Attachment 25

Non-proprietary Westinghouse Electric Company document WNA-AR-00189-WBT-NP, "Post Accident Monitoring System Reliability Analysis," Revision 1

Westinghouse

Westinghouse Non-Proprietary Class 3

Nuclear Automation
Watts Bar Unit 2 NSSS Completion Program
I&C Projects

Post Accident Monitoring System Reliability Analysis

WNA-AR-00189-WBT-NP,
Rev. 1

October 2011

APPROVALS

Function	Name and Signature
Author	Stephen A. Nass* Principal Engineer, Risk Applications & Methods I
Reviewer	Dennis N. Menard* Principal Engineer, Safety Systems Support & Upgrades
	Stephanie L. Smith* Project Manager, Nuclear Automation Licensing
Approver	Robert E. Single* Manager, Reactor Protection Systems AP1000 China

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

WESTINGHOUSE NON-PROPRIETARY CLASS 3

LIST OF CONTRIBUTORS

Revision	Name and Title
0, 1	Jenna L. Tyger Technical Editor, Technical Communications
1	Matthew A. Shakun Engineer, Nuclear Automation Licensing

REVISION HISTORY

RECORD OF CHANGES

Revision	Author	Description	Completed
0	Stephen A. Nass	This version is based on WNA-AR-00189-WBT with proprietary information redacted.	08/10
1	Stephen A. Nass	Figures 2.1-1 and 2.1-2 were updated. References were updated to latest applicable revision. Minor editorial and formatting changes were made.	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

TABLE OF CONTENTS (cont.)

TABLE OF CONTENTS (cont.)

LIST OF TABLES

LIST OF FIGURES

TABLE OF CONTENTS (cont.)

LIST OF FIGURES (cont.)

ACRONYMS AND TRADEMARKS

Acronyms used in the document are defined in WNA-PS-00016-GEN, "Standard Acronyms and Definitions" (Reference 1), or included below to ensure unambiguous understanding of their use within this document.

Acronym	Definition
AC160	Advant Controller series 160
AF100	Advant Fieldbus 100
CCF	Common Cause Failure
CET	Core Exit Thermocouples
Common Q	Common Qualified Platform
DC	Direct Current
FMEA	Failure Modes and Effects Analysis
FPD	Flat Panel Display
MTP	Maintenance and Test Panel
OM	Operator's Module
PAMS	Post Accident Monitoring System
PC	Personal Computer
RBD	Reliability Block Diagram
RJT	Reference Junction Thermocouple
SMM	Sub-cooled Margin Monitor
SWCMF	Software Common Mode Failure

Advant is a registered trademark of ABB Process Automation Corporation.

QNX is a registered trademark of QNX Software Systems GmbH & Co. KG ("QSSKG") and is used under license by QSS.

Common Q is a trademark or registered trademark in the United States of Westinghouse Electric Company LLC, its subsidiaries and/or its affiliates. This mark may also be used and/or registered in other countries throughout the world. All rights reserved. Unauthorized use is strictly prohibited.

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

Standard terms used in the document are defined in WNA-PS-00016-GEN, "Standard Acronyms and Definitions" (Reference 1), or included below to ensure unambiguous understanding of their use within this document.

Term	Definition
None.	

REFERENCES

Following is a list of references used throughout this document.

1. WNA-PS-00016-GEN, Rev. 5, "Standard Acronyms and Definitions," Westinghouse Electric Company LLC.

2. WCAP-16097-P-A, Appendix 1, "Common Qualified Platform Post Accident Monitoring Systems," Westinghouse Electric Company LLC.

3. ANSI/IEEE 352, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Stations Safety Systems," Institute of Electrical and Electronics Engineers, Inc., 1987.

4. 00000-ICE-30156, Rev. 8, "System Requirements Specification for the Common Q Post Accident Monitoring System," Westinghouse Electric Company LLC.

5. WNA-DS-01617-WBT-P, Rev. 4, "Post Accident Monitoring System – System Requirements Specification," Westinghouse Electric Company LLC.

6. WNA-DS-01667-WBT-P, Rev. 4, "Post Accident Monitoring System - System Design Specification," Westinghouse Electric Company LLC.

7. 00000-ICE-30155, Rev. 11, "System Requirements Specification for the Common Q Generic Flat Panel Display," Westinghouse Electric Company LLC.

8. WNA-AR-00180-WBT-P, Rev. 2, "Failure Modes and Effects Analysis (FMEA) for the Post Accident Monitoring System," Westinghouse Electric Company LLC.

9. Watts Bar Technical Specification - Section 3.3.3 Post-Accident Monitoring (PAM) Instrumentation, Amendment 55.

10. WNA-IG-00056-GEN, Rev. 1, "Standard Reliability Analysis Guidelines," Westinghouse Electric Company LLC.

11. WNA-IG-00064-GEN, Rev. A, "Reliability and Availability Analysis Methods," Westinghouse Electric Company LLC.

12. GKW F 310 708, Rev. 0, "Reliability Data Sheet, Advant Controller 160 Including S600 I/O," ABB Power Plant Control, February 16, 1998.

13. MIL-HDBK-217F, "Military Handbook reliability Prediction of Electronic Equipment," U.S. Department of Defense, December 2, 1991.

14. NPRD-95, "Nonelectronic Parts Reliability Data," U.S. Department of Defense Reliability Analysis Center, 1995.

REFERENCES (cont.)

15. NUREG/CR-6928, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," U.S. Nuclear Regulatory Commission, February 2007.

(Last Page of Front Matter)

SECTION 1
INTRODUCTION

1.1 PURPOSE

This reliability study provides an estimation of the availability of the Watts Bar Unit 2 Post Accident Monitoring System (PAMS), which is based on the Common Q™ safety platform described in WCAP-16097-P-A, "Common Qualified Platform Post Accident Monitoring Systems," Appendix 1 (Reference 2).

1.2 SCOPE

The scope of the analysis shall include all of the electronics provided for PAMS under the Watts Bar Unit 2 NSSS Completion Program Instrumentation & Control (I&C) Project, and the sensors that provide input to the functions of PAMS.

This availability analysis is done in accordance with the guidance provided in ANSI/IEEE Standard 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Stations Safety Systems" (Reference 3). Specifically, the Reliability Block Diagram (RBD) method described in clause 4.3 of that standard will be applied. Other guidance on availability quantification found in the standard will also be applied as appropriate.

1.3 AVAILABILITY GOALS

00000-ICE-30156, "System Requirements Specification for the Common Q Post Accident Monitoring System" (Reference 4, subsection 3.3.3.2) establishes the operational unavailability goal of [ ]^{a,c}. The quantitative results of this study will be compared to this goal.

1.4 SUMMARY OF RESULTS

The analysis has shown that the estimated availability of PAMS is [ ]^{a,c}. This compares favorably with the required availability of [ ]^{a,c}.

(Last Page of Section 1)

SECTION 2
SYSTEM DESCRIPTION

2.1 SYSTEM ARCHITECTURE

The Watts Bar Unit 2 PAMS is described in WNA-DS-01617-WBT-P, Rev. 4, "Post Accident Monitoring System – System Requirements Specification" (Reference 5) and WNA-DS-01667-WBT-P, Rev. 4, "Post Accident Monitoring System - System Design Specification" (Reference 6). This system is a two train data acquisition and display system that also performs calculations on the input variables to determine margins to critical safety function limits. Figure 2.1-1 (refer to Reference 6, Figure 2.1-1) shows the basic architecture of the Watts Bar Unit 2 PAMS. Figure 2.1-2 (refer to Reference 6, Figure 4.2-2) shows the power distribution diagram for the Watts Bar Unit 2 PAMS.

The Watts Bar Unit 2 PAMS consists of two separate Class 1E trains that are built on an Advant® Controller 160 (AC160) platform. Each of the two independent trains is capable of carrying out the required functions. Each train consists of two AC160 racks, a power supply, and one maintenance and test panel (MTP). Each train is mounted in a dedicated cabinet, with identical hardware. An operator's module (OM) for each train is also provided in the main control room.

Each train of PAMS has a flat panel display (FPD) for its MTP and OM. The system requirements specification for the FPD is provided in 00000-ICE-30155, Rev. 11, "System Requirements Specification for the Common Q Generic Flat Panel Display" (Reference 7).

The elements of the PAMS components are interconnected by a fiber optic Advant Fieldbus 100 (AF100) communications network.

a,c

Figure 2.1-1. PAMS Configuration

a,c

Figure 2.1-2. Power Distribution Wiring Diagram

2.2 FAILURE MODES AND EFFECTS

The relationship of the various components of PAMS to the operational availability of the system is discussed in WNA-AR-00180-WBT-P, "Failure Modes and Effects Analysis (FMEA) for the Post Accident Monitoring System" (Reference 8). The reliability modeling contained in this study is based on that FMEA report.

(Last Page of Section 2)

SECTION 3
ANALYSIS ASSUMPTIONS AND CONSIDERATIONS

The following assumptions and considerations apply to this reliability analysis:

1. The goal of this study is to estimate the operational unavailability of PAMS, where:

   Operational Unavailability = Downtime/Operating Time

2. Downtime shall include the duration of random hardware failures until such time as they are repaired. It shall also include any time spent in planned maintenance activities such as periodic surveillance testing when that activity is planned to be performed during normal operation (Tech Spec Modes 1-3) (Technical Specification – Section 3.3.3, Post-Accident Monitoring (PAM) Instrumentation, Reference 9). However, since the planned surveillance test interval for activities that require taking a channel "off-line" is 24 months, it is assumed that this activity will be performed during Modes 4-6.

3. PAMS shall be considered to be available if either one of the redundant trains is available.

4. The availability analysis assumes only single random independent failures. The mean time to repair (MTTR) is orders of magnitude smaller than the mean time between failure (MTBF) for all PAMS modules and components. Therefore, multiple failures are not considered.

5. A PAMS Train is considered to be available if it is completely capable of performing its system function. Train availability requires all of the following:

[

]a,c

[

]^{a,c}

6. The availability of the process measurements received from the existing I&C systems will be estimated using typical failure rates and repair times for the sensors and devices such as isolators that are directly in the signal path.

7. Loss of the watch dog timer input that is used to synchronize time display will not cause the unavailability of the train.

8. While failure of the digital output card may defeat the alarm function, this information is also available through the operator workstation displays. Therefore, these modules may be excluded from the analysis.

9. [ ]^{a,c}

10. Repairs of cabinet and control desk mounted electronic equipment will only be performed during the daylight shift. This assumption is justified by the allowance of operation with one PAMS channel out of service for an extended period of time. [ ]^{a,c}

11. The [ ]^{a,c} can only be replaced during the refueling outage, which has a 24 month interval.

12. Common cause failure (CCF) can be ignored in the quantitative analysis. This is justified by the relatively high goal for operational unavailability. The chance for hardware CCF is largely reduced through the environmental qualification of the equipment. The residual causes, such as design error and maintenance induced failures, are generally considered to be less than 1 percent

of the failure rate of a single non-redundant component. Thus, hardware CCF probabilities are less than the uncertainties of the analysis.

13. Software common mode failure (SWCMF) is excluded from the availability analysis. The industry has not developed a satisfactory method of quantifying software reliability or the likelihood of SWCMF. However, it is generally accepted that, for software that is developed using a high quality process and is subjected to Verification and Validation (V&V), the probability of SWCMF is less than 10-4. Thus, SWCMF probabilities are less than the uncertainties of the analysis.

14. The analysis will exclude external failure mechanisms including fire, flood, physical damage by force, maintenance errors, electromagnetic interference, and environments beyond those specified in the System Requirements Specification.

15. Surveillance testing will be conducted on a 24 month basis during refueling outages. This testing will reveal all failures that affect functional availability that were not previously disclosed through self-diagnostics or routine operator observation of the control room displays. The contribution of the test to each train downtime is assumed to be zero since the tests will be conducted during a plant mode where the PAMS function is not required by the Tech Specs.

16. The MTP is excluded from the calculation of operational unavailability on the basis that if an MTP is found to be inoperative when the technician has a task requiring it, there is sufficient time available to repair the MTP and then accomplish the task in a timely manner.

17. Failures of passive components, such as cables and connectors, can be neglected since their failure effects are the same as those of the components they connect, and their failure rate is more than an order of magnitude smaller than the active components.

18. The computers implementing PAMS perform a comprehensive set of diagnostics aimed at the early detection of failures. Furthermore, the redundant measurements being displayed by PAMS are continuously compared against each other so that discrepancies caused by failures will be immediately brought to the attention of the operator. Therefore, it is assumed, with a few exceptions, that the detectability of failures is 100 percent, either by intentional diagnostics or by obvious evidence to the plant operator. The exceptions are:

    a. While the coverage of the diagnostics performed by the AC160 processor is high, there may be some undetected failures, such as in the floating point computational sections of the microprocessor, that would only be discovered during the channel calibration performed every 24 months. Therefore, the detectability of the PM646A module is set to [ ]^{a,c}.

    b. The personal computer (PC) node box does not perform as extensive a set of diagnostics as the primary AC160 controller. There could be some failure that would prevent transfer of fresh data, but that would be obscure to the operator looking at the display. Therefore, the detectability of the PC node box is set to [ ]^{a,c}.

c. The vast majority of failures of the analog input modules will either be detectable by the on-line diagnostics or by a comparison of the redundant measurements. However, it is possible that a small calibration shift could occur that would cause the channel to be out of specification, but would not cause a sufficient enough deviation in the signal to raise an alarm. Such failures would be detected during calibration. Engineering judgment places the likelihood of such occurrence at less than 1 percent; thus, the detectability of analog input modules is set at [ ]^{a,c}.

19. Based on the recommended spare parts inventory, it is assumed that replacement parts are available at the site for MTTR calculations.

20. For purposes of determining component availability, worst case scenarios are considered with regards to selecting failure mode, probability of detection (Pd), and surveillance test interval (Ts).

(Last Page of Section 3)

SECTION 4
RELIABILITY MODELING

4.1 BLOCK DIAGRAM MODELS

This study will apply the RBD method that is described in ANSI/IEEE 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Stations Safety Systems" (Reference 3) and WNA-IG-00056-GEN, Rev. 1, "Standard Reliability Analysis Guidelines" (Reference 10). Figure 4.1-1 shows the top level RBD for PAMS functional availability. It consists of the two redundant trains.

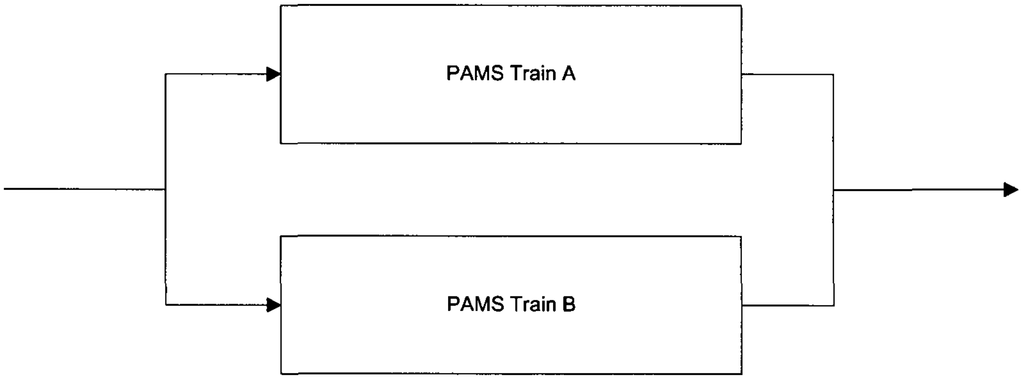

Figure 4.1-1. Top Level PAMS RBD

Each of the PAMS trains requires proper function of [ ]^{a,c} in order to be considered available. This is shown in Figure 4.1-2.

a,c

[ ]

Figure 4.1-2. Typical PAMS Train RBD

Proper function of the RF616 primary subrack requires the [ ]^{a,c}. The RBD for the RF616 primary subrack is shown in Figure 4.1-3. The required digital sensor inputs consist of [ ]^{a,c}. The RBD for the sensor inputs for the DI620 module is shown in Figure 4.1-4. The required analog sensor inputs consist of [ ]^{a,c}. The RBD for the sensor inputs for the AI688 modules is shown in Figure 4.1-5.

a,c

Figure 4.1-3. RF616 Primary Subrack RBD

a,c

Figure 4.1-4. Sensor Inputs for DI620 Module at Position 4 RBD

a,c

Figure 4.1-5. Sensor Inputs for AI688 Modules at Positions 5 and 6 RBD

Proper function of the RF620 extension subrack requires the [ ]^{a,c}. The RBD for the RF620 extension subrack is shown in Figure 4.1-6. The required analog sensor inputs [ ]^{a,c}

[$]^{a,c}$.

The required analog sensor inputs [$]^{a,c}$. The RBDs for the sensor inputs for the AI687 modules is shown in Figures 4.1-7 and 4.1-8.

a,c

Figure 4.1-6. RF620 Extension Subrack RBD

a,c

Figure 4.1-7. Sensor Inputs for AI687 Card at Positions 11, 12, and 13 RBD

a,c

[ ]

Figure 4.1-8. Sensor Inputs for AI687 Card at Position 14 RBD

Power to the PAMS components is supplied through a Common Q power supply assembly. [

]^{a,c} The RBD for the PAMS power supply is shown in Figure 4.1-9. The bulk power supply supplies power [

]^{a,c} The bulk power supply RBD is shown in Figure 4.1-10. [

]^{a,c} The power supply RBDs for these modules are shown in Figures 4.1-11, 4.1-12, and 4.1-13.

a,c

[ ]

Figure 4.1-9. Power Supply RBD

a,c

[ ]

Figure 4.1-10. Bulk Power Supply RBD

a,c

Figure 4.1-11. Chassis Power Supply RBD

a,c

Figure 4.1-12. DP1, DP2, and DP3 Power Supply RBD

a,c

Figure 4.1-13. Aux Power Supply RBD

A typical operator workstation display RBD is shown in Figure 4.1-14. [
]^{a,c}

a,c

Figure 4.1-14. OM RBD

The AF100 communications is shown in Figure 4.1-15. [
]^{a,c}

a,c

Figure 4.1-15. Communications RBD

The plant computer link requires [
]^{a,c}. This is shown in Figure 4.1-16.

a,c

Figure 4.1-16. Plant Computer Link RBD

4.2 AVAILABILITY EQUATIONS

The equations and definitions presented in this section are used to perform the reliability analysis. They apply to repairable equipment with failures that occur randomly in time, and are based on the equations presented in Section 2 of WNA-IG-00064-GEN, Rev. A, "Reliability and Availability Analysis Methods" (Reference 11).

4.2.1 Component Availability

The probability that a component will perform its function at a given instant in time is the availability of that component. From EQN 2-5 in Reference 11, component availability is expressed as:

$$A_n = \left[1 + \lambda \cdot \left((1 - P_d) \cdot \frac{T_s}{2} + T_R\right)\right]^{-1} \qquad \text{Eq. 4-1}$$

where,

A_n is the availability of the nth component
λ is the component failure rate in hours
P_d is the probability of immediate detection of failure by diagnostics
T_s is the surveillance test interval
T_R is the MTTR the failure including any "wait time"

The failure rate (λ) of a component is related to its MTBF as follows (from EQN 2-2 in Reference 11):

$$\lambda = {}^{1}\!/_{MTBF} \qquad \text{Eq. 4-2}$$

Also from EQN 2-5 in Reference 11, the complement of availability (i.e., the component unavailability), is expressed as:

$$U_n = 1 - A_n \qquad \text{Eq. 4-3}$$

where,

U_n is the unavailability of the nth component

4.2.2 System Availability

When multiple units are combined in a system to accomplish a function, the system availability can be determined from the availability of the individual units using the following equations.

From EQN 2-9 in Reference 11, for a number (n) of components in a series arrangement where failure of any one component may cause failure of the system, the combined availability (A_s) is expressed as:

$$A_s = \prod_{i=1}^{n} A_i \qquad \text{Eq. 4-4}$$

From EQN 2-10 in Reference 11, for a number (n) of components in a parallel arrangement where any one of the components is sufficient to carry out the function, the combined availability (A_p) is expressed as:

$$A_p = 1 - \prod_{i=1}^{n} (1 - A_i) \qquad \text{Eq. 4-5}$$

From EQN 2-11 in Reference 11, for the case of majority voting (coincidence of M-out-of-N components), the combined availability ($A_{M/N}$) is expressed as:

$$A_{M/N} = \sum_{r=0}^{N-M} \binom{N}{r} A^{N-r} (1 - A)^r \qquad \text{Eq. 4-6}$$

The complement of the system availability (i.e., the system unavailability), is expressed as:

$$U_{sys} = 1 - A_{sys} \qquad \text{Eq. 4-7}$$

where,

U_{sys} is the unavailability of the system A_{sys}

(Last Page of Section 4)

SECTION 5
FAILURE RATE DATA

5.1 AC160 COMPONENTS

Failure rates for the AC160 components are taken from GKW F 310 708, Rev. 0, "Reliability Data Sheet, Advant Controller 160 Including S600 I/O" (Reference 12). They represent an estimation basis on a methodology similar to that found in MIL-HDBK-217F, "Military Handbook reliability Prediction of Electronic Equipment" (Reference 13), but using component failure rate data from ABB experience. Table 5.1-1 contains the AC160 failure rates pertinent to this study.

Table 5.1-1. AC160 Failure Rate Data

b,c

Module Identifier	Description	λ [failures/ 10^6 hours]	Notes
Circuit Breaker		0.3574	7
RFI Suppresser		0.1958	7
Line Filter		0.1958	7
Bulk Power Supply	300 Vdc front end module	1.5811	7
Chassis Power Supply	24 Vdc chassis power supply module	1.5811	7
DP Cell Power Supply	28 Vdc DP cell power supply module	1.5811	7
Aux Power Supply	24 Vdc Auxiliary power supply module	1.5811	7
Diode	Diode	0.0209	8

Table 5.1-1. AC160 Failure Rate Data (cont.)

Notes:

1. [
]^{a,c}

2. [
]^{a,c}

3. [
]^{a,c}

4. [
]^{a,c}

5. [
]^{a,c}

6. [
]^{a,c}

7. The failure rates are obtained from NPRD-95, "Nonelectronic Parts Reliability Data" (Reference 14) as follows:
   - Circuit Breaker (Molded Case) from page 2-38
   - Line Filter and RFI Suppressor (Module, Line, Power) from page 2-142
   - Power Supplies from page 2-153

8. The failure rate is calculated using the methodology specified in Reference 13, Section 6.1. The environment is assumed to be Ground Benign (G_B), which represents non-mobile, temperature and humidity controlled environments that are readily accessible to maintenance. In addition, commercial (non-military) quality grade is assumed.

   λ_b = 0.0030 (power rectifier/Schottky power diode)

   π_T = 3.0 (T_J = 60°C, nominal G_B ambient plus 25°C junction rise)

   π_S = 0.29 (V applied/V rated between 50% to 60%)

   π_C = 1.0 (metallurgically bonded contact)

   π_Q = 8.0 (plastic quality)

   π_E = 1.0 (G_B)

   The failure rate is $\lambda_p = \lambda_b \pi_T \pi_S \pi_C \pi_Q \pi_E = 0.0209 \times 10^{-6}$ failures/hour

5.2 SENSORS

Since there is no Watts Bar Unit 2 plant-specific failure rate data available, generic industry data from NUREG/CR-6928, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants" (Reference 15) was used to estimate reasonable failure rates for the plant sensors. The mean value of λ for sensors/transmitters of 0.8×10^{-6} failures per hour is listed in Table A.2.43-4 in Reference 15. This value was used for each of the sensor inputs to the PAMS input modules.

5.3 FLAT PANEL DISPLAYS

The FPDs used in the operator workstations are relatively new devices. As such, there is not an experience basis for estimating their failure rate. For the purpose of this analysis, it will be assumed that their failure rate, including that of the input devices used to make display selections (touch screen and trackball), is 50 x 10^{-6} failures/hour. This is more than twice that of a typical PC.

5.4 PC NODE BOX

Like the FPD, there is not a substantial amount of experience data available for the PC node box that drives this display. The following assumptions are made for this collection of equipment:

- The failure rate of the mother board is the same as for the AC160 processor – [ ]^{a,c}
- The failure rate of the AF100 bus communications and TCP/IP controllers is the same as the communications controller in the AC160 sub-rack – [ ]^{a,c}
- The failure rate of the power supply is the same as for AC160 (although in this case it is not redundant) – [ ]^{a,c}
- The failure rate of the compact flash memory from which the computer boots is [ ]^{a,c}
- Rotating devices (CD ROM drives, floppy drives, etc.) and other peripherals such as keyboards are not required for continued operation, rather they are only needed for maintenance

Thus the total failure rate of the QNX® PC that drives the FPDs is [ ]^{a,c} (mother board plus compact flash memory). The power supply and communications controllers are modeled separately.

5.5 PROBABILITY OF FAILURE DETECTION

As defined in equation 1 in Section 4, probability of detection (*Pd*) is the probability that a failure is detected by system diagnostics. In general, failures that are immediately detected by diagnostics are assigned a value of 1.00. The computers implementing PAMS perform a comprehensive set of diagnostics aimed at the early detection of failures. Furthermore, the redundant measurements being displayed by PAMS are continuously compared against each other so that discrepancies caused by failures will be immediately brought to the attention of the operator. Therefore, it is assumed, with a few exceptions, that the detectability of failures is 100 percent, either by intentional diagnostics or by obvious evidence to the plant operator.

In a few cases, the failure modes of components warrant assigning a value other than 1.00. These cases are discussed below.

- While the coverage of the diagnostics performed by the AC160 processor is high, there may be some undetected failures, such as in the floating point computational sections of the microprocessor that would only be discovered during the channel calibration performed every 24 months. [ ]^{a,c}

- The PC node box does not perform as extensive a set of diagnostics as the primary AC160 controller. There could be some failure that would prevent transfer of fresh data, but that would be obscure to the operator looking at the display. [ ]^{a,c}

- The majority of analog input module failures are detected by the on-line diagnostics or by a comparison of the redundant measurements. However, it is possible that a small calibration shift could occur that would cause the channel to be out of specification, but would not cause a sufficient enough deviation in the signal to raise an alarm. Such failures would be detected during calibration. Engineering judgment conservatively places the probability of this failure at less than five percent. [ ]^{a,c}

5.6 SURVEILLANCE TEST INTERVAL

Based on equation 1 in Section 4, surveillance test interval (*Ts*) is meaningful only in cases where the *Pd* is < 1.00. Therefore, *Ts* is assigned a value of zero when probability of detection is assigned a value of 1.00.

Otherwise, surveillance testing will be conducted on a 24 month basis during refueling outages. This testing will reveal all failures that affect functional availability that were not previously disclosed through self-diagnostics or routine operator observation of the control room displays. The contribution of the test to each channel downtime is assumed to be zero since the tests will be conducted during a plant mode where the PAMS function is not required by the technical specifications.

5.7 MEAN TIME TO REPAIR

MTTR values are assigned using the guidance provided in Section 7 of Reference 11. The twelve repair segments described therein are utilized with the single exception that Access Control (Repair Segment III) is replaced with Work Order Processing. Given that the PAMS equipment is located in accessible areas, access to the equipment simply involves obtaining a key from the Plant Operating Staff. The time allocation for this activity is included in Briefing (Repair Segment II).

Table 5.7-1 provides the estimated MTTR for PAMS components that are considered in the reliability analysis.

Table 5.7-1. MTTR

a,c

Repair Segment	Description	Normal Duration (hours)

(Last Page of Section 5)

SECTION 6
RELIABILITY CALCULATIONS

6.1 PAMS AVAILABILITY

Using the data presented in Section 5, the MTBF and availability of the PAMS components are calculated using Eq. 4-1 and Eq. 4-2 from Section 4. The results of these calculations are presented in Table 6.1-1.

Table 6.1-1. PAMS Component Availability

a,c

Component	λ (failures/ 10^6 hours)	MTBF (hours)	P_d	T_s (hours)	MTTR (hours)	A_n	U_n

Table 6.1-1. PAMS Component Availability (cont.)

Component	λ (failures/ 10^6 hours)	MTBF (hours)	P_d	T_s (hours)	MTTR (hours)	A_n	U_n

a,c

The remaining tables presented in this section contain spreadsheets that calculate, using the equations in Section 4.2, the PAMS availability based on the RBDs presented in Section 4.1. In order to enhance understanding of the calculations, the relationships between the rows in each table are shown by circles and arrows.

The RBD for the plant computer link is shown in Figure 4.1-16 and the availability is calculated in Table 6.1-2.

Table 6.1-2. Plant Computer Link Availability

Component	Source	A_n	U_n

a,c

The RBD for the communications is shown in Figure 4.1-15 and the availability is calculated in Table 6.1-3.

Table 6.1-3. Communications Availability

a,c

Component	Source	A_n	U_n

The RBD for the OM is shown in Figure 4.1-14 and the availability is calculated in Table 6.1-4.

Table 6.1-4. OM Availability

a,c

Component	Source	A_n	U_n

The RBD for the auxiliary power supply is shown in Figure 4.1-13 and the availability is calculated in Table 6.1-5.

Table 6.1-5. Auxiliary Power Supply Availability

a,c

Component	Source	A_n	U_n

The RBD for the DP cell power supplies is shown in Figure 4.1-12 and the availability is calculated in Table 6.1-6.

Table 6.1-6. DP Cell Power Supply Availability

a,c

Component	Source	A_n	U_n

The RBD for the chassis power supply is shown in Figure 4.1-11 and the availability is calculated in Table 6.1-7.

Table 6.1-7. Chassis Power Supply Availability

a,c

Component	Source	A_n	U_n

The RBD for the bulk power supply is shown in Figure 4.1-10 and the availability is calculated in Table 6.1-8.

Table 6.1-8. Bulk Power Supply Availability

a,c

Component	Source	A_n	U_n

The RBD for the power supply availability is shown in Figure 4.1-9, and the availability is calculated in Table 6.1-9.

Table 6.1-9. Power Supply Availability

a,c

Component	Source	A_n	U_n

The RBD for the sensor inputs for the AI687 card at position 14 is shown in Figure 4.1-8, and the availability is calculated in Table 6.1-10.

Table 6.1-10. Sensor Inputs for AI687 Card at Position 14 Availability

a,c

Component	Source	A_n	U_n

The RBD for the sensor inputs for the AI687 cards at positions 11, 12, and 13 is shown in Figure 4.1-7, and the availability is calculated in Table 6.1-11.

Table 6.1-11. Sensor Inputs for AI687 Cards at Positions 11, 12 and 13 Availability

a,c

Component	Source	A_n	U_n

The RBD for the RF620 extension subrack is shown in Figure 4.1-6. [

]^{a,c}

The availability for the RF620 extension subrack is calculated in Table 6.1-12.

Table 6.1-12. RF620 Extension Subrack Availability

a,c

Component	Source	A_n	U_n

The RBD for the sensor inputs for the AI688 modules at positions 5 and 6 is shown in Figure 4.1-5 and the availability is calculated in Table 6.1-13.

Table 6.1-13. Sensor Inputs for AI688 Modules at Positions 5 and 6 Availability

a,c

Component	Source	A_n	U_n

The RBD for the sensor inputs for the DI620 module at position 4 is shown in Figure 4.1-4 and the availability is calculated in Table 6.1-14.

Table 6.1-14. Sensor Inputs for DI620 Module at Position 4 Availability

a,c

Component	Source	A_n	U_n

The RBD for the RF616 primary subrack is shown in Figure 4.1-3 and the availability is calculated in Table 6.1-15.

Table 6.1-15. RF616 Primary Subrack Availability

a,c

Component	Source	A_n	U_n

The RBD for a typical PAMS train is shown in Figure 4.1-2 and the availability is calculated in Table 6.1-16.

Table 6.1-16. Typical PAMS Train Availability

a,c

Component	Source	A_n	U_n

The RBD for PAMS is shown in Figure 4.1-1 and the availability is calculated in Table 6.1-17.

Table 6.1-17. PAMS System Availability

a,c

Component	Source	A_n	U_n

6.2 SENSITIVITIES

One measure of the importance of individual components to the overall unavailability of a system is the fractional change in system availability with the component guaranteed not to fail or be out of service. This importance measure is the Fussell Vesely (FV) of the component. Equation 6-1 shows the calculation of the FV for a component X.

$$FV = \left(U_{Baseline} - U_{X=0}\right) \Big/ U_{Baseline} \qquad \text{Eq. 6-1}$$

where,

$U_{Baseline}$ is the PAMS unavailability with all components at their baseline failure rates (λ) and
$U_{X=0}$ is the PAMS unavailability with component X failure rate set to 0.

Table 6.2-1. Component FV Importance

a,c

Component	Baseline λ	PAMS Unavailability w/λ = 0	FV

Table 6.2-1. Component FV Importance (cont.)

a,c

Component	Baseline λ	PAMS Unavailability w/λ = 0	FV

The components listed in Table 6.2-1 are sorted by their FV importance. This shows that an improvement in the reliability of the [ ]^{a,c} has the greatest effect on the overall PAMS unavailability. It also shows that [ ]^{a,c} improvement of the overall PAMS unavailability.

(Last Page of Section 6)

Attachment 26

Westinghouse Electric Company document CAW-11-3262, “Application For Withholding Proprietary Information From Public Disclosure, WNA-AR-00189-WBT-P, Rev. 1, "Post Accident Monitoring System Reliability Analysis" (Proprietary)” dated October 7, 2011

Westinghouse

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-3526

CAW-11-3262

October 7, 2011

APPLICATION FOR WITHHOLDING PROPRIETARY INFORMATION FROM PUBLIC DISCLOSURE

Subject: WNA-AR-00189-WBT-P, Rev. 1, "Post Accident Monitoring System Reliability Analysis" (Proprietary)

The proprietary information for which withholding is being requested in the above-referenced report is further identified in Affidavit CAW-11-3262 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-11-3262, 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

J. A. Gresham, Manager
Regulatory Compliance

Enclosures

CAW-11-3262

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:

JAGresham

J. A. Gresham, Manager
Regulatory Compliance

Sworn to and subscribed before me
this 7th day of October 2011

Cynthia Olesky

Notary Public

COMMONWEALTH OF PENNSYLVANIA
Notarial Seal
Cynthia Olesky, Notary Public
Manor Boro, Westmoreland County
My Commission Expires July 16, 2014
Member, Pennsylvania Association of Notaries

(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 WNA-AR-00189-WBT-P, Rev. 1, "Post Accident Monitoring System Reliability Analysis" (Proprietary), dated October 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 (PAMS) 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 technical licensing information to the NRC that is required for approval of the Watts Bar Nuclear Unit 2 PAMS System.

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 licensing in-core instrumentation systems.

(b) Its use by a competitor would improve his competitive position in the development and licensing of a similar product.

(c) The information requested to be withheld reveals the distinguishing aspects of a design 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 WNA-AR-00189-WBT-P, Rev. 1, "Post Accident Monitoring System Reliability Analysis " (Proprietary)

2. __ copies of WNA-AR-00189-WBT-NP, Rev. 1, "Post Accident Monitoring System Reliability Analysis " (Non-Proprietary)

Also enclosed is the Westinghouse Application for Withholding Proprietary Information from Public Disclosure CAW-11-3262, 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-11-3262 and should be addressed to J. A. Gresham, Manager, Regulatory Compliance, Westinghouse Electric Company LLC, Suite 428, 1000 Westinghouse Drive, Cranberry Township, Pennsylvania 16066.