:

Regulatory Position

The objective of testing the design features of the secure operational environment is to ensure that the design requirements intended to ensure system reliability are validated by the execution of integration, system, and acceptance tests where practical and necessary.

Testing includes system hardware configuration (including all connectivity to other systems, including external systems), software integration testing, software qualification testing, system integration testing, system qualification testing, and system factory acceptance testing.

System Features

The secure operational environment design requirements and configuration items intended to ensure reliable system operation should be part of the validation effort for the overall system requirements and design configuration items. Therefore, design configuration items for the secure operational environment are just one element of the overall system validation. Each system design feature of the secure operational environment should be validated to verify that the implemented feature achieves its intended function to protect against inadvertent access or the effects of undesirable behavior of connected systems and does not degrade the safety system's reliability.

Development Activities

The developer should correctly configure and enable the design features of the secure operational environment. The developer should also test the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity. Attention should be focused on built-in original equipment manufacturer features.

WBN Unit 2 Post Accident Monitoring System (PAMS) Testing

The relationship between requirements in the SysRS, SDS and SRS and the items tested in the Channel Integration Test/Factory Acceptance Test (CIT/FAT) (WNA-TP-02988-WBT, Revision 0, "Nuclear Automation Watts Bar Unit 2 NSSS Completion Program I&C Projects, Post Accident Monitoring System Channel Integration Test/Factory Acceptance Test) is documented in the RTM. Refer to WCAP-17427-P, Revision 1, "Watts Bar Nuclear Plant Unit 2 Common Q Post Accident Monitoring System Computer Security Assessment," section 2.6, "Testing Phase" for additional information.

The CIT/FAT included a test of the Maintenance and Test Panel (MTP) software data diode function. The software data diode is the qualified isolation device. Its function is to protect the safety-related PAMS functions from feedback from the Integrated Computer System (ICS). A data storm test of the MTP to ICS connection was performed. As documented in WNA-TR-02426-WBT, "Post-Accident Monitoring System

Watts Bar Nuclear Unit 2
Common Q Post Accident Monitoring System
Conformance to the Secure Development and Operational Environment Requirements of
Regulatory Guide 1.152 Revision 3
Page 8 of 12
September 1, 2011.

Data Storm Test Report," the test confirmed that the MTP performed its qualified isolation function without the data storm impacting the PAMS safety-related functions.

2. Secure Operational Environment

Per Regulatory Guide 1.152, Revision 3 a Secure Operational Environment is defined as the condition of having appropriate physical, logical and administrative controls within a facility to ensure that the reliable operation of digital safety systems are not:

- A) degraded by undesirable behavior of connected systems and
- B) events initiated by inadvertent access to the system.

The Common Q Post Accident Monitoring System (PAMS) installed in Watts Bar Unit 2, uses a combination of design features, access control, procedural controls and testing to provide a secure operational environment. In the following discussion those items associated with undesirable behavior of connected systems will be designed with "(A)" and those with inadvertent access to the system will be designed by "(B)".

a. Design Features

i. System Controls

The system controls provide a hierarchy that limits what can be done at the Operator's Module (OM) or Maintenance and Test Panel (MTP) without breaching at least one access control point and actuating the "PAMS System Trouble" alarm in the Main Control Room (MCR). (B)

- (1) The touch screen on the Operators Modules (OM) on the main control boards and the Maintenance and Test Panel (MTP) can access any of the screens but cannot change any constants or alarm setpoints unless the Function Enable (FE) Keyswitch is placed in the "Enable" position.
- (2) Placing the FE keyswitch in "Enable" allows for enabling print screen function (MTP only), bypassing any input signal, changing selected alarm setpoints, changing alarm reset points, system functional tests, and parameters through the OM and MTP.
- (3) Changing any variable or input requires a two step process (i.e., change and confirm) in order to implement changes.
- (4) With the Software Load Enable (SLE) keyswitch in the "Enable" position at the MTP the technician can install software updates or access the software hard drive to reinstall software.

Watts Bar Nuclear Unit 2
Common Q Post Accident Monitoring System
Conformance to the Secure Development and Operational Environment Requirements of
Regulatory Guide 1.152 Revision 3
Page 9 of 12
September 1, 2011

ii. Locks

Access to the PAMS system hardware requires access to the normally locked PAMS panels in the Auxiliary Instrument Room (AIR) or access to the main control boards. Access to the PAMS panel keys is controlled by Operations. (B)

- (1) The MTP door requires a key to access the system controls.
- (2) The OM Personal Computer (PC) Node Boxes are located in the main control boards which require Operations permission to access. Access to the PC Node Box is required to install the FE keyswitch.

iii. Alarms

The "PAMS Trouble" alarm in the MCR provides notification to the MCR operators of system access based on the following: This prevents access without knowledge of the MCR staff. (B)

- (1) MTP Door Alarm - When the door is opened the "PAMS Trouble Alarm" is actuated in the Main Control Room (MCR).
- (2) Function Enable Keyswitch Alarm - Placing either the MTP or OM FE keyswitch in the "Enable" position actuates the "PAMS Trouble Alarm" in the MCR.
- (3) Software Load Enable (SLE) Keyswitch Alarm - Placing the SLE Keyswitch on the MTP in the "Enable" position actuates the "PAMS Trouble Alarm" in the MCR.

iv. Software Data Diode

The MTP is the qualified isolation device between the PAMS and the ICS. Isolation between the MTP and ICS is accomplished by a software program that restricts the Transmission Control Protocol/Internet Protocol (TCP/IP) traffic coming into the MTP to only the specific TCP/IP commands necessary to maintain the flow of information from the MTP to the ICS. (A)

v. Hardware Data Diode

In addition to the MTP software data diode, a non-qualified hardware data diode is installed between the MTP and ICS. This provides a backup to the MTP software data diode. (A)

vi. Keyswitches

The use of keyswitches limits the ability of operators or technicians to inadvertently access the system control functions. Specifically:

- (1) The keys for the FE keyswitches on the OM and MTP are removable from the "OFF" position only.

(2) The key for the SLE keyswitch on the MTP shall be removable from the "OFF" position only.

(3) The FE and SLE keyswitches are keyed differently.

Having the keys removable in the "OFF" position only prevents an operator or technician from inadvertently leaving the key without the MCR operator's knowledge because the "PAMS Trouble Alarm" would not reset. (B)

Having the keyswitches keyed differently prevents inadvertent operation of the wrong switch. (B)

vii. Analog Inputs

With the exception of the connection to the ICS, all external system connections are via analog links. The use of analog connections eliminates the potential for external system issues from propagating to the PAMS. (A)

b. Access Control

i. Plant Access control procedures

Access to the protected area of the plant requires that personnel pass required screening to ensure they are reliable. The Continuous Behavior Observation Program is designed to detect if there is a change in behavior that would call into question the reliability and trustworthiness of personnel with unrestricted access. (B)

ii. Equipment Location

The PAMS equipment is located in the MCR and AIR. These are vital areas and only those personnel with a need to access vital areas are allowed to enter these areas. (B)

c. Procedural Controls

i. Control of Keys

Procedural control of keys prevents inadvertent access to the PAMS hardware. The specific controls are: (B)

(1) Technical Instruction TI-12.09, "Plant Key Control"

(a) Keys must be checked out from: On Shift Manager (SM), Unit Supervisor (US), Work Control Center (WCC) Shift Technical Advisor (STA)/Senior Reactor Operator (SRO).

(b) Keys must be returned by the end of each shift.

Watts Bar Nuclear Unit 2
Common Q Post Accident Monitoring System
Conformance to the Secure Development and Operational Environment Requirements of
Regulatory Guide 1.152 Revision 3
Page 11 of 12
September 1, 2011

- (c) Keys stored in the MCR must be accounted for by the off going US at the end of each shift.
 - (d) Keys stored in the WCC must be accounted for the off going STA/SRO at the end of each shift.
 - (e) The SM's Clerk performs a daily verification of the keys that are stored in the Shift Operations Supervisor Office
- (2) Periodic Instruction 0-PI-OPS-12.0, "Key Accountability Verification"
- (a) Key accountability is verified annually
- ii. Software Control, NPG-SPP-12.7 "Computer Software Control"
- (1) Requires documentation of the approved version
 - (2) Requires secure storage of the media
 - (3) Requires that changes be processed using the design change process.

d. Testing

As part of the (CIT/FAT) a data storm test was performed on the MTP digital interface with the ICS. As documented in WNA-TR-02426-WBT, "Post-Accident Monitoring System Data Storm Test Report," the test confirmed that the MTP performed it's qualified isolation function without the data storm impacting the PAMS safety-related functions. (A)

After the system is installed a site acceptance test (SAT) will be performed in accordance with WNA-TP-03945-WBT, Rev. 1 "Post Accident Monitoring System Site Acceptance Test Procedure."

Watts Bar Nuclear Unit 2
Common Q Post Accident Monitoring System
Conformance to the Secure Development and Operational Environment Requirements of
Regulatory Guide 1.152 Revision 3
Page 12 of 12
September 1, 2011

References

1. Regulatory Guide 1.152, Revision 3, "Criteria For Use Of Computers In Safety Systems Of Nuclear Power Plant" U.S. Nuclear Regulatory Commission, July 2011.
2. WNA-VR-00279-WBT, Revision 4, "Requirements Traceability Matrix for the Post-Accident Monitoring System" Westinghouse Electric Company LLC.
3. WNA-DS-01617-WBT-P, Revision 4, "Post Accident Monitoring System-System Requirements Specification," Westinghouse Electric Company LLC.
4. WNA-DS-01667-WBT-P, Revision 4, "Post Accident Monitoring System-System Design Specification," Westinghouse Electric Company LLC.
5. WNA-SD-00239-WBT-P, Revision 4, "Software Requirements Specification for the Post Accident Monitoring System," Westinghouse Electric Company LLC.
6. WNA-LI-00058-WBT-P, Revision 3, "Post-Accident Monitoring System (PAMS) Licensing Technical Report," Westinghouse Electric Company LLC.
7. WNA-TP-02988-WBT, Revision 0, "Nuclear Automation Watts Bar Unit 2 NSSS Completion Program I&C Projects, Post Accident Monitoring System Channel Integration Test/Factory Acceptance Test," Westinghouse Electric Company LLC.
8. WCAP-16096-NP-A, Revision 1A, "Software Program Manual for Common Q Systems," Westinghouse Electric Company LLC.
9. WCAP-17427-P, Revision 1, "Watts Bar Nuclear Plant Unit 2 Common Q Post Accident Monitoring System Computer Security Assessment," Westinghouse Electric Company LLC.
10. TVA Procedure TI-12.09, Revision 6, "Plant Key Control"
11. TVA Procedure 0-PI-OPS-12.0, Revision 7, "Key Accountability Verification"
12. TVA Procedure NPG-SPP-12.7, Revision 1, "Computer Software Control"
13. WNA-TR-02451-WBT, Rev. 0 "Test Summary Report for the Post Accident Monitoring System," Westinghouse Electric Company LLC.
14. WNA-TP-03945-WBT, Rev. 1 "Post Accident Monitoring System Site Acceptance Test Procedure," Westinghouse Electric Company LLC.
15. WNA-TR-02426-WBT, Revision 1, "Post-Accident Monitoring System Data Storm Test Report," Westinghouse Electric Company LLC.