



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

U.S. Nuclear Regulatory Commission
 ATTENTION: Document Control Desk
 Washington, D.C. 20555

Direct tel: 412-374-6206
 Direct fax: 724-940-8505
 e-mail: sisk1rb@westinghouse.com

Your ref: Docket No. 52-006
 Our ref: DCP_NRC_002927

June 22, 2010

Subject: Submittal of Chapter 7 Documents

Westinghouse is submitting responses to the NRC request for additional information (RAI) on SRP Section 7 and two additional reports. These RAI responses are submitted in support of the AP1000 Design Certification Amendment Application (Docket No. 52-006). The information included in the response is generic and is expected to apply to all COL applications referencing the AP1000 Design Certification and the AP1000 Design Certification Amendment Application.

Enclosure 3 (Proprietary) and 4 (Non-Proprietary) provides the following responses:

OI-SRP7.1-ICE-03-R1	NP
OI-SRP7.2-ICE-02-R1	NP
RAI-SRP7.0-ICE-05 R1	P & NP
RAI-SRP7.0-ICE-11 R1	NP
RAI-SRP7.0-ICE-13 R1	P & NP
RAI-SRP7.0-ICE-14 R1	NP
RAI-SRP7.0-ICE-15	NP
RAI-SRP7.1-SHA-01	NP
RAI-SRP7.8-DAS-05	P & NP
RAI-SRP7.8-DAS-06	NP
RAI-SRP7.8-DAS-07	NP
RAI-SRP7.8-DAS-08	NP
RAI-SRP7.8-DAS-09	NP

RAI-SRP7.8-DAS-10	NP
RAI-SRP7.8-DAS-11	NP
RAI-SRP7.8-DAS-12	NP
RAI-SRP7.8-DAS-13	NP
RAI-SRP7.1-FMEA-06	P & NP
APP-GW-GLR-143 (WCAP-17179) R2 (CIM TR)	P draft
APP-GW-GLR-145 (WCAP-17184) (DAS TR)	P draft
APP-GW-J0R-012	P

Pursuant to 10 CFR 50.30(b), proprietary and non-proprietary versions of the response to the request for additional information on SRP Section 7 are submitted as Enclosures 3 and 4. Also enclosed is one copy of the Application for Withholding, AW-10-2862 (non-proprietary) with Proprietary Information Notice, and one copy of the associated Affidavit (non-proprietary).

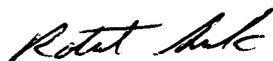
This submittal contains proprietary information of Westinghouse Electric Company, LLC. In conformance with the requirements of 10 CFR Section 2.390, as amended, of the Commission's regulations, we are enclosing with this submittal an Application for Withholding from Public Disclosure and an affidavit. The affidavit sets forth the basis on which the information identified as proprietary may be withheld from public disclosure by the Commission.

DO63
 NRC
 6/22/2010 5:35 PM

Correspondence with respect to the affidavit or Application for Withholding should reference AW-10-2862 and should be addressed to James A. Gresham, Manager, Regulatory Compliance and Plant Licensing, Westinghouse Electric Company, LLC, P. O. Box 355, Pittsburgh, Pennsylvania 15230-0355.

Questions or requests for additional information related to the content and preparation of this response should be directed to Westinghouse. Please send copies of such questions or requests to the prospective applicants for combined licenses referencing the AP1000 Design Certification. A representative for each applicant is included on the cc: list of this letter.

Very truly yours,



Robert Sisk, Manager
Licensing and Customer Interface
Regulatory Affairs and Strategy

/Enclosures

1. AW-10-2862 "Application for Withholding Proprietary Information from Disclosure," dated June 22, 2010
2. AW-10-2862, Affidavit, Proprietary Information Notice, Copyright Notice dated June 22, 2010
3. Chapter 7 Documents (Proprietary)
4. Chapter 7 Documents (Non-Proprietary)

cc:	D. Jaffe	- U.S. NRC	4E
	E. McKenna	- U.S. NRC	4E
	S. K. Mitra	- U.S. NRC	4E
	T. Spink	- TVA	4E
	P. Hastings	- Duke Power	4E
	R. Kitchen	- Progress Energy	4E
	A. Monroe	- SCANA	4E
	P. Jacobs	- Florida Power & Light	4E
	C. Pierce	- Southern Company	4E
	E. Schmiech	- Westinghouse	4E
	G. Zinke	- NuStart/Entergy	4E
	R. Grumbir	- NuStart	4E
	B. Seelman	- Westinghouse	4E

ENCLOSURE 1

AW-10-2862

APPLICATION FOR WITHHOLDING
PROPRIETARY INFORMATION FROM DISCLOSURE



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

U.S. Nuclear Regulatory Commission
ATTENTION: Document Control Desk
Washington, D.C. 20555

Direct tel: 412-374-6206
Direct fax: 412-374-5005
e-mail: sisk1rb@westinghouse.com

Your ref: Docket Number 52-006
Our ref: AW-10-2862

June 22, 2010

APPLICATION FOR WITHHOLDING PROPRIETARY
INFORMATION FROM PUBLIC DISCLOSURE

Subject: Submittal of Chapter 7 Documents

The Application for Withholding is submitted by Westinghouse Electric Company, LLC (Westinghouse), pursuant to the provisions of Paragraph (b) (1) of Section 2.390 of the Commission's regulations. It contains commercial strategic information proprietary to Westinghouse and customarily held in confidence.

The proprietary material for which withholding is being requested is identified in the proprietary versions of the listed documents. In conformance with 10 CFR Section 2.390, Affidavit AW-10-2862 accompanies this Application for Withholding, setting forth the basis on which the identified proprietary information may be withheld from public disclosure.

Accordingly, it is respectfully requested that the subject 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 this Application for Withholding or the accompanying affidavit should reference AW-10-2862 and should be addressed to James A. Gresham, Manager, Regulatory Compliance and Plant Licensing, Westinghouse Electric Company, LLC, P.O. Box 355, Pittsburgh, Pennsylvania, 15230-0355.

Very truly yours,

A handwritten signature in black ink, appearing to read "Robert Sisk".

Robert Sisk, Manager
Licensing and Customer Interface
Regulatory Affairs and Strategy

ENCLOSURE 2

Affidavit

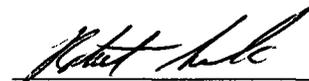
AFFIDAVIT

COMMONWEALTH OF PENNSYLVANIA:

SS

COUNTY OF BUTLER:

Before me, the undersigned authority, personally appeared Robert Sisk, 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:



Robert Sisk, Manager
Licensing and Customer Interface
Regulatory Affairs and Strategy

Sworn to and subscribed
before me this 22nd day
of June 2010.

COMMONWEALTH OF PENNSYLVANIA
Notarial Seal
Linda J. Bugle, Notary Public
City of Pittsburgh, Allegheny County
My Commission Expires June 18, 2013
Member, Pennsylvania Association of Notaries



Notary Public

- (1) I am Manager, Regulatory Affairs and Strategy, 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" 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 Submittal of Chapter 7 Documents, in support of the AP1000 Design Certification Amendment Application, being transmitted by Westinghouse letter (DCP_NRC_002927) and Application for Withholding Proprietary Information from Public Disclosure, to the Document Control Desk. The proprietary information as submitted by Westinghouse for the AP1000 Design Certification Amendment application is expected to be applicable in all licensee submittals referencing the AP1000 Design Certification and the AP1000 Design Certification Amendment Application in response to certain NRC requirements for justification of compliance of the safety system to regulations.

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

- (a) Manufacture and deliver products to utilities based on proprietary designs.

- (b) Advance the AP1000 Design and reduce the licensing risk for the application of the AP1000 Design Certification
- (c) Determine compliance with regulations and standards
- (d) Establish design requirements and specifications for the system.

Further this information has substantial commercial value as follows:

- (a) Westinghouse plans to sell the use of similar information to its customers for purposes of plant construction and operation.
- (b) Westinghouse can sell support and defense of safety systems based on the technology in the reports.
- (c) The information requested to be withheld reveals the distinguishing aspects of an approach and schedule 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 digital technology safety systems and licensing defense services for commercial power reactors without commensurate expenses. Also, public disclosure of the information would enable others to use the information to meet NRC requirements for licensing documentation without purchasing the right to use the information.

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

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

Further the deponent sayeth not.

PROPRIETARY INFORMATION NOTICE

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

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

COPYRIGHT NOTICE

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

ENCLOSURE 4

Response to Request for Additional Information on SRP Section 7

(Non-Proprietary)

OI-SRP7.1-ICE-03-R1	NP
OI-SRP7.2-ICE-02-R1	NP
RAI-SRP7.1-SHA-01	NP
RAI-SRP7.0-ICE-05 R1	NP
RAI-SRP7.0-ICE-11 R1	NP
RAI-SRP7.0-ICE-13 R1	NP
RAI-SRP7.0-ICE-14 R1	NP
RAI-SRP7.0-ICE-15	NP
RAI-SRP7.8-DAS-05	NP
RAI-SRP7.8-DAS-06	NP
RAI-SRP7.8-DAS-07	NP
RAI-SRP7.8-DAS-08	NP
RAI-SRP7.8-DAS-09	NP
RAI-SRP7.8-DAS-10	NP
RAI-SRP7.8-DAS-11	NP
RAI-SRP7.8-DAS-12	NP
RAI-SRP7.8-DAS-13	NP
RAI-SRP7.1-FMEA-06	NP

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: OI-SRP7.1-ICE-03 R1 (RAI-SRP7.1-ICE-12) (OI-SRP-7.1-01)
Revision: 1

Question:

For material associated with the AP1000 Design Certification Amendment, provide a consistent reference of standards and other guidance throughout all docketed and referenced technical documents.

Upon review of various technical reports, several references cited were from different revisions of the same accepted industry standard. For example Technical Report 89 (WCAP 16675-P) references IEEE 7-4.3.2-2003 while Technical Report 42 (APP-GW-GLR-017) references the 1993 version of the standard

Westinghouse Response:

DCD Rev 17, Tier 2, Table 19.59-18 (Sheet 7 of 25), states that the PMS software is designed, tested, and maintained to be reliable under a controlled verification and validation program written in accordance with IEEE 7-4.3.2 (1993) that has been endorsed by Regulatory Guide 1.152, Rev. 1.

In addition, Tier 2, Appendix 1A under Reg. Guide 1.152, Rev.1 – Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants, states that the AP1000 conforms to ANSI/IEEE-ANS-7-4.3.2-1993.

Westinghouse standard practices allow for use of later versions of standards as long as they "envelope" the standard called out in the DCD. In this case, the standard called out in the DCD is IEEE 7-4.3.2 (1993). As stated in the above question, Technical Report 89 (WCAP 16675-P) references IEEE 7-4.3.2-2003, which envelopes 1993. The enveloping of the 1993 version of the standard does not modify the DCD Revision 17 commitment.

As a supplement to the above Westinghouse response, this subject was discussed during the October 15th and 16th 2008 I&C Technical Review Meetings between Westinghouse and the NRC. The following actions related to this RAI resulted from that meeting:

1. The NRC will communicate guidance for license basis consistency and advise WEC.
2. By 11/15/2008, WEC will review all Chapter 7 PMS related docketed documents for consistency with the DCD regulatory basis.

Question OI-SRP-7.1-01:

7.1.3.2 Compliance with Industry Standards

WEC submitted a number of technical reports (TRs) associated with I&C systems that it incorporated by reference into the AP1000 DCD. In several cases, WEC referenced industry standards and other regulations to different revisions of the same document. For example, TR WCAP 16675-P (APP-GW-GLR-071), "AP1000 Protection and Safety Monitoring System Architecture Report," Revision 2, references the Institute of Electrical and Electronics Engineers

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

(IEEE) Standard (Std.) 7-4.3.2-2003, while TR APP-GW-GLR-017, "Resolution of Common Q NRC Items for AP1000," Revision 0, references the 1993 version of the IEEE standard. The NRC originally addressed this issue under RAI-SRP-7.1-ICE-12. Although WEC committed to reference all newly created or revised technical documents to current guidance or industry standards, the NRC discovered different versions of a given standard in several newly submitted reports. **The NRC staff identified this as OI-7.1-01.**

Westinghouse Response:

The industry standards referenced in Westinghouse documents, including the Chapter 7 docketed documents, support the AP1000 certified design and are consistent with the DCD regulatory basis. Westinghouse standard practices, including newly created or revised technical documents, allow for use of later versions of industry standards as long as they "envelope" the standard called out in the DCD. In cases where the design has changed, WEC will work with the Staff, on a case by case basis, to address questions on versions of reference documents.

NRC Comment from 6/15/10 Meeting:

Westinghouse submitted a response to OI-SRP-7.1-ICE-01 in January 2010. In the response Westinghouse discussed the removal of some, but not all of the references within Section 7.1.7 – References. As such, the staff was unable to determine the acceptability of all the reference removals. WEC must state the reason for the reference changes. All of the technical reports issued to the NRC should be scrubbed and the Cyber Security reference should be removed. Also, the IIS WCAP is to be added as a reference to DCD Chapter 7.

Westinghouse Response to Revision 1:

Of particular interest to the staff are the following issues:

A. The reasoning behind Westinghouse's removal of the following References:

3. WCAP 13383, Revision 1 (Non Proprietary), "AP600 Instrumentation and Control Hardware and Software Design, Verification and Validation Process Report," June 1996

The staff's concern deals with the fact that the above reference is a Tier 2* document, listed in the Tier 2* table of the DCD Introduction and no information was offered by the applicant detailing why it is appropriate to remove the reference. The staff requests Westinghouse explain why the reference is no longer valid.

This reference was applicable to the Eagle 21 platform but not the Common Q platform. The appropriated process documents for the Common Q Platform are the Common Q Software Program Manual (WCAP-16096-NP-A) and the Design Process for AP1000 Common Q Systems (WCAP-15927).

10. WCAP 15927, Revision 0, "Design Process for AP1000 Common Q Safety Systems," August 2002.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

The staff's concern is based upon this document also being a Tier 2* document and its removal also requires prior NRC approval. Further, as this document now resides at Revision 2 on the docket, the staff's expectation would be to restore the reference within Section 7.1.7 of the AP1000 DCD and the Tier 2* tables or offer a satisfactory explanation revealing why the document's removal from Section 7.1.7 is justified.

The DCD will be revised as follows:

Table 1.6-1 (Sheet 12 of 20)

Replace NABU-DP-00014-GEN (P) Design Process for Common Q Safety Systems, Revision 1, March 2006 **with** [WCAP-15927 (NP) Design Process for AP1000 Common Q Safety Systems, Revision 2, November 2008]*

Replace the last paragraph in Section 7.1.2.14.1 Design Process which reads, “[WCAP-16096-NP-A (Reference 9) and the NRC-approved Westinghouse Quality Management System (Reference 21) describe design processes that will be used for AP1000.]* NABU-DP-00014-GEN (Reference 20) provides lower-level process implementation details.” **with** “[WCAP-16096-NP-A (Reference 9), WCAP-15927, and the NRC-approved Westinghouse Quality Management System (Reference 21) describe design processes that will be used for AP1000.]*”

Replace reference 20 on page 7.1-15, ‘NABU-DP-00014-GEN, Revision 1 (Proprietary), ‘Design Process for Common Q Safety Systems,’ March 2006.’ **with** ‘[WCAP-15927, Revision 2 (Non-proprietary), ‘Design Process for AP1000 Common Q Safety Systems,’ November 2008.]*’

15. IEEE 7-4.3.2 1993, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.”

The staff fails to understand why a recognized reference for the use of digital systems would be removed from a high level licensing document. Although an incorporate by reference technical report may also utilize the reference, the staff concluded the removal of the IEEE Standard from the References section is not justified.

WEC will reinstate IEEE 7-4.3.2 1993 in the references.

17. WCAP 16361-P (Proprietary) and WCAP 16361-NP (Non-Proprietary), “Westinghouse Setpoint Methodology for Protection Systems – AP1000,” May 2006.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

The staff fails to understand why this reference would not be utilized as the primary Tier 2* document as it relates to the selection of AP1000 safety-related I&C system setpoints. The staff recommends Westinghouse evaluate the potential for including the AP1000 Setpoint Methodology as a Tier 2* document.

This issue was discussed at the June 2010 Chapter Closeout Meeting between Westinghouse and the USNRC. The USNRC took an action to check with the Tech Spec Branch. If the NRC already reviews all changes to the Tech Specs, there would be no need to classify this WCAP a Tier 2*.

22. APP-GW-GLR-104, "AP1000 Cyber Security Implementation," Westinghouse Electric Company LLC

The staff's position related to Cyber Security issues reveals that cyber security is not a 10 CFR Part 50 review item. As such, the reference to APP-GW-GLR-104, should be removed and replaced with a docketed report describing the secure development and operational environment in which Westinghouse chooses to develop its software-based and programmable technology based devices, paying particular attention to IEEE 603 – 1991 Clauses 5.3, Quality; 5.6.3, Independence; and 5.9 Access Control.

The following portions of Section 7.1.1 will be deleted:

7.1.1 The AP1000 Instrumentation and Control Architecture

Figure 7.1-1 illustrates the instrumentation and control architecture for the AP1000. The figure shows two major sections separated by the real-time data network. Figure 7.1-1 depicts the real-time data highway as a single network. ~~To meet cyber security concerns, the real-time data highway will be separated into security levels as described in Reference 22.~~

Cyber Security

~~Reference 22 describes the cyber security implementation for AP1000.~~

The following statement will be added to Section 7.1.2.14.1, Design Process:

Reference 22 describes the process for ensuring that the design life cycle process for the Protection and Safety Monitoring System meets the computer security requirements of IEEE 603 and Regulatory Guide 1.152.

The following portion of Section 7.1.7 will be changed:

7.1.7 References

22. APP-GW-~~GLRJ0R-104012~~, "AP1000 ~~Cyber Security Implementation~~Protection and Safety Monitoring System Computer Security Plan," Westinghouse Electric Company LLC.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

B. The staff concludes that with the addition of newly created or modified technical reports, Westinghouse should determine which reports should be added to Section 7.1.7 – References within Chapter 7 of the AP1000 DCD. Westinghouse should also identify how these documents, and the ones previously listed in the References Section of 7.1.7, will be incorporated by reference into the AP1000 DCD to be included as part of the licensing basis.

Examples include:

- APP-GW-GLR-065 / WCAP 16674-P, “I&C Data Communication and Manual Control of Safety Systems and Components, “ Revision 2

“This document will be cited as follows in the DCD:

“7.1.2.8 Communication Functions

~~Reference 19, Section 3~~ Reference Y describes the communication functions.”

Reference Y will be WCAP-16674-P and the reference number will be defined in Section 7.1.7 at the time the DCD is revised.

- APP-GW-GLR-143 / WCAP 17179-P, “AP1000 Component Interface Module Technical Report,” Revision 0

This document will be included in the next rev. of the DCD as follows:

“7.1.2.1 Plant Protection Subsystems

Reference 19, Section 2.2 describes the plant protection subsystems. Reference X describes the component interface module subsystem. Reference Y describes the interfaces of the plant protection system.”

Reference X will be WCAP-17179-P and the reference number will be defined in Section 7.1.7 at the time the DCD is revised.

- APP-GW-JJ-002 / WCAP 16438-P, “FMEA of AP1000 Protection and Safety Monitoring System,” Revision 2
 - See section 7.2.3 and 7.2.4 for the reference to the FMEA in the DCD.
- APP-PMS-GER-001 / WCAP 16592-P, “Software Hazard Analysis of AP1000 Protection and Safety Monitoring System, Revision 1
 - See section 7.2.3 and 7.2.4 for the reference to the SHA in the DCD.
- APP-GW-GLR-148 / WCAP 17201-P, “AC160 High Speed Link Communication Compliance to DI&C-ISG-04 Staff Positions 9, 12, 13 and 15 Technical Report”

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Westinghouse indicated in its response to RAI-SRP7.1-ICE-10, how the DCD will reference this new technical report:

“DCD Chapter 7 for the AP1000 has been written to describe the protection system hardware utilizing the Common Qualified Platform (Common Q) described in Reference 8 (which includes the NRC SER), and augmented by Reference X.”

Reference X will be WCAP-17201-P and the reference number will be defined in Section 7.1.7 at the time the DCD is revised

- Whatever report replaces the cyber security (APP-GW-J0H-001) report.
This is addressed in a separate document; the draft was submitted via email to the NRC for review on 6/10/10.

IEEE Std. 603–1991 requires among other things that, safety systems within nuclear power plants be designed and constructed with sufficient Quality, Clause 5.3; and Reliability, Clause 5.15. Westinghouse also committed to following the guidance within Branch Technical Position BTP) 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,” of NUREG – 0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: Light Water Reactor Edition,” (SRP). Within the “Acceptance Criteria for Planning,” in Section B.3.1 of BTP 7-14, it relates the applicant should address traceability such that all plans and references utilized are traceable back to recognized and accepted and endorsed industry standards. Westinghouse must demonstrate how they adequately address the traceability criterion within BTP 7-14.

Design Control Document (DCD) Revision:

Table 1.6-1 (Sheet 12 of 20)		
MATERIAL REFERENCED		
DCD Section Number	Westinghouse Topical Report Number	Title
6A	WCAP-15846 (P) WCAP-15862	WGOTHIC Application to AP600 and AP1000, Revision 1, March 2004
	WCAP-14135 (P) WCAP-14138	Final Data Report for Passive Containment Cooling System Large Scale Test, Phase 2 and Phase 3, Revision 3, November 1998

(P) Denotes Document is Proprietary



AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

	WCAP-15613 (P) WCAP-15706	AP1000 PIRT and Scaling Assessment Report, March 2001
7.1	[WCAP-14605 (P) WCAP-14606 (NP)]	Westinghouse Setpoint Methodology for Protection Systems – AP600, April 1996]*
	WCAP-16361-P WCAP-16361-NP	Westinghouse Setpoint Methodology for Protection Systems - AP1000, May 2006
	WCAP-15775	AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report, March 2003
	[WCAP-16096-NP-A	Software Program Manual for Common Q Systems, Revision 01A, January 2004]*
	[WCAP-16097-P-A WCAP-16097-NP-A	Common Qualified Platform, Revision 01, May 2003]*
	WCAP-15776	Safety Criteria for the AP1000 Instrumentation and Control Systems, April 2002
	WCAP-16675-P WCAP-16675-NP	AP1000 Protection and Safety Monitoring System Architecture Technical Report, Revision 1
	APP-GW-GLR-017	AP1000 Standard Combined License Technical Report, Resolution of Common Q NRC Items
	NABU-DP-00014-GEN (P) WCAP-15927 (NP)	Design Process for Common Q Safety Systems, Revision 1, March 2006 Design Process for AP1000 Common Q Safety Systems, Revision 2, November 2008]*
		Westinghouse Electric Company Quality Management System (QMS), (Non-Proprietary), Revision 5, October 2002
	APP-GW-GLR-104	AP1000 Cyber Security Implementation, May 2007

7.1.1 The AP1000 Instrumentation and Control Architecture

Figure 7.1-1 illustrates the instrumentation and control architecture for the AP1000. The figure shows two major sections separated by the real-time data network. Figure 7.1-1 depicts the real-time data highway as a single network. ~~To meet cyber security concerns, the real-time data highway will be separated into security levels as described in Reference 22.~~

The lower portion of the figure includes the plant protection, control, and monitoring functions. At ~~the lower~~ the lower right-hand side is the protection and safety monitoring system. It performs the reactor trip functions, the engineered safety features (ESF) actuation functions, and the Qualified Data Processing (QDPS) functions. The I&C equipment performing reactor trip and ESF actuation functions, their related sensors, and the reactor trip switchgear

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

are, for the most part, four-way redundant. This redundancy permits the use of bypass logic so that a division or individual channel out of service can be accommodated by the operating portions of the protection system reverting to a two-out-of-three logic from a two-out-of-four logic.

The ESF coincidence logic performs system-level logic calculations, such as initiation of the passive residual heat removal system. It receives inputs from the plant protection subsystem bistables and the main control room. The ESF actuation subsystems provide the capability for on-off control of individual safety-related plant loads. They receive inputs from the ESF coincidence logic, remote shutdown workstation and the main control room.

The plant control system performs nonsafety-related instrumentation and control functions using both discrete (on/off) and modulating (analog) type actuation devices.

The nonsafety-related real-time data network, which horizontally divides Figure 7.1-1, is a high speed, redundant communications network that links systems of importance to the operator. Safety-related systems are connected to the network through gateways and qualified isolation devices so that the safety-related functions are not compromised by failures elsewhere. Plant protection, control, and monitoring systems feed real-time data into the network for use by the control room and the data display and processing system.

The upper portion of the figure depicts the control rooms and data display and processing system. The main control room is implemented as a set of compact operator consoles featuring color graphic displays and soft control input devices. The graphics are supported by a set of graphics workstations that take their input from the real-time data network. An advanced alarm system, implemented in a similar technology, is also provided.

The data display and processing (plant computer) system is implemented in a distributed architecture. The working elements of the distributed computer system are graphics workstations, although their graphics capability is secondary to their computing performance. The distributed computer system obtains its input from the real-time data network and delivers its output over the network to other users.

WCAP-15775 (Reference 7) describes the diversity and defense-in-depth features of the AP1000 instrumentation and control architecture.

Protection and Safety Monitoring System

The protection and safety monitoring system provides detection of off-nominal conditions and actuation of appropriate safety-related functions necessary to achieve and maintain the plant in a safe shutdown condition. The protection and safety monitoring system controls safety-related components in the plant that are operated from the main control room or remote shutdown workstation.

In addition, the protection and safety monitoring system provides the equipment necessary to monitor the plant safety-related functions during and following an accident as required by Regulatory Guide 1.97.

Special Monitoring System

The special monitoring system does not perform any safety-related or defense-in-depth functions. The special monitoring system consists of specialized subsystems that interface with the instrumentation and control architecture to provide diagnostic and long-term monitoring functions.

The special monitoring system is the metal impact monitoring system. The metal impact monitoring system detects the presence of metallic debris in the reactor coolant system when the debris impacts against the internal parts of the reactor coolant system. The metal impact monitoring system is composed of digital circuit boards, controls, indicators, power supplies and remotely located sensors and related signal processing devices. A minimum of two sensors are located at each natural collection region, connected to separate instrumentation channels, to maintain the impact monitoring function if a sensor fails in service. The metal impact monitoring system is described in subsection 4.4.6.4.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Plant Control System

The plant control system provides the functions necessary for normal operation of the plant from cold shutdown through full power. The plant control system controls nonsafety-related components in the plant that are operated from the main control room or remote shutdown workstation.

The plant control system contains nonsafety-related control and instrumentation equipment to change reactor power, control pressurizer pressure and level, control feedwater flow, and perform other plant functions associated with power generation. The plant control system is described in subsections 7.1.3 and 7.7.1.

Diverse Actuation System

The diverse actuation system is a nonsafety-related, diverse system that provides an alternate means of initiating reactor trip and actuating selected engineered safety features, and providing plant information to the operator. The diverse actuation system is described in subsection 7.7.1.11.

Operation and Control Centers System

The operation and control centers system includes the main control room, the technical support center, the remote shutdown room, emergency operations facility, local control stations and associated workstations for these centers. With the exception of the control console structures, the equipment in the control room is part of the other systems (for example, protection and safety monitoring system, plant control system, data display and processing system). The boundaries of the operation and control centers system for the main control room and the remote shutdown workstation are the signal interfaces with the plant components. These interfaces are via the plant protection and safety monitoring system processor and logic circuits, which interface with the reactor trip and ESF plant components; the plant control system processor and logic circuits, which interface with the nonsafety-related plant components; and the plant real-time data network, which provides plant parameters, plant component status, and alarms.

Data Display and Processing System

The data display and processing system provides the equipment used for processing data that result in nonsafety-related alarms and displays for both normal and emergency plant operations, generating these displays and alarms, providing analysis of plant data, providing plant data logging and historical storage and retrieval, and providing operational support for plant personnel.

The data display and processing system also contains the real-time data network, which is a redundant data highway that links the elements of the AP1000 instrumentation and control architecture.

Incore Instrumentation System

The primary function of the incore instrumentation system is to provide a three-dimensional flux map of the reactor core. This map is used to calibrate neutron detectors used by the protection and safety monitoring system, as well as to optimize core performance. A secondary function of the incore instrumentation system is to provide the protection and safety monitoring system with the thermocouple signals necessary for the post-accident inadequate core cooling monitor. The incore instrument assemblies house both fixed incore flux detectors and core exit thermocouples. The incore instrumentation system is described in subsection 4.4.6.1.

Cyber Security

Reference 22 describes the cyber security implementation for AP1000.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

7.1.2.14.1 Design Process

[WCAP-16096-NP-A (Reference 9) provides a planned design process for software development during life cycle stages:

- Conceptual phase (may also be referred to as design requirements phase)
- Requirements phase (may also be referred to as system definition phase)
- Design phase (may also be referred to as hardware and software development phase)
- Implementation phase (may also be referred to as hardware and software development phase)
- Test phase (may also be referred to as system integration and test phase)
- Installation and checkout phase (may also be referred to as installation phase)]*

The conceptual phase (design requirements phase) has been completed for AP1000.

~~[WCAP-16096-NP-A (Reference 9), NABU-DP-00014-GEN (Reference 20), and the NRC approved Westinghouse Quality Management System (Reference 21) describe design processes that will be used for AP1000.]*~~

~~NABU-DP-00014-GEN (Reference 20) provides lower level process implementation details.~~

~~[WCAP-15927, Revision 2 (Non-proprietary), "Design Process for AP1000 Common Q Safety Systems," November 2008.]*~~

~~Reference 22 describes the process for ensuring that the design life cycle process for the Protection and Safety Monitoring System meets the computer security requirements of IEEE 603 and Regulatory Guide 1.152.~~

7.1.7 References

1. IEEE 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
2. Deleted/Not used.
3. Deleted/Not used.
4. Deleted/Not used.
- [5. WCAP-14605 (Proprietary) and WCAP-14606 (Non-Proprietary), "Westinghouse Setpoint Methodology for Protection Systems, AP600," April 1996.]*
6. 10 CFR 21, "Reporting of Defects and Noncompliance."

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

7. WCAP-15775, Revision 2, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report," March 2003.
- [8. WCAP-16097-P-A (Proprietary) and WCAP-16097-NP-A (Non-Proprietary), Revision 0, "Common Qualified Platform," May 2003.]*
- [9. WCAP-16096-NP-A, Revision 01A, "Software Program Manual for Common Q Systems," January 2004.]*
10. Not used.Deleted.
11. Not used.Deleted.
12. WCAP-15776, "Safety Criteria for the AP1000 Instrument and Control Systems," April 2002.
13. Not used.Deleted.
14. Not used.Deleted.
- ~~15. Not used.Deleted.~~
15. IEEE 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."
16. Not used.Deleted.
17. WCAP-16361-P (Proprietary) and WCAP-16361-NP (Non-Proprietary), "Westinghouse Setpoint Methodology for Protection Systems – AP1000," May 2006.
18. APP-GW-GLR-017, AP1000 Standard Combined License Technical Report, "Resolution of Common Q NRC Items," Westinghouse Electric Company LLC.
19. WCAP-16675-P (Proprietary) and WCAP-16675-NP (Non-Proprietary), "AP1000 Protection and Safety Monitoring System Architecture Technical Report," Revision 1 February 2007.
- ~~20. NABU-DP-00014-GEN, Revision 1 (Proprietary), "Design Process for Common Q Safety Systems," March 2006.~~
20. [WCAP-15927, Revision 2 (Non-proprietary), "Design Process for AP1000 Common Q Safety Systems," November 2008.]*
21. Westinghouse Electric Company Quality Management System (QMS), Revision 5 (Non-Proprietary), October 1, 2002.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

22. APP-GW-~~GLRJ0R-104012~~, "AP1000 ~~Cyber Security Implementation~~Protection and Safety Monitoring System Computer Security Plan," ~~Revision 1~~, Westinghouse Electric Company LLC~~May 2008~~.

PRA Revision: None

Technical Report (TR) Revision: None

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

RAI Response Number: OI-SRP7.2-ICE-02

Revision: 1

Question: OI-SRP7.2-ICE-02

Clause 5.3 of IEEE Std. 603-1991 and Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50 require safety-related I&C systems to be designed, manufactured, inspected, installed, and tested under an acceptable quality assurance program. SRP Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2"; Section 5.3; and BTP 7-14 specifically address the criteria for a quality software development process. Additionally, the staff evaluated the documentation in the SLC against the guidance in the following documents:

- Regulatory Guide 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 1012-1998, "IEEE Standard for Software Verification and Validation," and IEEE Std. 1028-1997, "IEEE Standard for Software Reviews and Audits"
- Regulatory Guide 1.169 "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 828-1990, "IEEE Standard for Software Configuration Management Plans"
- Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 829-1983, "IEEE Standard For Software Test Documentation"
- Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing"
- Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 830-1993, "IEEE Recommended Practice for Software Requirements Specifications"
- Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 1074-1995, "IEEE Standard for Developing Software Lifecycles and Processes"

In Section 7.2.2.2, the staff discusses the approval of the Common Q platform topical report. However, additional requirements were placed on the SLC for the AP1000 safety system, as described in the Software Program Manual (SPM), WCAP-16096-NP-A, "Software Program Manual for Common Q Systems," Revision 1A, dated January 21, 2005 (ADAMS Accession No. ML050350234); and WCAP-15927, "Design Process for AP1000 Common Q Safety Systems," Revision 0. The certified design (Revision 15) of the AP1000 DCD designated the SPM and WCAP-15927 as Tier 2* documents, requiring NRC approval before altering WEC commitments. The staff recently received and reviewed WCAP-15927, Revision 2 (ADAMS Accession No. ML091890752).

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

In AP1000 DCD Tier 1, Table 2.5.2-8, Item 11, WEC removed the design requirements and system definition phases of the PMS SLC ITAAC. The design requirements phase corresponds to the planning activities phase of the SLC in SRP BTP 7-14, and the system definition phase corresponds to the requirements activities phase in the same SRP BTP. WEC made available for audit the software planning documents to support removal of the design requirements phase. The staff audited those software planning documents on several occasions. WEC describes its quality software development process for the AP1000 project in the Common Q SPM and WCAP-15927, Revision 2. The staff reviewed the proprietary and nonproprietary documentation associated with the first two phases of the SLC as it relates to PMS system development.

WEC originally provided 11 documents that comprise the design requirements phase of the AP1000 SLC. On April 9–11, 2008; October 9–16, 2008; January 22–30, 2009; and July 30, 2009, the staff conducted site visits at the Twinbrook WEC location in Rockville, MD, to review the proprietary documents associated with the design requirements phase. WEC continues to modify design and technical information in the documents affecting the supervisory, subordinate, and peer-to-peer relationships of the design requirements phase documents. In RAI-SRP7.1-ICE-03, the NRC asked WEC to explain in the DCD how it meets the requirements of the planning ITAAC. This may include a diagram of the planning process and planning documents related to cyber security and other project-specific documents. **The NRC staff identified this issue as OI-SRP-7.2-02.**

Westinghouse Response:

Westinghouse will revise the DCD as described below to explain how WEC meets the requirements of the planning ITAAC, also known as the design requirements phase of the software lifecycle.

Design Control Document (DCD) Revision:

7.1.2.14.1 Design Process

[WCAP-16096-NP-A (Reference 9) provides a planned design process for software development during life cycle stages:

- Conceptual phase (may also be referred to as design requirements phase)*
- Requirements phase (may also be referred to as system definition phase)*
- Design phase (may also be referred to as hardware and software development phase)*
- Implementation phase (may also be referred to as hardware and software development phase)*
- Test phase (may also be referred to as system integration and test phase)*
- Installation and checkout phase (may also be referred to as installation phase)]**

~~The conceptual phase (design requirements phase) has been completed for AP1000.~~

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

[WCAP-16096-NP-A (Reference 9) and the NRC-approved Westinghouse Quality Management System (Reference 21) describe design processes that will be used for AP1000.]*
NABU-DP-00014-GEN (Reference 20) provides lower-level process implementation details.

The planning (or design requirements) phase documents are listed below. Figure 7.1xxxxx shows the relationship of the same documents.

Document 1: WNA-PN-00043-WAPP, “NuStart/DOE Design Finalization Program.”

Document 2: WNA-PQ-00201-WAPP, “NuStart/DOE Design Finalization Program Project Quality Plan.”

Document 3: WNA-PN-00045-WAPP, “NuStart/DOE Design Finalization Protection and Safety Monitoring System Project Plan.”

Document 4: WNA-PD-00042-WAPP, “NuStart/DOE Design Finalization Protection and Safety Monitoring System So, “ftware Development Plan.”

Document 5: WCAP-16096-NP-A, “Software Program Manual for Common Q Systems”

Document 6: NABU-DP-00014-GEN, “Design Process for Common Q Safety Systems”

Document 7: WNA-PV-00009-GEN, “Verification & Validation Process for the Common Q Safety Systems”

Document 8: WNA-PT-00058-GEN, “Testing Process for Common Q Safety Systems”

Document 9: NABU-DP-00015-GEN, “Common Q Software Configuration Management Guidelines”

Document 10: 00000-ICE-3889, “Coding Standards & Guidelines for Common Q Systems”

Document 11: WNA-VR-00213-GEN, and is now APP-PMS-GER-020, “Protection and Safety Monitoring System Concept Phase V&V Summary Report.”

Document 12: APP-PMS-T5-001, “AP1000 Protection and Safety Monitoring System Test Plan”

Document 13: WCAP-15927, “Design Process for AP1000 Common Q Safety Systems”

Document 14: APP-GW-J0H-001, “AP1000 I&C Systems Cyber Security Plan”

NRC Comment from 6/15/10 Meeting:

WEC is to provide a figure (document tree) and swap out the cyber/computer security reference.

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

Westinghouse Rev 1 Response:

[WCAP-16096-NP-A provides a planned design process for software development during life cycle stages:

- Conceptual phase (may also be referred to as design requirements phase)
- Requirements phase (may also be referred to as system definition phase)
- Design phase (may also be referred to as hardware and software development phase)
- Implementation phase (may also be referred to as hardware and software development phase)
- Test phase (may also be referred to as system integration and test phase)
- Installation and checkout phase (may also be referred to as installation phase)]*

[WCAP-16096-NP-A (Reference 9), WCAP 15927 (Reference 20), and the NRC-approved Westinghouse Quality Management System (Reference 21) describes design processes that will be used for AP1000.]*
~~NABU-DP-00014-GEN (Reference 20) provides lower level process implementation details.~~

The planning (or design requirements) phase documents are listed below. Figure 7.1-2 shows the relationship of the same documents.

References:

None

Design Control Document (DCD) Revision:

7.1.2.14.1 Design Process

[WCAP-16096-NP-A (Reference 9) provides a planned design process for software development during life cycle stages:

- Conceptual phase (may also be referred to as design requirements phase)
- Requirements phase (may also be referred to as system definition phase)
- Design phase (may also be referred to as hardware and software development phase)
- Implementation phase (may also be referred to as hardware and software development phase)
- Test phase (may also be referred to as system integration and test phase)
- Installation and checkout phase (may also be referred to as installation phase)]*

[WCAP-16096-NP-A (Reference 9), WCAP-15927 (Reference 20) and the NRC-approved Westinghouse Quality Management System (Reference 21) describe design processes that will be used for AP1000.]*
~~NABU-DP-00014-GEN (Reference 20) provides lower level process implementation details.~~

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

The planning (or design requirements) phase documents are listed below. Figure 7.1-2~~xxxxx~~ shows the relationship of the same documents.

Document 1: WNA-PN-00043-WAPP, “NuStart/DOE Design Finalization Program.”

Document 2: WNA-PQ-00201-WAPP, “NuStart/DOE Design Finalization Program Project Quality Plan.”

Document 3: WNA-PN-00045-WAPP, “NuStart/DOE Design Finalization Protection and Safety Monitoring System Project Plan.”

Document 4: WNA-PD-00042-WAPP, “NuStart/DOE Design Finalization Protection and Safety Monitoring System Software Development Plan.”

Document 5: WCAP-16096-NP-A, “Software Program Manual for Common Q Systems”

Document 6: NABU-DP-00014-GEN, “Design Process for Common Q Safety Systems”

Document 7: WNA-PV-00009-GEN, “Verification & Validation Process for the Common Q Safety Systems”

Document 8: WNA-PT-00058-GEN, “Testing Process for Common Q Safety Systems”

Document 9: NABU-DP-00015-GEN, “Common Q Software Configuration Management Guidelines”

Document 10: 00000-ICE-3889, “Coding Standards & Guidelines for Common Q Systems”

Document 11: ~~WNA-VR-00213-GEN, and is now~~ APP-PMS-GER-020, “Protection and Safety Monitoring System Concept Phase V&V Summary Report.”

Document 12: APP-PMS-T5-001, “AP1000 Protection and Safety Monitoring System Test Plan”

Document 13: WCAP-15927, “Design Process for AP1000 Common Q Safety Systems”

~~Document 14: APP-GW-J0H-001, “AP1000 I&C Systems Cyber Security Plan”~~

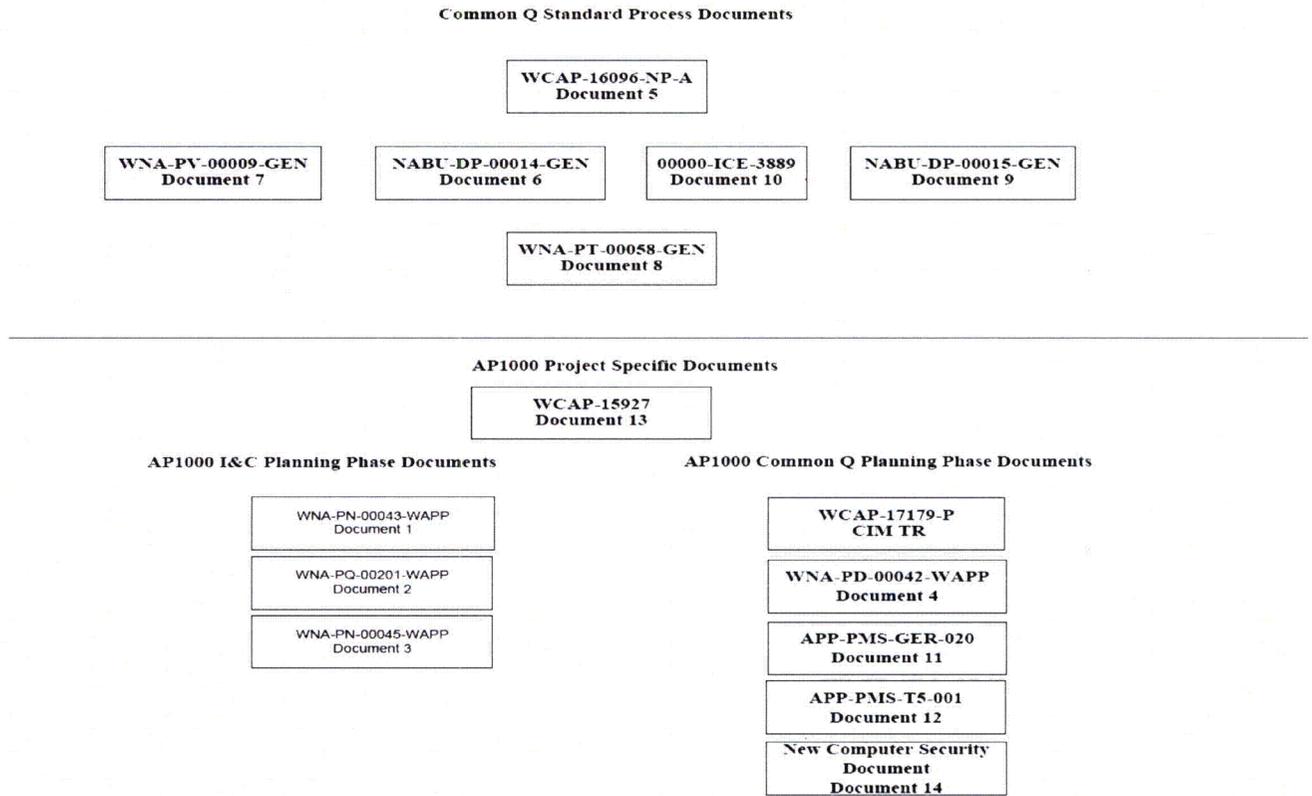
Document 14: APP-GW-J0R-012, AP1000™ Protection and Safety Monitoring System Computer Security Plan

Document 15: APP-GW-GLR-143, AP1000™ Component Interface Module Technical Report

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

Figure 7.1-2 Common Q Standard Process and AP1000 Project Specific Documents



AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

Figures 7.1-~~23~~ through 7.1-11 not used.

PRA Revision:

None

Technical Report (TR) Revision:

None

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

RAI Response Number: RAI-SRP7.1-SHA-01 (OI-SRP7.1-ICE-02)
Revision: 0

Question:

Westinghouse submitted WCAP 16592-P, "Software Hazards Analysis of AP1000 Protection and Safety Monitoring System, (SHA) Revision 1. The report fails to mention any potential failures introduced into the PMS as a result of a design or programming error of the Component Interface Module (CIM). While the CIM uses no software during its operation, a programming language is used extensively during the device's development.

Westinghouse committed to follow IEEE Standard (Std.) 603–1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995," that is an incorporate by reference standard within 10 CFR 50.55a, "Codes and Standards". IEEE Std. 603–1991 requires among other things that, safety systems within nuclear power plants be designed and constructed with sufficient Quality, Clause 5.3; and Reliability, Clause 5.15. Westinghouse also committed to following the guidance within Branch Technical Position BTP) 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," of NUREG – 0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: Light Water Reactor Edition," (SRP). Within the "Acceptance Criteria for Resources Characteristics of Planning Documents," of BTP 7-14, it relates the applicant should address the use of methods or tools employed for use or development of the safety system. Additionally, Section B.3.1.9, Software Safety Plan discusses the use of a Software Safety Plan and the discussion of risks and hazards the software, or programmable technology, is expected to control. The staff understands the AP1000 PMS SHA is intended to address these hazards and, as such, the staff requires discussion within the AP1000 PMS SHA to focus upon the issue of software hazards encountered, and successfully mitigated or eliminated during the CIM development process.

Westinghouse Response:

WCAP-16592-P (APP-PMS-GER-001), Rev 1 "Software Hazards Analysis of AP1000 Protection and Safety Monitoring System" will be revised as follows:

Section 2.4:

The ILC cabinet contains redundant ILP process stations, in two separate subracks, each receiving HSLs from the two LCL process stations that generate the system-level automatic commands. The two ILP process stations output the component actuation commands via independent HSLs through a safety remote node controller (SRNC). The SRNC is described in WNA-DS-01272-GEN, "Safety System Remote Note Controller Hardware Requirements Specification" (Reference 9). The commands then go via the SRNC to a component interface module (CIM) for air-operated valve (AOV), hydraulic-operated valve (HOV), motor-operated valve (MOV), solenoid-operated valve (SOV), switchgear, and squib

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

operated valves. The CIM is described in detail in WNA-DS- 01271-GEN, "Component Interface Module (CIM) Hardware Requirements Specification" (Reference 10). The two ILP process stations use a unidirectional HSL to the CIM via the SRNC. The CIM actuation logic is a logical AND to prevent spurious actuations on single failures.

The following paragraph is added to the end of Section 2.4:

"The SRNCs and CIMs are logic based modules that do not use microprocessors or software for operation, but instead utilize architecture based on FPGA technology. FPGA-based systems employ software tools to configure and test the resulting customized circuitry. As a result, the SRNC and CIM software development tools are considered in the software hazard analysis for AP1000."

The following table will be added to Section 5:

Name	Hazard Description	Hazard Cause	Method of Detection	Potential Consequences	Safety Hazard Mitigation	Safety Hazard Control Verification Method
CIM or SRNC	Logical programming error of the CIM or SRNC.	Programming error during creation of the FPGA logic in the software tool.	Random single failure or CCF of multiple divisions detected by component feedback signals, periodic surveillance testing, or by effect on plant process.	CIMs or SRNCs do not function as intended. Possible spurious actuation of ESF function or prevention of component actuation.	DAS for common mode failure affecting CIMs in multiple divisions	IV&V review of the functional logic. IV&V testing to functional requirements.
	Error in software tool used to configure FPGA.	An error in the FPGA software tool results in the wrong FPGA configuration.	Random single failure or CCF of multiple divisions detected by component feedback signals, periodic surveillance testing, or by effect on plant process.	CIMs or SRNCs do not function as intended. Possible spurious actuation of ESF function or prevention of component actuation.	If random tool error failure, then other PMS divisions will perform function. CCF covered by DAS.	IV&V testing to functional requirements.

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

Error in software tool used to test FPGA.	An error in the simulation tool used to test the FPGA results in improper indication that FPGA design is correct.	Random single failure or CCF of multiple divisions detected by component feedback signals, periodic surveillance testing, or by effect on plant process.	CIMs or SRNCs do not function as intended. Possible spurious actuation of ESF function or prevention of component actuation.	If random tool error failure, then other PMS divisions will perform function. CCF covered by DAS.	IV&V review of the FPGA logic to functional requirements. Two independent test benches are developed on two independent simulation tools.
---	---	--	--	---	---

References:

1. WCAP-16592-P (APP-PMS-GER-001), Rev 1 "Software Hazards Analysis of AP1000 Protection and Safety Monitoring System"

Design Control Document (DCD) Revision:

None

PRA Revision:

None

Technical Report (TR) Revision:

1. WCAP-16592-P (APP-PMS-GER-001), Rev 1 "Software Hazards Analysis of AP1000 Protection and Safety Monitoring System"

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.0-ICE-05
Revision: 1

Question:

WCAP-17179-P does not adequately describe the system response (e.g. Is the signal output locked-in?) when a CIM or SRNC goes from an operational state to an inadvertently non-operational state, such as during a momentary loss of power. Additionally, the terms "initialization," "reset," and "default state" associated with CIM and SRNC start-up and operational modes should be defined.

Westinghouse Response:

The following text will be reworded in sections 2.3.1.2.8 and 2.3.2.2.6 in the AP1000 Component Interface Module Technical Report, WCAP-17179 Revision 1.

[

]a,c

The following definitions will be added to the AP1000 Component Interface Module Technical Report, WCAP-17179 Revision 1.

Default State The state of the CIM output devices and the CIM data passed from the SRNC to the CIM, when the CIM and SRNC are not in operational mode.

The default state of the CIM output devices is described in R004.50, "Component Interface Module Hardware Requirements Specification," WNA-DS-01271-GEN, Revision 7.

The default state of the CIM data passed from the SRNC to the CIM is described in R004.2, "Safety System Remote Node Controller Requirements," WNA-DS-01272-GEN, Revision 5.

Reset Mode [

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

] ^{a,c} [

] ^{a,c}

Operational Mode A mode of operation where the power supplied to the FPGA is within the predetermined acceptable range. In this mode, the CIM and SRNC are fully functional and operational.

NRC Question from 6/24/10 Email:

WEC commits to update WCAP 17179-P report explaining system response and what occurs to devices' output in "default" state.

Westinghouse Rev 1 Response:

The following definition will be revised in the AP1000 Component Interface Module Technical Report, WCAP-17179 Revision 2.

Default State The state of the CIM output devices and the CIM data passed from the SRNC to the CIM, when the CIM and SRNC are not in operational mode.

The default state of the CIM output devices is described in R004.50, "Component Interface Module Hardware Requirements Specification," WNA-DS-01271-GEN, Revision 7. [

] ^{a,c}

The default state of the CIM data passed from the SRNC to the CIM is described in R004.2, "Safety System Remote Node Controller Requirements," WNA-DS-01272-GEN, Revision 5. [

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

J^{a,c}

Design Control Document (DCD) Revision:
None

PRA Revision:
None

Technical Report (TR) Revision:
WCAP-17179, Revision 1

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.0-ICE-11
Revision: 1

Question:

WCAP-17179-P should state that the CIM and SRNC are programmable technology devices and not imply they are hardware devices and therefore be treated as discrete or analog technology. The report should describe the high quality lifecycle development process for the devices.

Westinghouse Response:

The following wording will be updated throughout the AP1000 Component Interface Module Technical Report, WCAP-17179 Revision 1.

The CIM and SRNC are logic based modules that do not use microprocessors or software for operation, but instead utilize architecture based on programmable technology. The logic is implemented using field programmable gate array (FPGA) technology.

Section 2.7 of "AP1000 Component Interface Module Technical Report," WCAP-17179, Revision 1, will be updated to more thoroughly describe the high quality development process for the CIM and SRNC modules.

NRC Question from 6/24/10 Email:

The CIM TR should describe logic being treated as software.

Westinghouse Rev 1 Response:

The CIM development process, as described in Section 2.7 of "AP1000 Component Interface Module Technical Report," WCAP-17179, will be deleted in Revision 2 of the WCAP. Additionally, all references to the MSFIS project and/or Wolf Creek Generating Station will be removed from WCAP-17179.

The following sentences will be updated in Section 1.1.

The CIM system components are logic based modules that do not use microprocessors or software for operation, but instead utilize architecture based on FPGA technology. FPGA-based systems employ software tools to configure and test the resulting customized circuitry. As a result, the CIM will be developed following a high-quality software lifecycle development process.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

In addition, the DCD Revision 18 will include an ITAAC to describe the CIM development process. The following words constitute this ITAAC.

Design Control Document (DCD) Revision:

Table 2.5.2.-8 Inspections, Tests, Analyses, and Acceptance Criteria		
Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
14. The Component Interface Module (CIM) is developed using a planned design process which provides for specific design documentation and reviews.	An inspection and or an audit will be performed of the processes used to design the hardware, development software, qualification and testing.	A Safety Evaluation Report exists and concludes that CIM meets the below listed life cycle stages and is approved for use in the AP1000 safety related PMS. Life cycle stages: <ul style="list-style-type: none">a. Design requirements phase, may be referred to as conceptual or project definition phaseb. System definition phasec. Hardware and software development phase, consisting of hardware and software design and implementationd. System integration and test phasee. Installation phase

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Add item 14 to DCD Tier 1 Subsection 2.5.2

2.5.2 Protection and Safety Monitoring System

14. The Component Interface Module (CIM) is developed using a planned design process which provides for specific design documentation and reviews during the following life cycle stages:

- a) Design requirements phase, may be referred to as conceptual or project definition phase
- b) System definition phase
- c) Hardware and software development phase, consisting of hardware and software design and implementation
- d) System integration and test phase
- e) Installation phase

PRA Revision:

None

Technical Report (TR) Revision:

WCAP-17179, Revision 2

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.0-ICE-13
Revision: 1

Question:

WCAP-17184-P should describe how a sufficient measure of human diversity exists between the CIM and DAS development processes.

Westinghouse Response:

The following information will be added to WCAP-17184-P in section 9.4 "Human Diversity:

The design, verification, and validation programs for I&C systems, as described in []^{a,c} and the DAS Design Process (Reference 15), require and specify the use of independent review. It is a requirement of the DAS that different people (personnel not assigned to safety system engineering) will be responsible for its design and fabrication, including V&V.

The AP1000 Component Interface Module (CIM), [

] ^{a,c} The AP1000 CIM Technical Report, Reference 21, identifies []^{a,c}

The CIM Technical Report WCAP-17179-P, section 2.11 "Diversity", contains information regarding the diversity between the DAS and CIM. Section 2.11.4 "Human Diversity" contains the following information:

The purpose of human diversity is to reduce the chance of common errors in similar designs. [

] ^{a,c}

The diversity discussion between DAS and CIM will be maintained in the CIM Technical Report only.

NRC Question from 6/24/10 Email:

The language in WCAP 17179 is to include human diversity information similar to what is in the DAS TR.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Westinghouse Rev 1 Response:

The diversity discussion between DAS and CIM will be maintained in the CIM Technical Report only. The following information will be added to WCAP-17184, which is also described in the DAS TR.

The design, verification, and validation programs for I&C systems, as described in [

] ^{a,c} and the DAS Design Process (Reference 15), require and specify the use of independent review.....

The CIM TR will also contain the following information:

The purpose of human diversity is to reduce the chance of common errors in similar designs. [

] ^{a,c}

Design Control Document (DCD) Revision:

None

PRA Revision:

None

Technical Report (TR) Revision:

WCAP-17184-P, Rev. 1

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.0-ICE-14

Revision: 1

Question:

WCAP-15775, "AP1000 Instrumentation and Control Defense and Depth and Diversity Report," Revision 3, makes several references to obsolete document titles or references that must be updated.

Westinghouse Response:

An NRC audit of the AP1000 I&C Systems Requirements, Design Specification, and Sub-system Requirements located an instance in which requirements are inconsistent with the design commitments made within the AP1000 DCD. These inconsistencies were discovered in document APP-GW-J1R-004 / WCAP-15775. A revised document APP-GW-J1R-004 / WCAP-15775 is being prepared for submittal on the docket. The tracking number for this Corrective Action is IR#10-141-M033.

NRC Question from 6/24/10 Email:

After review, references to documents and document numbers and titles in WCAP 15775 were found updated, but the document must clarify why a Tier 2* document (13383) is being removed. Also, the D3 report to be updated to remove 13383 and 15927. These are both Tier 2* documents.

Westinghouse Rev 1 Response:

As explained at the June 16th meeting with the NRC WCAP-13383 is no longer needed as a reference in the DCD and it was replaced with WCAP-15927 in WCAP-15775.

WCAP-13383, "AP600 Instrumentation and Control Hardware and Software Design Verification, and Validation Process Report" mostly addresses the design of an "Eagle 21" safety system. WCAP-13383 is replaced by WCAP 15927, "Design Process for AP1000 Common Q Safety Systems" because it is a more current, relevant document, and it is specifically written for the design of the actual safety system used in the AP1000 design.

In Rev 17, WCAP-13383 and WCAP-15927 were replaced by NABU-DP-00014-GEN because it was the all inclusive version of WCAP-15927. This is explained on page 12 of TR-80. Because NABU- DP-00014-GEN is a proprietary document and because the NRC requested changes to WCAP-15927, WCAP-15927 will be reinstated back into the DCD and NABU-DP-00014-GEN removed.

In conclusion, WCAP-15927 is the reference for the design process of the AP1000 Common Q.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Design Control Document (DCD) Revision:

None

PRA Revision:

None

Technical Report (TR) Revision:

APP-GW-J1R-004 / WCAP-15775 Revision 5 will contain the above discussed changes to the list of references.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.0-ICE-15
Revision: 1

Question:

WCAP-15775, makes reference to multiplexers which were removed from the I&C design in Revision 16 of the AP1000 DCD.

Westinghouse Response:

An NRC audit of the AP1000 I&C Systems Requirements, Design Specification, and Sub-system Requirements discovered that WCAP-15775 (APP-GW-J1R-004) makes reference to multiplexers, a term that was removed from the I&C design in Revision 16 of the AP1000 DCD. Document APP-GW-J1R-004 / WCAP-15775 is being revised to remove all references to multiplexers. The revised document will be submitted on the docket. The tracking number for this Corrective Action is IR#10-141-M033.

NRC Question from 6/24/10 Email:

The language in WCAP 17179-P, WCAP-17184-P and WCAP 15775 must agree, or point to one "parent" reference to ensure different personnel work on CIM, CIM IV&V, and DAS systems. Alos, the D3 report must be updated to remove MUX from the figure.

Westinghouse Rev 1 Response:

As discussed in the NRC meeting on June 16th, the language in WCAP 17179-P, WCAP-17184-P and WCAP 15775 are in agreement in describing the diversity of the personnel work on CIM, CIM IV&V, and DAS systems.

The removal of "MUX" from WCAP-15775 will be addressed in Revision 5 of the WCAP.

Design Control Document (DCD) Revision:

None

PRA Revision:

None

Technical Report (TR) Revision:

APP-GW-J1R-004 / WCAP-15775 Revision 5

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.8-DAS-05
Revision: 0

Question:

Provide the criteria for implementation of diversity at the common design and manufacturing facility of the Component Interface Module (CIM) and the Diverse Actuation System (DAS).

10 CFR Part 50, Appendix A, General Design Criteria 22, requires, in part, that design techniques such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of protective function. The staff understands that a portion of the Protection and Monitoring System, the CIM, will be developed by the same company that develops the DAS. Identify the criteria, practices, and processes that will ensure adequate diversity in the development of the CIM and the DAS. In particular, address the diversity with respect to human and equipment diversity.

NRC Comment from 6/15/10 Meeting:

The DCD Tier 1 wording for programming languages for CIM/DAS requires the use of different approaches. WEC plan was to use the same FPGA programming language, but processed using different methods.

Westinghouse Response:

Tier 1 and Tier 2 of the DCD will be updated to include the following words to address software diversity:

“Software diversity between DAS and PMS will be achieved through the use of different algorithms, logic, program architecture, executable operating system and executable software/logic.”

In addition, the DAS Technical Report (WCAP-17184-P) will also be updated.

The specific markups to the DCD and the DAS Technical Report are below and highlighted in yellow.

Design Control Document (DCD) Revision:

DCD Tier 1 Update:

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

2.5.1 Diverse Actuation System

Design Description

The diverse actuation system (DAS) initiates reactor trip, actuates selected functions, and provides plant information to the operator.

The component locations of the DAS are as shown in Table 2.5.1-5.

1. The functional arrangement of the DAS is as described in the Design Description of this Section 2.5.1.
2. The DAS provides the following nonsafety-related functions:
 - a) The DAS provides an automatic reactor trip on low wide-range steam generator water level or on low pressurizer water level separate from the PMS.
 - b) The DAS provides automatic actuation of selected functions, as identified in Table 2.5.1-1, separate from the PMS.
 - c) The DAS provides manual initiation of reactor trip and selected functions, as identified in Table 2.5.1-2, separate from the PMS. These manual initiation functions are implemented in a manner that bypasses the control room multiplexers, if any; the PMS cabinets; and the signal processing equipment of the DAS.
 - d) The DAS provides main control room (MCR) displays of selected plant parameters, as identified in Table 2.5.1-3, separate from the PMS.
3. The DAS has the following features:
 - a) The signal processing hardware of the DAS uses input modules, output modules, and microprocessor or special purpose logic processor boards that are different than those used in the PMS.
 - b) The display hardware of the DAS uses a different display device than that used in the PMS.
 - c) ~~Any operating systems or programming languages used by DAS are different than those used in the PMS.~~ Software diversity between DAS and PMS will be achieved through the use of different algorithms, logic, program architecture, executable operating system and executable software/logic.
 - d) The DAS has electrical surge withstand capability (SWC), and can withstand the electromagnetic interference (EMI), radio frequency (RFI), and electrostatic discharge (ESD) conditions that exist where the DAS equipment is located in the plant.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

- e) The sensors identified on Table 2.5.1-3 are used for DAS input and are separate from those being used by the PMS and plant control system.
- f) The DAS is powered by non-Class 1E uninterruptible power supplies that are independent and separate from the power supplies which power the PMS.
- g) The DAS signal processing cabinets are provided with the capability for channel testing without actuating the controlled components.
- h) The DAS equipment can withstand the room ambient temperature and humidity conditions that will exist at the plant locations in which the DAS equipment is installed at the times for which the DAS is designed to be operational.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Table 2.5.1-4 (cont.) Inspections, Tests, Analyses, and Acceptance Criteria		
Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
3.c) Any operating systems or programming languages used by DAS are different than those used in the PMS. Software diversity between the DAS and PMS will be achieved through the use of different algorithms, logic, program architecture, executable operating system and executable software/logic.	Inspection of the DAS and PMS design documentation will be performed.	Any DAS operating systems and programming languages are different than those used in the PMS. Any DAS algorithms, logic, program architecture, executable operating systems, and executable software/logic are different than those used in the PMS.

DCD Tier 2 Update

7.7.1.11 Diverse Actuation System

The diverse actuation system is a nonsafety-related system that provides a diverse backup to the protection system. This backup is included to support the aggressive AP1000 risk goals by reducing the probability of a severe accident which potentially results from the unlikely coincidence of postulated transients and postulated common mode failure in the protection and control systems.

The protection and safety monitoring system is designed to prevent common mode failures. However, in the low probability case where a common mode failure does occur, the diverse actuation system provides diverse protection. The specific functions performed by the diverse actuation system are selected based on the PRA evaluation. The diverse actuation system functional requirements are based on an assessment of the protection system instrumentation common mode failure probabilities combined with the event probability.

The functional logic for the diverse actuation system is shown in Figure 7.2-1, sheets 19 and 20.

Automatic Actuation Function

The automatic actuation signals provided by the diverse actuation system are generated in a functionally diverse manner from the protection system actuation signals. The common-mode failure of sensors of a similar design is also considered in the selection of these functions.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

The automatic actuation function is accomplished by redundant logic subsystems. Input signals are received from the sensors by an input signal conditioning block, which consists of one or more electronic modules. This block converts the signals to standardized levels, provides a barrier against electromagnetic and radio frequency interference, and presents the resulting signal to the input signal conversion block. The conversion block continuously performs analog to digital signal conversions and stores the value for use by the signal processing block.

The signal processing block polls the various input signals, evaluates the input signals against stored setpoints, executes the logic when thresholds are exceeded, and issues actuation commands.

The resulting output signals are passed to the output signal conversion block, whose function is to convert logic states to parallel, low-level dc signals. These signals are passed to the output signal conditioning block. This block provides high-level signals capable of switching the traditional power plant loads, such as breakers and motor controls. It also provides a barrier against electromagnetic and radio frequency interference.

The DAS automatic actuation signals are generated in a functionally diverse manner from the PMS signals. Diversity between DAS and PMS is achieved by the use of different architectures, different hardware implementations, and different software, if any.

~~Diversity of any software is achieved by running different operating systems and programming in different languages.~~ Software diversity between the DAS and PMS will be achieved through the use of different algorithms, logic, program architecture, executable operating system and executable software/logic.

14.3 Certified Design Material

Table 14.3-6 (Sheet 7 of 10)

PROBABILISTIC RISK ASSESSMENT		
Section	7.7.1.11	<p>The DAS automatic actuation signals are generated in a functionally diverse manner from the PMS signals. Diversity between DAS and PMS is achieved by the use of different architectures, different hardware implementations, and different software, if any.</p> <p>Software diversity between the DAS and PMS will be achieved through the use of different algorithms, logic,</p>

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

PRA Revision:

None

Technical Report (TR) Revision:

WCAP-17184, Rev. 2

DAS Technical Report (WCAP-17184-P) updates.

10.2.2 DAS Applicability

[

•

•

] ^{a,c}

9.6 [

] ^{a,c}

[

] ^{a,c}

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Software diversity between the DAS and PMS will be achieved through the use of different algorithms, logic, program architecture, executable operating system and executable software/logic.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.8-DAS-06

Revision: 0

Question:

Explain design basis for discrepancy between DAS manual actuations listed.

1 OCFR52.47(a)(2) states that an application must contain a "description and analysis of the structures, systems, and components (SSCs) of the facility, with emphasis upon performance requirements, the bases, with technical justification therefore, upon which these requirements have been established, and the evaluations required to show that safety functions will be accomplished.... The description shall be sufficient to permit understanding of the system designs and their relationship to the safety evaluations ... ," The design information provided for the design basis items, taken alone and in combination, should have one and only one interpretation, Therefore, the staff requests the applicant to provide correct and unambiguous design descriptions for the DAS manual actuations.

The staffs review of manual actuation discrepancies are listed in Table 07.08-1 below:

Table 07.08-1 - DAS Manual Actuation Discrepancies*			
Manual Actuation	Manual Action(s) Listed in		
	Revision 17, Tier 2, FSAR Section 7.7.1.11	WCAP-17184-R1; Section 2.3	WCAP-17184-R1; Table B-1
Reactor trip			
Turbine Trip			Not Listed
Passive containment cooling actuation			
Core makeup tank actuation and reactor coolant pump trip			
Open stage 1 automatic depressurization system valves			
Open stage 2 automatic depressurization system valves			
Open stage 3 automatic depressurization system valves			
Open stage 4 automatic depressurization system valves			
Open the passive residual heat removal discharge isolation valves and close the in-containment refueling water storage tank gutter isolation valves			
Selected containment penetration isolation			
Containment hydrogen igniter actuation		Not Listed	
Initiate in-containment refueling water storage tank injection			
Initiate containment recirculation			
Initiate in-containment refueling water storage tank drain to containment		Not Listed	
Reactor Coolant Pump trip	Not Listed	Not Listed	

*A blank entry means that the stated manual actuation is listed in document.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Westinghouse Response:

Both the current certified AP1000 design (DCD Revision 15) and in Revision 17 Tier 2, Chapter 16, Appendix B, Section 3.3.5, the Diverse Actuation System (DAS) manual controls provide non-Class 1E backup controls in case of common-mode failure of the Protection and Safety Monitoring System (PMS) automatic and manual actuations evaluated in the AP1000 PRA. These DAS manual controls are not credited for mitigating accidents in the DCD Chapter 15 (safety) analyses.

DAS manual actions are not "design basis" items as posited in this RAI. Probabilistic Risk Assessment (PRA) analytical techniques were used to provide insights as to the relative importance of DAS manual actions for beyond design basis occurrences. In no case does the failure to manually actuate a DAS function result in an unacceptable result using PRA analytical techniques. No DAS manual actuations are credited in the AP1000 Safety Analysis.

Westinghouse does recognize that, regardless of the lack of a relationship to the design basis, correct and unambiguous design descriptions for the DAS manual actions are needed. The description of these is contained in the DAS TR (APP-GW-GLR-145).

The list in the DCD is all inclusive of any manual actuation performed by DAS. It is correct and the tripping of the Reactor Coolant Pumps is only done in conjunction with the Core Makeup tank actuation and therefore not separately listed in the DCD.

The list in section 2.3 of WCAP-17184 is the list of manual actuations that are cited in the PRA for enabling AP1000 to meet its aggressive LRF goal for beyond design basis events, as the WCAP currently states. Therefore this list would be different than the list in the DCD because not all of the DAS manual actuations are needed to meet the LRF goal for beyond design basis events.

The table B-1 in WCAP-17184 is also not intended to be a complete list of all of the manual actuations. This table will be modified to only include those manual actuations that do not have automatic DAS actuations.

Design Control Document (DCD) Revision:

None

PRA Revision:

None

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Technical Report (TR) Revision:

The DAS TR WCAP-17184 will be updated in Revision 2 to reflect the changes to Appendix B. See the DAS TR mark-up (submitted separately) for details.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.8-DAS-07

Revision: 0

Question:

WCAP-17184-P Revision 1 Appendix B, Table B-1 lists manual actuation of the hydrogen igniters. Explain why this action is not a credited DAS manual operator action and/or a DAS automatic function. In addition, provide the design basis for its inclusion.

10 CFR Part 50, Appendix A, GDC 22, requires, in part, that design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protective function. Branch Technical Position HICB19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," Revision 4 (BTP-7-19), states that where operator action is cited as the diverse means for response to an event, the applicant should demonstrate that adequate information (indication) and sufficient time is available for operator action. The staff's review of WCAP-17184-P, Section 10.2.1.1, determined that the stated design descriptions do not provide an explanation of how manual actions are used in the DAS design beyond listing the manual actions. From the PRA evaluation there appears to be a 19 minute window for accomplishing this action. Therefore, the staff could not identify clear design basis descriptions that will permit sufficient understanding of credited DAS manual actuations and their conformance to the applicable regulatory requirements.

Westinghouse Response:

Both the current certified AP1000 design (DCD Revision 15) and in Revision 17 Tier 2, Chapter 16, Appendix B, Section 3.3.5, the Diverse Actuation System (DAS) manual controls provide non-Class 1E backup controls in case of common-mode failure of the Protection and Safety Monitoring System (PMS) automatic and manual actuations evaluated in the AP1000 PRA. These DAS manual controls are not credited for mitigating accidents in the DCD Chapter 15 (safety) analyses.

Probabilistic Risk Assessment (PRA) analytical techniques were used to provide insights as to the relative importance of DAS manual actions for beyond design basis occurrences. In no case does the failure to manually actuate a DAS function result in an unacceptable result using PRA analytical techniques. No DAS manual actuations are credited in the AP1000 Safety Analysis.

For this particular scenario, PRA analysis techniques show acceptable results even if the act of manually actuating the hydrogen igniters is not accomplished (operator fails to act with 100% certainty). For this reason, manual actuation of the hydrogen igniters is not a credited manual operator action nor is it required (or credited) for hydrogen igniters to operate automatically. The 19 minute window as described in the PRA analysis cited in this RAI is for a beyond design basis event. This PRA analysis was used to provide insights into this particular scenario.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Hydrogen igniters were added to the AP1000 design even though they are not credited in the design basis.

Design Control Document (DCD) Revision:

None

PRA Revision:

None

Technical Report (TR) Revision:

Table B-1 of Appendix B of the DAS TR (APP-GW-GLR-145) will be updated in Revision 2 to include the reasoning behind installation of hydrogen igniters. Markup submitted separately.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.8-DAS-08
Revision: 0

Question:

WCAP-17184-P, Appendix B, lists "ADS" as the "system manually actuated by DAS." Explain the specific manual operator actions this includes. Explain why these actions are not credited DAS manual operator actions and/or DAS automatic actions. Provide the design basis for the inclusion.

10 CFR Part 50, Appendix A, GDC 22, requires, in part, that design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protective function. Branch Technical Position HICB19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," Revision 4 (BTP-7-19), states that where operator action is cited as the diverse means for response to an event, the applicant should demonstrate that adequate information (indication) and sufficient time is available for operator action. The staff's review of WCAP-17184-P, Section 10.2.1.1, determined that the stated design descriptions do not provide an explanation of how manual actions are used in the DAS design beyond listing the manual actions. From the PRA evaluation there appears to be a 20 minute window for accomplishing this action. Therefore, the staff could not identify clear design basis descriptions that will permit sufficient understanding of credited DAS manual actuations and their conformance to the applicable regulatory requirements.

Westinghouse Response:

Both the current certified AP1000 design (DCD Revision 15) and in Revision 17 Tier 2, Chapter 16, Appendix B, Section 3.3.5, the Diverse Actuation System (DAS) manual controls provide non-Class 1E backup controls in case of common-mode failure of the Protection and Safety Monitoring System (PMS) automatic and manual actuations evaluated in the AP1000 PRA. These DAS manual controls are not credited for mitigating accidents in the DCD Chapter 15 (safety) analyses.

DAS manual actions are not "design basis" items as posited in this RAI. Probabilistic Risk Assessment (PRA) analytical techniques were used to provide insights as to the relative importance of DAS manual actions for beyond design basis occurrences. In no case does the failure to manually actuate a DAS function result in an unacceptable result using PRA analytical techniques. No DAS manual actuations are credited in the AP1000 Safety Analysis.

For this particular case, Westinghouse acknowledges that Appendix B to WCAP-17184-P needs to be clarified to explain the context of the manual actuation of "ADS."

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Design Control Document (DCD) Revision:

None

PRA Revision:

None

Technical Report (TR) Revision:

Appendix B of the DAS TR WCAP-17184 will be updated in Revision 2 to include clarification of the context of manual ADS actuation. See DAS TR mark ups (submitted separately).

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.8-DAS-09

Revision: 0

Question:

WCAP-17184-P, Appendix B, lists the DAS manual initiation of IRWST gravity injection. Explain why this action is not a credited DAS manual operator action and/or DAS automatic actuation. Provide the design basis for its inclusion.

10 CFR Part 50, Appendix A, GDC 22, requires, in part, that design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protective function. Branch Technical Position HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," Revision 4 (BTP-7-19), states that where operator action is cited as the diverse means for response to an event, the applicant should demonstrate that adequate information (indication) and sufficient time is available for operator action. The staff's review of WCAP-17184-P, Section 10.2.1.1, determined that the stated design descriptions do not provide an explanation of how manual actions are used in the DAS design beyond listing the manual actions. From the PRA evaluation there appears to be a 20 minute window for accomplishing this action. Therefore, the staff could not identify clear design basis descriptions that will permit sufficient understanding of credited DAS manual actuations and their conformance to the applicable regulatory requirements.

Westinghouse Response:

Both the current certified AP1000 design (DCD Revision 15) and in Revision 17 Tier 2, Chapter 16, Appendix B, Section 3.3.5, the Diverse Actuation System (DAS) manual controls provide non-Class 1E backup controls in case of common-mode failure of the Protection and Safety Monitoring System (PMS) automatic and manual actuations evaluated in the AP1000 PRA. These DAS manual controls are not credited for mitigating accidents in the DCD Chapter 15 (safety) analyses.

DAS manual actions are not "design basis" items as posited in this RAI. Probabilistic Risk Assessment (PRA) analytical techniques were used to provide insights as to the relative importance of DAS manual actions for beyond design basis occurrences. In no case does the failure to manually actuate a DAS function result in an unacceptable result using PRA analytical techniques. No DAS manual actuations are credited in the AP1000 Safety Analysis.

For this particular scenario, PRA analysis techniques show acceptable results even if the act of manually actuating IRWST gravity injection is not accomplished (operator fails to act with 100% certainty). For this reason, manual actuation of IRWST gravity injection is not a credited manual operator action nor is it required (or credited) for automatic operation. The 20 minute window as described in the PRA analysis cited in this RAI is for a beyond design basis event. This PRA

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

analysis was used to provide insights into this particular scenario. Out of an abundance of caution, the capability to manually actuate IRWST gravity injection from DAS was added to the AP1000 design even though it is not credited in the design basis.

Design Control Document (DCD) Revision:

None

PRA Revision:

None

Technical Report (TR) Revision:

Appendix B of the DAS TR WCAP-17184 will be updated in Revision 2 to include clarification of the reasoning behind providing for the manual initiation of IRWST gravity injection. See document mark up (submitted separately).

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.8-DAS-10
Revision: 0

Question:

Provide the design basis explaining why the DAS allowances for "Containment Temperature High" and "Pressurizer Water Level Low," stated in WCAP-17184-P, Revision 1, Appendix A, are outside of 1.15/2.

10 CFR Part 50, Appendix A, GDC 22, requires, in part, that design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protective function. GDC 10, requires, in part, that control and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences. Branch Technical Position HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," Revision 4 (BTP-7-19), states that where a common-mode failure is compensated by a different automatic function, a basis is provided which demonstrates that the different function constitutes adequate mitigation for the conditions of the event. In addition, BTP-7-19 states that assumptions made to compensate for missing information in the design description materials or to explain particular interpretations of the analysis guidelines as applied to the system are documented by the applicant. The applicant states in WCAP-17184-P that due to the DAS not being a Class 1 E system, a 75% probability / 75% confidence level is defined as the basis for determination of the random and independent terms of the square root sum of the squares (SRSS) calculation. The applicant applied 75% (1.15sigma) confidence level to the DAS systems and therefore the allowances of the DAS system are reduced to 1.15/2 from the PMS allowances. The staff could not identify design descriptions that would explain why several DAS allowances are outside of 1.15/2.

Westinghouse Response:

The changes are described in the marked-up DAS TR (submitted separately). The marked changes describe why the DAS channel statistical allowances for "Containment Temperature High" and "Pressurizer Water Level Low" do not conform to the typical ratio of $1.15\sigma/2\sigma$ when comparing a 75% probability / 75% confidence level to 95% probability / 95% confidence level for determination of the random and independent terms of the square root sum of the squares calculation. Additionally, a justification for the use of a 75% probability / 75% confidence level is provided. These changes include the addition of a note to the tables for both "Containment Temperature High" (page A-3) and "Pressurizer Water Level Low" (page A-6) in Appendix A, and a revision to the second paragraph of page A-1 of Appendix A.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Design Control Document (DCD) Revision:

None

PRA Revision:

None

Technical Report (TR) Revision:

None

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.8-DAS-11
Revision: 0

Question:

Remove discussion of cyber security from technical reports.

10 CFR 52.47 requires design certification applications to provide a level of design information sufficient to enable the Commission to reach a final conclusion on all safety questions associated with the design before the certification is granted. In WCAP-17184, Revision 1, and in WCAP-17179, "AP1000 Component Interface Module Technical Report," Revision 1, both discuss cyber security, which is addressed by 10 CFR 73.54. Since the evaluation of cyber security pertains to combined license applicants, and the staff's review of Chapter 7 of the AP1000 FSAR does not address cyber security, discussion of cyber security should be removed from the design certification. It is appropriate to point to plans for a secure development and operational environment for safety-related digital instrumentation and control systems, where it is deemed necessary.

Westinghouse Response:

Westinghouse will remove any reference to cyber security from existing documents related to design certification. The following documents are affected and will be revised:

- APP-GW-GLR-700 Revision 17, AP1000™ Design Control Document
- WCAP-17184, AP1000™ Diverse Actuation System Planning and Functional Design Summary Technical Report
- WCAP-17179, "AP1000™ Component Interface Module Technical Report
- WCAP-16675-P, AP1000™ Protection and Safety Monitoring System Architecture Technical Report

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Design Control Document (DCD) Revision:

Tier 2, Table 1.6-1

Table 1.6-1 (Sheet 12 of 20)		
MATERIAL REFERENCED		
DCD Section Number	Westinghouse Topical Report Number	Title
6A	WCAP-15846 (P) WCAP-15862	<u>W</u> GOthic Application to AP600 and AP1000, Revision 1, March 2004
	WCAP-14135 (P) WCAP-14138	Final Data Report for Passive Containment Cooling System Large Scale Test, Phase 2 and Phase 3, Revision 3, November 1998
	WCAP-15613 (P) WCAP-15706	AP1000 PIRT and Scaling Assessment Report, March 2001
7.1	[WCAP-14605 (P) WCAP-14606 (NP)]	<i>Westinghouse Setpoint Methodology for Protection Systems – AP600, April 1996</i> *
	WCAP-16361-P WCAP-16361-NP	Westinghouse Setpoint Methodology for Protection Systems - AP1000, May 2006
	WCAP-15775	AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report, March 2003
	[WCAP-16096-NP-A	<i>Software Program Manual for Common Q Systems, Revision 01A, January 2004</i> *
	[WCAP-16097-P-A WCAP-16097-NP-A	<i>Common Qualified Platform, Revision 01, May 2003</i> *
	WCAP-15776	Safety Criteria for the AP1000 Instrumentation and Control Systems, April 2002
	WCAP-16675-P WCAP-16675-NP	AP1000 Protection and Safety Monitoring System Architecture Technical Report, Revision 1
	APP-GW-GLR-017	AP1000 Standard Combined License Technical Report, Resolution of Common Q NRC Items

(P) Denotes Document is Proprietary

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

NABU-DP-00014-GEN (P) WCAP-15775	Design Process for Common Q Safety Systems, Revision 1, March 2006 Design Process for AP1000 Common Q Safety Systems, Revision 2, November 2008]*
	Westinghouse Electric Company Quality Management System (QMS), (Non-Proprietary), Revision 5, October 2002
APP-GW-GLR-104	AP1000 Cyber Security Implementation, May 2007
APP-GW-J0R-012	AP1000 Protection and Safety Monitoring System Computer Security Plan

7.1.1 The AP1000 Instrumentation and Control Architecture

Figure 7.1-1 illustrates the instrumentation and control architecture for the AP1000. The figure shows two major sections separated by the real-time data network. Figure 7.1-1 depicts the real-time data highway as a single network. ~~To meet cyber-computer security concerns, the real-time data highway will be separated into security levels as described in Reference 22.~~

The lower portion of the figure includes the plant protection, control, and monitoring functions. At the lower right-hand side is the protection and safety monitoring system. It performs the reactor trip functions, the engineered safety features (ESF) actuation functions, and the Qualified Data Processing (QDPS) functions. The I&C equipment performing reactor trip and ESF actuation functions, their related sensors, and the reactor trip switchgear are, for the most part, four-way redundant. This redundancy permits the use of bypass logic so that a division or individual channel out of service can be accommodated by the operating portions of the protection system reverting to a two-out-of-three logic from a two-out-of-four logic.

The ESF coincidence logic performs system-level logic calculations, such as initiation of the passive residual heat removal system. It receives inputs from the plant protection subsystem bistables and the main control room. The ESF actuation subsystems provide the capability for on-off control of individual safety-related plant loads. They receive inputs from the ESF coincidence logic, remote shutdown workstation and the main control room. The plant control system performs nonsafety-related instrumentation and control functions using both discrete (on/off) and modulating (analog) type actuation devices.

The nonsafety-related real-time data network, which horizontally divides Figure 7.1-1, is a high speed, redundant communications network that links systems of importance to the operator. Safety-related systems are connected to the network through gateways and qualified isolation devices so that the safety-related functions are not compromised by failures elsewhere. Plant protection, control, and monitoring systems feed real-time data into the network for use by the control room and the data display and processing system.

The upper portion of the figure depicts the control rooms and data display and processing system. The main control room is implemented as a set of compact operator consoles featuring color graphic displays and soft control input devices. The graphics are supported by a set of graphics workstations that take their input from the real-time data network. An advanced alarm system, implemented in a similar technology, is also provided.

The data display and processing (plant computer) system is implemented in a distributed architecture. The working elements of the distributed computer system are graphics workstations, although their graphics capability is secondary to their computing performance. The distributed computer system obtains its input from the real-time data network and delivers its output over the network to other users.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

WCAP-15775 (Reference 7) describes the diversity and defense-in-depth features of the AP1000 instrumentation and control architecture.

Protection and Safety Monitoring System

The protection and safety monitoring system provides detection of off-nominal conditions and actuation of appropriate safety-related functions necessary to achieve and maintain the plant in a safe shutdown condition. The protection and safety monitoring system controls safety-related components in the plant that are operated from the main control room or remote shutdown workstation. **Secure development and operational environments for the Protection and Safety Monitoring System are utilized during design as described in Reference 22.**

In addition, the protection and safety monitoring system provides the equipment necessary to monitor the plant safety-related functions during and following an accident as required by Regulatory Guide 1.97.

Special Monitoring System

The special monitoring system does not perform any safety-related or defense-in-depth functions. The special monitoring system consists of specialized subsystems that interface with the instrumentation and control architecture to provide diagnostic and long-term monitoring functions.

The special monitoring system is the metal impact monitoring system. The metal impact monitoring system detects the presence of metallic debris in the reactor coolant system when the debris impacts against the internal parts of the reactor coolant system. The metal impact monitoring system is composed of digital circuit boards, controls, indicators, power supplies and remotely located sensors and related signal processing devices. A minimum of two sensors are located at each natural collection region, connected to separate instrumentation channels, to maintain the impact monitoring function if a sensor fails in service. The metal impact monitoring system is described in subsection 4.4.6.4.

Plant Control System

The plant control system provides the functions necessary for normal operation of the plant from cold shutdown through full power. The plant control system controls nonsafety-related components in the plant that are operated from the main control room or remote shutdown workstation.

The plant control system contains nonsafety-related control and instrumentation equipment to change reactor power, control pressurizer pressure and level, control feedwater flow, and perform other plant functions associated with power generation. The plant control system is described in subsections 7.1.3 and 7.7.1.

Diverse Actuation System

The diverse actuation system is a nonsafety-related, diverse system that provides an alternate means of initiating reactor trip and actuating selected engineered safety features, and providing plant information to the operator. The diverse actuation system is described in subsection 7.7.1.11.

Operation and Control Centers System

The operation and control centers system includes the main control room, the technical support center, the remote shutdown room, emergency operations facility, local control stations and associated workstations for these centers. With the exception of the control console structures, the equipment in the control room is part of the other systems (for example, protection and safety monitoring system, plant control system, data display and processing system). The boundaries of the operation and control centers system for the main control room and the remote shutdown workstation are the signal interfaces with the plant components. These interfaces are via the plant protection and

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

safety monitoring system processor and logic circuits, which interface with the reactor trip and ESF plant components; the plant control system processor and logic circuits, which interface with the nonsafety-related plant components; and the plant real-time data network, which provides plant parameters, plant component status, and alarms.

Data Display and Processing System

The data display and processing system provides the equipment used for processing data that result in nonsafety-related alarms and displays for both normal and emergency plant operations, generating these displays and alarms, providing analysis of plant data, providing plant data logging and historical storage and retrieval, and providing operational support for plant personnel.

The data display and processing system also contains the real-time data network, which is a redundant data highway that links the elements of the AP1000 instrumentation and control architecture.

Incore Instrumentation System

The primary function of the incore instrumentation system is to provide a three-dimensional flux map of the reactor core. This map is used to calibrate neutron detectors used by the protection and safety monitoring system, as well as to optimize core performance. A secondary function of the incore instrumentation system is to provide the protection and safety monitoring system with the thermocouple signals necessary for the post-accident inadequate core cooling monitor. The incore instrument assemblies house both fixed incore flux detectors and core exit thermocouples. The incore instrumentation system is described in subsection 4.4.6.1.

Cyber Computer Security

~~Reference 22 describes the cyber computer security implementation for AP1000.~~

7.1.7 References

22. APP-GW-GLR-104J0R-012, "AP1000 Protection and Safety Monitoring System Computer Security Plan, ~~Cyber Security Implementation,~~" Westinghouse Electric Company LLC.

PRA Revision:

None

Technical Report (TR) Revision:

- APP-GW-GLR-700 Revision 17, AP1000™ Design Control Document
- WCAP-17184, AP1000™ Diverse Actuation System Planning and Functional Design Summary Technical Report
- WCAP-17179, "AP1000™ Component Interface Module Technical Report
- WCAP-16675-P, AP1000™ Protection and Safety Monitoring System Architecture Technical Report

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.8-DAS-12
Revision: 0

Question:

Provide a description in Chapter 7 of the AP1000, Tier 2, FSAR regarding completion of the Inspection, Tests, Analysis, and Acceptance Criteria (ITAAC) found in Tier 1.

10 CFR 52.47 requires design certification applications to provide a level of design information sufficient to enable the Commission to reach a final conclusion on all safety questions associated with the design before the certification is granted. In the proposed amendment to the AP1000 design control document, Tier 1, Items 4a and 4b are removed based on design work accomplished. Chapter 7 of the AP1000, Tier 2, FSAR, should provide a summary and justification for why the ITAAC found in Item 4a and 4b of AP1000, Tier 1, Table 2.5.1-4, can be removed.

Westinghouse Response:

The AP1000™ Diverse Actuation System is developed using a planned design process which provides for specific design documentation during the following life cycle stages:

- a) Design Requirements Phase
- b) System Definition Phase

The planned design process for the Design Requirements and System Definition Phases will be added to the AP1000™ Design Control Document, APP-GW-GL-700.

In addition, an ITTAC will be added that describes the Design Commitment, ITA, and Acceptance Criteria for DAS manual actuation.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Design Control Document (DCD) Revision:

Tier 1, 2.5.1 Diverse Actuation System

Table 2.5.1-4 Inspections, Tests, Analyses, and Acceptance Criteria		
Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
5. The DAS manual actuation of ADS, IRWST injection, and containment recirculation can be executed correctly and reliably.	An evaluation to confirm that the operator actions can be performed within the specified times.	b) A report exists and concludes that DAS manual operator action verification was conducted.

Tier 2

1.6 Material Referenced – Table 1.6-1

DCD Section # 7.1

WCAP-15775	AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report, March 2003
------------	---

DCD Section #7.7

WCAP-17184-P	AP1000™ Diverse Actuation System Planning and Functional Design Summary Technical Report
--------------	--

7.1.7 References

7. WCAP-15775, **Revision 2**, “AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report,” **March 2003**

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

23. WCAP-17184-P, AP1000™ Diverse Actuation System Planning and Functional Design Summary Technical Report

7.7.1.11 Diverse Actuation System

The diverse actuation system is a nonsafety-related system that provides a diverse backup to the protection system. This backup is included to reduce the probability of a severe accident which potentially results from the unlikely coincidence of postulated transients and postulated common mode failure in the protection and control systems.

The protection and safety monitoring system is designed to prevent common mode failures. However, in the low probability case where a common mode failure does occur, the diverse actuation system provides diverse protection. The specific functions performed by the diverse actuation system are selected based on the PRA evaluation. The diverse actuation system functional requirements are based on an assessment of the protection system instrumentation common mode failure probabilities combined with the event probability.

The functional logic for the diverse actuation system is shown in Figure 7.2-1, sheets 19 and 20.

The DAS is developed using a planned design process which provides for specific design documentation during the following life cycle stages:

- a) Design Requirements Phase
- b) System Definition Phase

These life cycle stages are completed by developing a number of specific design documents. The following documents are developed to address the Design Requirements and System Definition Phases:

- WCAP-17184-P, AP1000™ Diverse Actuation System Planning and Functional Design Summary Technical Report, including Appendix A DAS Setpoint Methodology Description and Appendix B PRA Performance Requirements Associated with DAS Manual Actuation.

The DAS Technical Report identifies the DAS architecture and associated licensing basis at the functional design level. The overall DAS detailed design is not identified in the report. Select design details are identified only for the purpose of architectural completeness or licensing compliance. The content of this report is to cover SRP 7.8. Appendix A of the Technical Report describes the DAS setpoint methodology and to provide a representative basis for DAS nominal trip setpoints. Appendix B addresses operator actions taken through DAS that are modeled in the AP1000™ Probabilistic Risk Assessment (PRA). These manual actions are not required to mitigate design basis accidents but instead are modeled in the PRA to provide insights into sequences that involve multiple failures. This appendix lists the

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

operator actions used in the PRA for manual DAS actions from the control room DAS actuation panel.

- WCAP-15775, AP1000™ Instrumentation and Control Defense-in-Depth and Diversity Report

Diversity is a principle in instrumentation of sensing different variables, using different technology, using different logic or algorithms, or using different actuation means to provide different ways of responding to postulated plant conditions. NUREG/CR-6303 segregates the types of diversity into six different areas: human, design, software, functional, signal, and equipment. The AP1000™ Instrumentation and Control Defense-in-Depth and Diversity Report describes the type of diversity that exists among the four echelons of defense for AP1000 and identifies dependencies among the echelons.

A number of additional design process documents are submitted to the USNRC for review and audit. They include:

1. AP1000™ Diverse Actuation System Logic Drawings”
2. AP1000™ Diverse Actuation System Sub-System Requirements”
3. DAS Requirements Traceability Report

PRA Revision:

None

Technical Report (TR) Revision:

None

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.8-DAS-13
Revision: 0

Question:

Correct the following issues pertaining to WCAP-17184, Revision 1.

- Section 6.1.2.2 references the Wolf Creek license amendment request regarding self-tests features of the DAS. However, the license amendment request is not part of the AP1000 licensing basis. Therefore, self-test features should be identified in the WCAP.
- The statement in Section 8.1 should be modified as it currently says that the “two-out-of-two logic ... lends itself to reliability.” However, this configuration is less reliable as compared to a single train configuration.
- Remove the two statements in Section 8.1 that *“The use of FPGAs results in a hardware-based design that is not subject to software common cause failures. The only software involved in the process is that used to burn-in the required logic design into the FPGA.”*

10 CFR 52.47 requires design certification applications to provide a level of design information sufficient to enable the Commission to reach a final conclusion on all safety questions associated with the design before the certification is granted. During the review of WCAP-17184, Revision 1, the staff identified issues with the bullet points above that should be corrected for technical and regulatory accuracy.

Westinghouse Response:

The three issues related to WCAP-17184 will be addressed in Revision 2 of the WCAP. The change pages are provided in this RAI response.

Design Control Document (DCD) Revision:

None

PRA Revision:

None

Technical Report (TR) Revision:

WCAP-17184, Revision 2

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

WCAP-17184-P
APP-GW-GLR-145

WESTINGHOUSE PROPRIETARY CLASS 2

AP1000

Typical self-tests include monitoring memory and memory reference integrity, using watchdog timers or processors, monitoring communication channels, monitoring central processing unit status, and checking data integrity.

Self-test functions should be verified during periodic functional tests.

Surveillance Testing

Systems should be able to conduct periodic surveillance testing consistent with the technical specifications and plant procedures. As delineated in Regulatory Guide 1.118, periodic testing consists of functional tests and checks, calibration verification, and time response measurements.

Actions on Failure Detection

The design should have either the automatic or manual capability to take compensatory action on detection of any failed or inoperable component. The design capability and plant technical specifications, operating procedures, and maintenance procedures should be consistent with each other.

6.1.2.2 DAS Applicability

Failure Detection

~~[Previously, the NRC staff has reviewed the failure detection and self test features of the Wolf Creek application of the ALS platform in Docket 50-482, Amendment 181 to License No. NPF 42, and determined that these features have been satisfactorily addressed within the development (ADAMS Accession No. ML090610317). The approach to failure detection and self test features will be fundamentally the same as the approach that was reviewed in this NRC review.]~~

The ALS platform incorporates failure detection and isolation techniques. The operation of the system is deterministic in nature and allows the system to monitor itself in order to validate its functional performance. The ALS platform incorporates self-diagnostic features that provide a means to detect and alarm failures within the platform. These failures include:

- Synchronization faults
- FPGA device defects
- External circuitry defects
- Noise related issues on communication lines
- Read or Write transaction failures on ALS buses.

In addition, application logic diagnostics are provided. These diagnostic are determined during the design implementation phase.]^{a,c}

Self-Test Features

The short term availability controls and technical specifications are platform neutral, [and therefore specific ALS fault diagnostics and fault test features are not references in the short term availability

Revision 1

6-2

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

WCAP-17184-P
APP-GW-GLR-145

WESTINGHOUSE PROPRIETARY CLASS 2

AP1000

8 RELIABILITY AND AVAILABILITY

8.1 RELIABILITY

The DAS employs an energize-to-actuate, two-out-of-two logic, which ~~leads~~ provides itself to reliability that is consistent with the PRA. The two-out-of-two logic reduces complexity of the system, making manufacturing and verification and validation easier, and therefore increasing the hardware reliability of the system. The two-out-of-two logic also facilitates simplicity by reducing the number of sensors and circuit complexity. A simpler circuit (less-complex) is also less prone to hardware failure. ~~more reliable~~.

The following is a summary of the analyses that will occur for the DAS during the detailed design phase.

An FMEA is a systematic, inductive reasoning process that determines the role of each component of an I&C system in achieving the overall system dependability goals. The FMEA will establish the qualitative reliability of the DAS and the information gained will be used to develop an analysis report. The report will be used to provide licensing support to prove the DAS meets and/or exceeds the reliability goals set for the system.

The DAS also has quantitative reliability goals and availability goals that must be measured. Since the DAS uses simpler functions, a reliability block diagram analysis will be used to determine the overall system function availability. The FMEA will be used as a guide for the analysis to determine the important system functions that need to be illustrated in the analysis. The reliability block diagram analysis will be used to estimate the functional availability and failure rates for the DAS. The results of this analysis may also be used to support licensing.

In order to perform the reliability block diagram analysis, the predicted failure rates of the various elements that make up the system are needed. A Mean Time Between Failure (MTBF) analysis will be performed on all major components of the system and will be documented in a bill of materials which lists the elements applied in the DAS, along with the estimated failure rates. The failure rates can be determined from a combination of sources such as MIL-HDBK-217F component failure models per field data, manufacturer data sheets or engineering judgment.

Once the FMEA, MTBF, and reliability block diagram analysis have been performed, the data will be used to support a maintainability analysis. The maintainability analysis will divide the DAS elements into a number of classes that share similar attributes. For each class, a checklist will be applied in each of the listed repair activities to assist in the characterization of typical durations for the activity. The durations will then be used to estimate an overall mean time to repair that will provide important input to determine the optimum number of spares to have on hand at the site. A DAS report will be prepared to support quantitative analysis as well as provide the utility valuable information for risk-informed decisions in the I&C maintenance area.

The DAS detailed design is not finalized at this time. However, sufficient detail about the DAS design (arrangement and hardware) is available to allow a reasonable estimate of its reliability. The reliability analysis herein is based on the preliminary DAS design as identified above. "CS Innovations" has been designated as the platform vendor. Except for relays, component quantities are considered representative of the final design. Total number of relays may vary $\pm 10\%$ of the total quantity specified in this analysis.

Revision 1

8-1

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

WCAP-17184-P
APP-GW-GLR-145

WESTINGHOUSE PROPRIETARY CLASS 2

AP1000.

[The CS Innovations (CSI) Advanced Logic System (ALS) platform uses Field Programmable Gate Array (FPGA) technology. ~~The use of FPGAs results in a hardware-based design that is not subject to software common cause failures. The only software involved in the process is that used to burn in the required logic design into the FPGA.~~ The logic in the FPGA is then checked for validity. The FPGA is then considered a hardware-based component, thus not requiring software for it to provide its function.

However, FPGA-based systems employ software tools to configure and test the resulting customized circuitry. Therefore, the CSI life cycle is based on BTP 7-14. The CSI life cycle process is discussed in Section 1, "AP1000™ DAS Design Process."

Signal conditioning equipment is shared between manual and automatic DAS. Associated failure rates of utilized components in the design are assigned to both manual and automatic DAS subsystems. The components used will be of quality sufficient to support the required reliability of the system. Cabling, connectors and terminals are not modeled, their contributions to the overall reliability are considered insignificant.

In addition, the DAS contains a RT interface and a squib valve interface that will require a Sneak Circuit Analysis (SCA). An SCA is used to identify a latent path or condition in a system potentially resulting in unexpected operational modes that are not caused by component failures but are due to design oversight. The SCA is a China contractual obligation used to identify the adequacy of the design.]^{a,c}

8.2 AVAILABILITY

[The design goal for DAS unavailability is 1E-02 per demand for each of the automatic and manual actuation functions performed by the DAS. This value includes the unavailability for test and maintenance. The preliminary calculation of the DAS probability values derived in this analysis are significantly better (Automatic DAS = 6.74E-04 and Manual DAS = 1.32E-03 considering a mission time of 24 hours is realized).]^{a,c}

Revision 1

8-2

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

RAI Response Number: RAI-SRP7.1-FMEA-06

Revision: 1

Question:

Discuss in the FMEA what methods (alarms, indications, testing, etc.) or design features are utilized to ensure the condition of a checksum failure that potentially prevents actuation of a division will not will not act as an undetected fault.

On page 2-14 of Revision 2 of the "Failure Modes and Effects Analysis (FMEA) of the AP1000 Protection and Safety Monitoring System" (PMS) it states: [

] ^{a,c}

Clause 5.1, the Single Failure Criterion, of IEEE Std. 603-1991, which is endorsed by 10 CFR 50.55a(h) Protection and Safety Systems states that IEEE Std. 379-1988, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems, provides guidance on the application of single failures. Per the definitions section of IEEE Std. 603-1991, it states IEEE Std. 379-1988 defines identifiable, but non-detectable failures within Section 5.2 and states that the non-detectable failures should either be designed out of the system or presumed to have occurred yet have no impact upon the system's ability to initiate and complete its safety function should it be required. Discuss how the checksum failure fault will be minimized; mitigated or eliminated from the PMS.

Westinghouse Response:

The case in point involves setpoint changes [

] ^{a,c}

NRC Comment from 6/15/10 Meeting:

The system of the primary and secondary setpoint change process check. For the primary, the setpoint won't change, but for the secondary, note that an alarm is available.

AP1000 TECHNICAL REPORT REVIEW

Response to Request For Additional Information (RAI)

Westinghouse Rev 1 Response:

The case in point involves setpoint changes [

] ^{a,c}

DCD Revision: None

PRA Revision: None

Technical Report (TR) Revision: None