AP1000 DOCUMENT COVER SHEET

TDC: _____ Permanent File: _____

AP1000 DOCUMENT NO.	REVISION	PAGE	ASSIGNED TO	OPEN ITEMS (Y/N)
APP-GW-GSC-020-NP	0	1 of 43	W-MCGINNIS	

ALTERNATE DOCUMENT NUMBER: WCAP-16787-NP WORK BREAKDOWN #: GW

ORIGINATING ORGANIZATION: Westinghouse Electric Company, LLC

TITLE: **AP1000 Protection and Safety Monitoring System Technical Specification Completion Time and Surveillance Frequency Justification**

ATTACHMENTS:	DCP #/REV. INCORPORATED IN THIS DOCUMENT REVISION:
CALCULATION/ANALYSIS REFERENCE:	

ELECTRONIC FILENAME	ELECTRONIC FILE FORMAT	ELECTRONIC FILE DESCRIPTION
APP-GW-GSC-020-NP	PDF	See EDMS

☒ **© 2008 WESTINGHOUSE ELECTRIC COMPANY LLC – WESTINGHOUSE NON-PROPRIETARY CLASS 3**

See the Form 36.

LEGAL REVIEW	SIGNATURE / DATE **(If processing electronic approval select option)**
PATENT REVIEW	SIGNATURE / DATE

☐ **© 2008 WESTINGHOUSE ELECTRIC COMPANY LLC – WESTINGHOUSE PROPRIETARY CLASS 2**

This document is the property of and contains Proprietary Information owned by Westinghouse Electric Company LLC and/or its subcontractors and suppliers. It is transmitted to you in confidence and trust, and you agree to treat this document in strict accordance with the terms and conditions of the agreement under which it was provided to you.

☐ **© 2008 WESTINGHOUSE ELECTRIC COMPANY LLC and/or STONE & WEBSTER, INC. WESTINGHOUSE PROPRIETARY CLASS 2 and/or STONE & WEBSTER CONFIDENTIAL AND PROPRIETARY**

This document is the property of and contains Proprietary Information owned by Westinghouse Electric Company LLC and/or is the property of and contains Confidential and Proprietary Information owned by Stone & Webster, Inc. and/or their affiliates, subcontractors and suppliers. It is transmitted to you in confidence and trust, and you agree to treat this document in strict accordance with the terms and conditions of the agreement under which it was provided to you.

ORIGINATOR(S)	SIGNATURE / DATE **(If processing electronic approval select option)**
K.F. Muller C.W. Suggs	**Electronically Approved*** **
REVIEWER(S)	SIGNATURE / DATE
C.E. Morgan	**Electronically Approved*** **
	SIGNATURE / DATE
	SIGNATURE / DATE

VERIFIER(S)	SIGNATURE / DATE	Verification Method: Independent Review
J.G. Ewald	**Electronically Approved*** **	

__Plant Applicability__: ☒ All AP1000 plants except: No exceptions
☐ Only the following plants:

APPLICABILITY REVIEWER**	SIGNATURE / DATE
J. A. Speer	**Electronically Approved*** **
RESPONSIBLE MANAGER*	SIGNATURE / DATE
C.A. McGinnis	**Electronically Approved*** **

* Approval of the responsible manager signifies that the document and all required reviews are complete, the appropriate proprietary class has been assigned, electronic file has been provided to the EDMS, and the document is released for use.

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

Westinghouse Non-Proprietary Class 3

WCAP-16787-NP
APP-GW-GSC-020
Revision 0

February 2008

AP1000 Protection and Safety Monitoring System Technical Specification Completion Time and Surveillance Frequency Justification

Westinghouse

AP1000 DOCUMENT COVER SHEET

TDC: _____ Permanent File: _____

AP1000 DOCUMENT NO.	REVISION	PAGE	ASSIGNED TO	OPEN ITEMS (Y/N)
APP-GW-GSC-020-NP	0	1 of 43	W-MCGINNIS	

ALTERNATE DOCUMENT NUMBER: WCAP-16787-NP WORK BREAKDOWN #: GW

ORIGINATING ORGANIZATION: Westinghouse Electric Company, LLC

TITLE: **AP1000 Protection and Safety Monitoring System Technical Specification Completion Time and Surveillance Frequency Justification**

ATTACHMENTS:	DCP #/REV. INCORPORATED IN THIS DOCUMENT REVISION:
CALCULATION/ANALYSIS REFERENCE:	

ELECTRONIC FILENAME	ELECTRONIC FILE FORMAT	ELECTRONIC FILE DESCRIPTION
APP-GW-GSC-020-NP	PDF	See EDMS

☒ **© 2008 WESTINGHOUSE ELECTRIC COMPANY LLC – WESTINGHOUSE NON-PROPRIETARY CLASS 3**
See the Form 36.

LEGAL REVIEW	SIGNATURE / DATE (If processing electronic approval select option)
PATENT REVIEW	SIGNATURE / DATE

☐ **© 2008 WESTINGHOUSE ELECTRIC COMPANY LLC – WESTINGHOUSE PROPRIETARY CLASS 2**
This document is the property of and contains Proprietary Information owned by Westinghouse Electric Company LLC and/or its subcontractors and suppliers. It is transmitted to you in confidence and trust, and you agree to treat this document in strict accordance with the terms and conditions of the agreement under which it was provided to you.

☐ **© 2008 WESTINGHOUSE ELECTRIC COMPANY LLC and/or STONE & WEBSTER, INC.**
WESTINGHOUSE PROPRIETARY CLASS 2 and/or STONE & WEBSTER CONFIDENTIAL AND PROPRIETARY
This document is the property of and contains Proprietary Information owned by Westinghouse Electric Company LLC and/or is the property of and contains Confidential and Proprietary Information owned by Stone & Webster, Inc. and/or their affiliates, subcontractors and suppliers. It is transmitted to you in confidence and trust, and you agree to treat this document in strict accordance with the terms and conditions of the agreement under which it was provided to you.

ORIGINATOR(S)	SIGNATURE / DATE (If processing electronic approval select option)
K.F. Muller C.W. Suggs	**Electronically Approved*** **
REVIEWER(S) C.E. Morgan	SIGNATURE / DATE **Electronically Approved*** **
	SIGNATURE / DATE
	SIGNATURE / DATE
VERIFIER(S) J.G. Ewald	SIGNATURE / DATE **Electronically Approved*** ** — Verification Method: Independent Review

**Plant Applicability: ☒ All AP1000 plants except: No exceptions
☐ Only the following plants:

APPLICABILITY REVIEWER**	SIGNATURE / DATE
J. A. Speer	**Electronically Approved*** **
RESPONSIBLE MANAGER*	SIGNATURE / DATE
C.A. McGinnis	**Electronically Approved*** **

* Approval of the responsible manager signifies that the document and all required reviews are complete, the appropriate proprietary class has been assigned, electronic file has been provided to the EDMS, and the document is released for use.

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

WCAP-16787-NP
APP-GW-GSC-020
Revision 0

AP1000 Protection and Safety Monitoring System Technical Specification Completion Time and Surveillance Frequency Justification

K. F. Muller*
Regulatory Compliance & Plant Licensing

C. W. Suggs*
Safety System Functional Design

February 2008

Reviewer: C. E. Morgan*
Regulatory Compliance & Plant Licensing

Verifier: J. G. Ewald*
Nuclear Systems Engineering

Approved: C. A. McGinnis*, Manager
Nuclear Systems Engineering

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

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

© 2008 Westinghouse Electric Company LLC
All Rights Reserved

OPEN ITEMS

Item	Description	Status
1	The AP1000 Protection and Safety Monitoring System Software Requirements Specification document (Reference 15) is not available.	Open

TABLE OF CONTENTS

LIST OF TABLES iv

LIST OF ACRONYMS AND ABBREVIATIONS v

DEFINITIONS vii

1 INTRODUCTION 1-1
- 1.1 OVERVIEW 1-1
- 1.2 OBJECTIVE 1-1
- 1.3 SCOPE 1-2
- 1.4 BASIS 1-2

2 EQUIVALENT HARDWARE AND REDUNDANCY BETWEEN CONVENTIONAL WESTINGHOUSE PLANT PROTECTION SYSTEM AND AP1000 PMS 2-1

3 FAILURE DETECTABILITY 3-1
- 3.1 OVERVIEW 3-1
- 3.2 BASIS 3-1
- 3.3 ASSURANCE OF AVAILABILITY (FAILURE DETECTABILITY) 3-2
- 3.4 EVALUATION 3-2
  - 3.4.1 Potential Faults and Failures 3-2
  - 3.4.2 Default Failure States and Error Prevention Measures 3-4
  - 3.4.3 Evaluation 3-4
- 3.5 SUMMARY AND CONCLUSIONS 3-8

4 COMPLETION TIMES 4-1
- 4.1 EVALUATION OF COMPLETION TIMES 4-1
- 4.2 CONCLUSIONS 4-4

5 SURVEILLANCE TEST FREQUENCIES 5-1
- 5.1 PMS SCOPE 5-1
- 5.2 REACTOR TRIP CHANNEL OPERATIONAL TEST (RTCOT) 5-1
- 5.3 CHANNEL OPERATIONAL TEST (COT) 5-2
- 5.4 SURVEILLANCE FREQUENCY EVALUATION CONCLUSIONS 5-2

6 CONCLUSIONS 6-1

7 REFERENCES 7-1

APPENDIX A DIAGNOSTIC FAULT COVERAGE A-1

LIST OF TABLES

Table 2-1 Comparison of Conventional Westinghouse Plant Protection System and AP1000 PMS Hardware and Redundancy 2-1

Table 3-1 Failure Criticality Classes 3-3

Table 3-2 Failure Detectability Classes 3-3

Table 3-3 Channel Diagnostic Coverage 3-5

Table 3-4 ESF and RT Paths Diagnostic Coverage 3-7

Table 4-1 AP1000 Completion Times Requiring Justification 4-2

Table 5-1 Evaluation of Instrumentation Surveillance Frequencies 5-1

LIST OF ACRONYMS AND ABBREVIATIONS

A/D	analog to digital
AI	analog input
ALT	actuation logic test
BIOB	backplane input/output bus
BPL	bistable processor logic
CDF	core damage frequency
CDP	cyclic data package
CIM	component interface module
CONTRM	control module
COT	channel operational test
CPU	central processing unit
CRC	cyclic redundancy check
CS	communication section
CVCS	chemical and volume control system
DPM	dual dual-port memory
ESF	engineered safety features
ESFAS	engineered safety feature actuation system
FMEA	failure modes and effects analyses
FPROM	flash programmable read read-only memory
HSL	high high-speed datalink
HSLR	high-speed link receive
I&C	instrumentation and control
ILC	integrated logic cabinet
ILP	integrated logic processor
ITP	interface and test processor
LCL	local coincidence logic
LCO	limiting condition for operation
MCR	main control room
MTP	maintenance and test panel
MUX	multiplexer
NIS	nuclear instrumentation system
PAMS	post-accident monitoring system
PMS	protection and safety monitoring system
PRA	probabilistic risk assessment
PROM	programmable read read-only memory
PS	processing section
QICC	quad integrated communication controller
RAM	random access memory
RT	reactor trip
RTB	reactor trip breaker
RTC	real-time clock
RTC	real real-time clock
RTCOT	reactor trip channel operational test
RTD	resistance temperature detector

LIST OF ACRONYMS AND ABBREVIATIONS (cont.)

RTM	reactor trip relay matrix
RTS	reactor trip system
SDP	service data package
SR	source range
SSPS	solid state protection system
ST	shunt trip
STB	staggered test basis
TADOT	trip actuating device operational test
UART	universal asynchronous receiver-transmitter
UV	undervoltage
V&V	verification and validation

Advant® is a registered trademark of ABB Process Automation Corporation.

AP1000™ is a trademark of Westinghouse Electric Company LLC.

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

DEFINITIONS

Channel	An arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined.
Division	The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components.

1 INTRODUCTION

1.1 OVERVIEW

The Completion Times and Surveillance Frequencies specified in APP-GW-GL-700, "AP1000 Design Control Document," Chapter 16, Technical Specifications (Reference 1) are consistent with the times specified in NUREG-1431, "Standard Technical Specifications Westinghouse Plants" (Reference 2). However, NUREG-1431 LCO 3.3.1, Reactor Trip Instrumentation and LCO 3.3.2, ESFAS Instrumentation, Completion Times and Surveillance Frequencies, justified by WCAP-10271, "Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrumentation System" (Reference 3) are only applicable to the conventional Westinghouse Plant Protection System (i.e., 7100, 7300, Eagle-21, relay logic systems, and solid state protection systems {SSPS}). The WCAP-10271 set of relaxations was approved based on a core damage frequency (CDF) increase of substantially less than 6 percent (Reference 3). Some benefit was credited for reduction of spurious actuations associated with relaxations in the Surveillance Frequencies.

The instrumentation and control (I&C) system-related inputs to the WCAP-10271 analysis included the system redundancy and equipment reliability (including the influence of the source range {SR} frequency). As shown in Section 2, Equivalent Hardware and Redundancy, the AP1000™ protection and safety monitoring system (PMS) redundancy is as good as or better than that of the conventional Westinghouse Plant Protection System. Although the PMS equipment reliability is considered to be equivalent to or better than that of the conventional Westinghouse Plant Protection System, a common basis for comparison to the digital portion of the PMS is not readily available.

However, independent of the comparative reliability, the continuous availability of the PMS safety functions is ensured by the online diagnostics that detect and report PMS failures to the operator. As shown in Section 3, Failure Detectability, the ability of the diagnostics to detect failures is judged to be sufficient to ensure that the safety function availability is improved as compared to the conventional Westinghouse Plant Protection System, which is monitored only by periodic surveillance tests.

1.2 OBJECTIVE

This report provides a basis for the application of the WCAP-10271 (Reference 3) instrumentation technical specifications Completion Times and Channel Operational Test Surveillance Frequencies to the AP1000 PMS.

1.3 SCOPE

Completion Times

AP1000 LCO 3.3.1 and 3.3.2 requirements (Reference 1) specify Completion Times and Surveillance Frequencies that are justified by WCAP-10271 (Reference 3) in the Standard Technical Specifications, NUREG-1431 (Reference 2). This report provides a new basis for application of the Completion Times and Surveillance Frequencies for the following AP1000 Conditions and Surveillance Requirements:

LCO 3.3.1

Condition D

Condition E

Condition F

Condition K

Condition L

Condition N

Condition R

SR 3.3.1.6

LCO 3.3.2

Condition B

Condition C (Note 1)

Condition I

Condition J

SR 3.3.2.5

Note 1 - AP1000 Condition C is new and is not covered by the NUREG-1431 or WCAP-10231 Completion Time justification.

1.4 BASIS

The adequacy of the times documented in NUREG-1431 (Reference 2) has been demonstrated by operating experience and, in some cases, justified by probabilistic risk assessment (PRA) studies. These times have been applied to AP1000 based on equivalent hardware, system design, and service conditions.

The NUREG-1431 times apply directly to the portions of the AP1000 I&C that are equivalent to existing systems, including the sensors, transmitters, contact inputs (i.e., switches, breakers, relays), reactor trip breakers (RTBs), and power supplies. The NUREG-1431 times apply to these portions of the AP1000 I&C based on the equivalent redundancy and reliability.

The digital portions of the PMS are sufficiently different from the existing systems that redundancy and reliability cannot be assumed to be equivalent.

Software

[

]a,c

Completion Times

WCAP-10271 (Reference 3) analysis examines the core damage frequency (CDF) change due to increased Completion Times for Actions that require placing inoperable channels in trip or bypass. The availability of operable, redundant channels was the primary equipment-related consideration in the analysis. The availability was based on the redundancy, reliability, and periodic surveillance testing of the channels. Each channel covered by these Actions includes a sensor, signal conditioning circuitry, power supply, and bistable. The Actions require setting the inoperable channel output to the voting logic in trip or bypass.

[

]a,c

Surveillance Frequencies

The surveillance requirements establish the operability of systems and equipment at a frequency that balances the risks due to testing and the benefits of failure detection and corrective action. The reliability and failure modes are important considerations in establishing the Surveillance Frequency. The failure modes determine if failures are self-revealing. If all failures are self-revealing or detected and alarmed, then reliability is not a factor. [

]a,c

According to NUREG-1431 (Reference 2), the 92-day Channel Operational Test (COT) frequency is justified by WCAP-10271 (Reference 3). [ ]a,c

[

]a,c

2 EQUIVALENT HARDWARE AND REDUNDANCY BETWEEN CONVENTIONAL WESTINGHOUSE PLANT PROTECTION SYSTEM AND AP1000 PMS

Comparison of the conventional Westinghouse Plant Protection System (basis for WCAP-10271 {Reference 3} analysis) to the PMS (References 4, 6, and 14) shows which portions of the PMS hardware and system redundancy are equivalent or improved, as illustrated in Table 2-1. The Completion Times and Surveillance Frequencies of equivalent parts of the PMS remain applicable based on equivalent or improved reliability.

Table 2-1 Comparison of Conventional Westinghouse Plant Protection System and AP1000 PMS Hardware and Redundancy

a,c

Feature	Conventional Westinghouse Plant Protection System	AP1000 PMS	AP1000 Comparison

Table 2-1 (cont.) Comparison of Conventional Westinghouse Plant Protection System and AP1000 PMS Hardware and Redundancy

Feature	Conventional Westinghouse Plant Protection System	AP1000 PMS	AP-1000 Comparison

a,c

Redundancy

[

]a,c

Equivalent Hardware

The PMS is considered to be equivalent to the conventional Westinghouse Plant Protection System if the hardware is the same type or of similar design to that employed at current plants. Equipment that is equivalent is assumed to have equivalent performance and reliability, such that the NUREG-1431 (Reference 2) basis for the Surveillance Frequencies and Completion Times remains applicable.

Conclusion

Only the digital portions of the PMS, including the BPL subsystems, communication links, and LCL subsystems, apply different types of equipment than that used by the conventional Westinghouse Plant Protection System. The availability of this digital equipment based on failure detectability is addressed in Section 3.

3 FAILURE DETECTABILITY

3.1 OVERVIEW

Completion Times

The I&C technical specification Completion Times justified in NUREG-1431 (Reference 2) by WCAP-10271 (Reference 3), have been specified for the AP1000 PMS. The WCAP-10271 analysis credited the availability of redundant, operable channels during the Completion Time based on surveillance testing and the reliability of the equipment.

[ ]a,c These failure detection capabilities are detailed below and provide a basis for continued specification of the Completion Times, previously justified for the conventional Westinghouse Plant Protection System by WCAP-10271.

Surveillance Frequencies

The Channel Operational Test and Reactor Trip Channel Operational Test are required to be performed every 92 days by the AP1000 Technical Specifications, LCO 3.3.1 and LCO 3.3.2 (Reference 1). These surveillance tests cover the digital portions of the PMS. Justification of the Surveillance Frequency for these tests is addressed below and is based on maintaining an equivalent level of operability at the 92-day frequency. [ ]a,c

3.2 BASIS

Confirmation that the reliability of the AP1000 PMS is as good as or better than that of the conventional Westinghouse Plant Protection System could justify continued use of the Completion Times. Although the PMS is considered to be as reliable as the conventional Westinghouse Plant Protection System, there is no readily available reliability information for reliability comparison of the conventional Westinghouse Plant Protection System and PMS.

An alternate approach that replaces reliability with assurance of availability has been used to justify the applicability of the NUREG-1431 Completion Times and Surveillance Frequencies to the PMS. Reliability is a measure of the failure rate of the system that forecasts the likelihood that the safety functions will be available when required. [ ]a,c

3.3 ASSURANCE OF AVAILABILITY (FAILURE DETECTABILITY)

WCAP-16438-P, "FMEA of AP1000 Protection and Safety Monitoring System" (Reference 5) evaluated the means of detection and notification of each failure postulated by the failure modes and effects analyses (FMEA) of the RT and ESF functions. For each potential failure, the Reference 5 analysis identified the Technical Specification surveillance tests and/or diagnostics that would detect the failure. [

]a,c

3.4 EVALUATION

3.4.1 Potential Faults and Failures

The FMEA tables of Reference 5 list potential failures that were examined with respect to existing diagnostics in the PMS; and whether these existing diagnostics tests could detect the failures correctly and in a timely manner. [

]a,c

Once a fault is detected, it is presumed that the subsequent repair actions required can be completed to restore the availability of the particular component, module, or subsystem.

As described in Reference 5, the tables identify the component of the particular station or subsystem and their anticipated failure modes. For each failure mode, information is provided in columns with the following headings:

- Symptoms and Local Effects Including Dependent Failures
- Effects on the Protection Function
- Method of Detection
- Fault Classification

The fault classification consists of two parts: the failure criticality and its failure detectability. The first part of the classification is defined in Table 3-1.

Table 3-1 Failure Criticality Classes

Class	Meaning
I	Loss of capability to perform the safety function or spurious actuation of a safety function is a direct result of this failure.
II	The safety function can still be accomplished but at degraded performance (accuracy, time response, etc.).
III	Redundancy is reduced to the point that a further single failure will prevent actuation of the safety function or cause spurious actuation.
IV	The failure requires restorative maintenance but does not otherwise prevent the functioning of the system.

The second part of the classification identifies the detectability of the failure as provided in Table 3-2.

Table 3-2 Failure Detectability Classes

Class	Meaning
A	The failure is self-revealing through the consequent action of plant equipment (improper valve motion, erroneous or anomalous sensor indications, unexpected breaker trip, etc.).
B	The failure is detected by diagnostic features of the system.
C	The failure is revealed by planned surveillance testing performed at the specified test interval.
D	The failure is not revealed unless uncovered by an additional failure(s) or by intentional investigation beyond the scope of normal surveillance testing.

[

]a,c

[

]a,c

Review of the Reference 5 FMEA of the PMS shows that there are no postulated failures within the digital portions of the PMS that affect the safety function and can only be detected by surveillance testing. The potential failures affecting the safety function are revealed by diagnostics or are otherwise self-revealing.

The Software Hazard Analysis (Reference 13) shows that, once the PMS has passed the surveillance tests and startup diagnostics, potential errors occurring during operation that may affect the safety functions are self-revealing or are revealed by diagnostics.

3.4.2 Default Failure States and Error Prevention Measures

Quality processing is described in Paragraph A.11 of Appendix A. Upon assignment of a BAD data quality by the quality processing diagnostics, predefined, default states are automatically assigned to ensure that appropriate logic is implemented to preserve availability of protective actions and to avoid spurious actuations.

An error-prevention measure is a positive action taken to prevent future errors or failures. [

]a,c

3.4.3 Evaluation

3.4.3.1 Channel Operability

Channel operability refers to the health of the PMS from the analog sensor and digital inputs to the bistable processor logic (BPL) process station to the inputs to the LCL process station. The surveillance tests applicable to the channel are the channel calibration and the COT, which ends at the LCL inputs. The main purpose of the COT is to verify correct bistable logic operation and the correctness of setpoints. Additionally, the RTCOT includes the BPL for the reactor trip functions.

[

]a,c

[

]a,c

Table 3-3 Channel Diagnostic Coverage

Signal Path System Element	Diagnostic Coverage (Appendix A Paragraph Reference)

a,c

[

]a,c

[

]a,c

3.4.3.2 Surveillance Test Paths

[

]a,c

[

]a,c

Table 3-4 ESF and RT Paths Diagnostic Coverage

Signal Path System Element	Diagnostic Coverage (Appendix A Paragraph Reference)

a,c

The table shows that all paths and elements are covered by a diagnostic and, in most cases, by more than one or by overlapping diagnostics. In addition, as detailed in subsection 3.4.3.1, the availability of the elements corresponding to the paths in Tables 3-3 and 3-4 is verified automatically and continually.

[

]a,c The advantage is based on the fact that most equipment and components have a constant or nearly constant failure rate during their useful lives. [

]a,c

3.5 SUMMARY AND CONCLUSIONS

[

]a,c

The periodic performance of the surveillance tests remains a useful independent check of the system and verifies the viability of the diagnostics by confirming that no undetected failures exist.

NUREG-1431 Completion Times and Surveillance Frequencies

The continued applicability of the NUREG-1431 (Reference 2) Completion Times previously justified by WCAP-10271 (Reference 3) to the AP1000 PMS is justified by the failure detectability of the digital portions of the PMS as established by the AP1000 PMS FMEA (Reference 5) and discussed in Sections 3.1 to 3.4, above.

[

]a,c

4 COMPLETION TIMES

4.1 EVALUATION OF COMPLETION TIMES

The Completion Times specified by the AP1000 instrumentation technical specifications Actions (Reference 1) limit the time allowed to restore compliance with the limiting condition for operation (LCO), perform compensatory actions, or establish conditions for which the inoperable equipment is not required. In general, if the safety function is maintained by the remaining operable channels, a period of time that is normally sufficient to restore inoperable equipment is provided to avoid the risk associated with plant mode changes.

The NUREG-1431 (Reference 2) instrumentation Completion Times specified are based on the reliability and redundancy of the equipment (e.g., conventional Westinghouse Plant Protection System) as well as other factors that are unrelated to the installed equipment, such as alternative safety function means, operating experience, low probability of an event, and time needed to complete Actions. Completion Times specified in NUREG-1431 that are justified by the WCAP-10271 (Reference 3) analysis are independently justified for the PMS, since the analysis is specific to the conventional Westinghouse Plant Protection System.

The Completion Times justified by the WCAP-10271 analysis can be applied to the PMS, if the availability of the operable redundant channels is as good as or better than that of the conventional Westinghouse Plant Protection System. [

]a,c

The PMS Actions that specify Completion Times previously justified by WCAP-10271 are listed in Table 4-1. Table 4-1 includes the following columns:

1. LCO, Condition

   The conditions that apply to inoperable channels are included. The PMS channels include the equipment from the sensor to the high-speed link input to the LCL.

   The condition inoperability is listed. [

   ]a,c

2. Required Action

   These Actions specify channel restoration or placing a channel in trip or bypass.

3. Completion Time

The NUREG-1431 (Reference 2) Completion Times justified by WCAP-10271 (Reference 3) that have been specified for AP1000 are listed.

4. Logic

Normal The **normal** logic, without any inoperable channels is listed. (2-out-of-4 logic is specified as 2/4.)

Before The degraded logic, **before** any corrective action, is listed. This logic indicates the status of the safety function availability and compliance with the single failure criterion. Most of the conditions specify "one or two channels inoperable." In these cases, the "Before" and "After" logic for two inoperable channels is listed.

After The logic **after** completion of the Action (place channels in trip or bypass, or restore channel) is listed.

Table 4-1 AP1000 Completion Times Requiring Justification

Condition	Required Action	Completion Time	Logic	Notes

a,c

Table 4-1 (cont.) AP1000 Completion Times Requiring Justification

Condition	Required Action	Completion Time	Logic	Notes

a,c

Table 4-1 (cont.) AP1000 Completion Times Requiring Justification

Condition	Required Action	Completion Time	Logic	Notes

a,c

Summary

The reactor trip and engineered safety feature actuation system (ESFAS) instrumentation conditions applicable to inoperable channels specify Completion Times depending on the case. The time is based on the availability of the safety function from the remaining channels and applicable modes (probability of an event). The specified times provide a reasonable time to complete the required Actions. [

]a,c

4.2 CONCLUSIONS

The AP1000 reactor trip and ESFAS instrumentation Completion Times, previously justified by WCAP-10271 (Reference 3) in NUREG-1431 (Reference 2), are acceptable based on assurance of channel availability that is as good as or better than that credited for the conventional Westinghouse Plant Protection System. The availability of the non-digital portions of the PMS channels is equivalent to that of the conventional Westinghouse Plant Protection System based on equivalent equipment reliability,

redundancy, and Surveillance Frequency as discussed in Section 2. The availability of the digital portion of the PMS channels is as good as or better than that of the conventional Westinghouse Plant Protection System based on failure detectability as discussed in Section 3.

5 SURVEILLANCE TEST FREQUENCIES

5.1 PMS SCOPE

Justification of the 92-day Surveillance Frequency specified for AP1000 surveillances SR 3.3.1.6 and SR 3.3.2.5 is required, since the digital portions of the PMS are different from the conventional Westinghouse Plant Protection System and cannot be justified by WCAP-10271 (Reference 3) as in NUREG-1431 (Reference 2). The WCAP-10271 basis for the frequency of these surveillances is the system reliability and redundancy, since only a few of the possible failures that might occur between surveillances are immediately self-revealing.

The RT Channel Operational Test (SR 3.3.1.6) verifies the operability of the RT instrumentation [ ]^{a,c} to the voting logic outputs (LCL subsystem) and is equivalent to the combined COT and Actuation Logic Test surveillances specified in NUREG-1431 for the RT instrumentation, LCO 3.3.1.

The Channel Operational Test (SR 3.3.2.5) verifies the operability of the ESF instrumentation [ ]^{a,c} and is equivalent to the COT surveillance specified in NUREG-1431 for the ESFAS instrumentation, LCO 3.3.2, as shown in Table 5-1.

Table 5-1 Evaluation of Instrumentation Surveillance Frequencies

AP1000	AP1000 Frequency/Basis	Corresponding NUREG-1431	NUREG-1431 Frequency/ Basis
SR 3.3.1.6 RTCOT	92 days Redundancy, failure detectability, reliability, etc.	SR 3.3.1.5 Actuation Logic Test	31 days on an STB Operating experience
		SR 3.3.1.6 COT	92 days WCAP-10271
SR 3.3.2.5 COT	92 days Redundancy, failure detectability, reliability, etc.	SR 3.3.2.5 COT	92 days WCAP-10271

5.2 REACTOR TRIP CHANNEL OPERATIONAL TEST (RTCOT)

The RT Channel Operational Test (SR 3.3.1.6) requires injection of sensor test signals and verification of the generation, at the proper setpoints, of RT and interlock signals at a frequency of 92 days. This frequency is consistent with the corresponding NUREG-1431 (Reference 2) RT COT and ALT frequencies, which are justified by WCAP-10271 (Reference 3).

The portions of the PMS that employ digital technology covered by this surveillance include the signal path from the BPL subsystem input termination units to the LCL subsystem outputs. As justified in

Section 3, continuous failure detectability for the signal path provides real-time assurance that these portions of the signal path are operable.

[

]a,c

The PMS failure detectability for the digital portions of the system, along with the equivalent hardware and redundancy for the non-digital portions of the system, and elimination of bistable drift, justify the SR 3.3.1.6, RTCOT, frequency of 92 days for the applicable RTS instrumentation PMS (Reference 1) channels.

5.3 CHANNEL OPERATIONAL TEST (COT)

The Channel Operational Test (SR 3.3.2.5) requires injection of a sensor test signal and verification of the generation of alarms, interlock signals, and actuation signals at the proper setpoints at a frequency of 92 days. This frequency is consistent with the corresponding NUREG-1431 (Reference 2) ESFAS COT frequency of 92 days, which is justified in WCAP-10271 (Reference 3).

The portions of the PMS that employ digital technology covered by this surveillance [ ]a,c. As justified in Section 3, continuous failure detectability for the signal path provides real-time assurance that these portions of the signal path are operable. [

]a,c

The PMS failure detectability for the digital portions of the system, along with equivalent hardware and redundancy for the non-digital portions of the system, and elimination of bistable drift justify the SR 3.3.2.5, COT frequency of 92 days for the applicable ESFAS instrumentation PMS (Reference 1) channels.

5.4 SURVEILLANCE FREQUENCY EVALUATION CONCLUSIONS

In the PMS, the equipment covered by the RT Channel Operational Test and the Channel Operational Test is primarily digital and is redundant within each division. In the conventional Westinghouse Plant Protection System, the equipment was neither digital nor redundant. The previous basis for the frequency of these surveillances was the system reliability (e.g., conventional Westinghouse Plant Protection System), since only a few self-revealing failures were detectable. The PMS failure tolerance (redundancy) and automatic failure detectability of the digital equipment provide a basis for continued application of the NUREG-1431 Surveillance Frequency for these tests. Periodic performance of the surveillances provides a functional test of the operability and verifies that the diagnostics are performing correctly.

6 CONCLUSIONS

The RT and ESF Instrumentation 92-day RTCOT and COT Surveillance Frequencies and Completion Times are justified based on the equivalent non-digital hardware and redundancy, and on continuous diagnostic test features, default failure states, and the self-revealing failure capabilities of the PMS, which provide an assurance of Technical Specification safety function availability that is as good as or better than that of the conventional Westinghouse Plant Protection System.

7 REFERENCES

Following is a list of references used throughout this document.

1. APP-GW-GL-700 (Proprietary), Rev. 16, Chapter 16, "AP1000 Design Control Document," Westinghouse Electric Company LLC.

2. NUREG-1431, Rev. 2, "Standard Technical Specifications Westinghouse Plants Specifications," April 2001.

3. WCAP-10271-P-A (Proprietary), "Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrumentation System," Westinghouse Electric Company LLC.

4. APP-GW-GLR-071, Rev. 0 (Proprietary), "AP1000 Protection and Safety Monitoring System Architecture Technical Report," Westinghouse Electric Company LLC.

5. APP-GE-JJ-002, Rev. 1 (Proprietary), "FMEA OF AP1000 Protection and Safety Monitoring System," Westinghouse Electric Company LLC.

6. APP-PMS-J4-020, Rev. A (Proprietary), "AP1000 System Design Specification for the Protection and Safety Monitoring System," Westinghouse Electric Company LLC.

7. Shooman, Martin L., "Probabilistic Reliability: An Engineering Approach," Second Edition, Krieger Publishing Company, Melbourne, FL, 1990.

8. APP-GW-J4-001, Rev. A (Proprietary), "AP1000 I&C System Design Specification," Westinghouse Electric Company LLC.

9. WCAP-16097-P-A, Rev. 0 (Proprietary), "Common Qualified Platform Topical Report," Westinghouse Electric Company LLC.

10. WCAP-16096-NP-A, Rev. 1A (Non-Proprietary), "Software Program Manual for Common Q Systems," Westinghouse Electric Company LLC.

11. 00000-ICE-3889, Rev. 8 (Proprietary) "Coding Standards and Guidelines for Common Q Systems," Westinghouse Electric Company LLC.

12. WNA-DS-00315-GEN, Rev. 2 (Proprietary), "Reusable Software Element Document – CRC for Calibration Data," Westinghouse Electric Company LLC.

13. APP-PMS-GER-001, Rev. 0 (Proprietary), "Software Hazard Analysis of AP1000 Protection and Safety Monitoring System," Westinghouse Electric Company LLC.

14. APP-PMS-J1-001, Rev. C (Proprietary), "AP1000 Protection and Safety Monitoring System Functional Requirements," Westinghouse Electric Company LLC.

15. (APP-PMS-J4-TBD) (Proprietary), "AP1000 Software Requirements Specification for the Protection and Safety Monitoring System," Westinghouse Electric Company LLC.

APPENDIX A
DIAGNOSTIC FAULT COVERAGE

a,c

a,c

a,c

a,c

a,c

a,c

a,c

a,c

a,c

a,c

a,c