

June 15, 2021

Docket Nos.: 52-025
52-026

ND-21-0486
10 CFR 50.71(e)
10 CFR 52 App. D, Section X.B.2

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

**Southern Nuclear Operating Company
Vogtle Electric Generating Plant Units 3 and 4
Updated Final Safety Analysis Report, Tier 1, Technical Requirements Manual and
Technical Specifications Bases Annual Submittal**

Ladies and Gentlemen:

This submittal is made with regard to Vogtle Electric Generating Plant, Units 3 and 4 (VEGP 3&4), license numbers NPF-91 and NPF-92, respectively, pursuant to the reporting requirements of 10 CFR 50.71(e) and 10 CFR Part 52, Appendix D, Section X.B.2.

Southern Nuclear Operating Company (SNC) hereby submits the following documents:

- VEGP 3&4 Updated Final Safety Analysis Report (UFSAR), Revision 10, including:
 - Incorporated by Reference (IBR) document APP-GW-J0R-012, Revision 5
 - IBR document WCAP-15775, Revision 8
 - IBR document WCAP-15871, Revision 7
 - IBR document WCAP-15927-P Revision 8
 - WCAP-15927-NP, Revision 8 [Non-proprietary version of WCAP-15927, Revision 8]
 - IBR document WCAP-16674-P Revision 9
 - WCAP-16674-NP, Revision 9 [Non-proprietary version of WCAP-16674, Revision 9]
 - IBR document WCAP-16675-P Revision 10
 - WCAP-16675-NP, Revision 10 [Non-proprietary version of WCAP-16675, Revision 10]
 - IBR document WCAP-17179-P Revision 6
 - WCAP-17179-NP, Revision 6 [Non-proprietary version of WCAP-17179, Revision 6]
- VEGP 3&4 Tier 1, Revision 9
- Vogtle Units 3 and 4 Technical Requirements Manual (TRM), Revision 18
- Vogtle Units 3 and 4 Technical Specifications (TS) Bases, Revision 68

The VEGP 3&4 UFSAR, VEGP 3&4 Tier 1, the Vogtle Units 3 and 4 TRM, and the Vogtle Units 3 and 4 TS Bases include the effects of plant-specific departures and changes through April 20, 2021.

The VEGP 3&4 UFSAR includes plant-specific Design Control Document (PS DCD) Tier 2 and Tier 2* information and site-specific and standard content. The VEGP 3&4 UFSAR includes colored text as a user's aid in identifying the origin of the text. A formatting legend is provided at the bottom of the Table of Contents page for each chapter. The VEGP 3&4 Tier 1 is also part of the PS DCD. In addition, the Vogtle Units 3 and 4 TRM contains Tier 2 information previously included in the VEGP 3&4 UFSAR, Section 16.3, Investment Protection, and is therefore considered part of the VEGP 3&4 PS DCD. The Vogtle Units 3 and 4 TRM is incorporated by reference into the VEGP 3&4 UFSAR.

The Vogtle Units 3 and 4 TS Bases is also provided with this submittal, in accordance with Vogtle Units 3 and 4 TS 5.5.6, TS Bases Control Program.

The Nuclear Development Quality Assurance Manual (NDQAM) Version 21.0, which is incorporated by reference into the UFSAR, was previously provided to the NRC on December 30, 2020 by SNC Letter ND-20-1415 [ADAMS Accession Number ML20365A058], in accordance with 10 CFR 50.71(e) and 10 CFR 50.55(f)(4).

This letter and all enclosures are submitted via digital virtual disc (DVD) in portable document format (PDF) due to the size of the submittal. Each DVD is appropriately labeled with material contained therein.

Enclosure 1 contains the complete VEGP 3&4 UFSAR and VEGP 3&4 Tier 1. Appropriate pre-submission checks have been performed on the files to ensure compliance with the NRC Guidance for Electronic Submissions.

Within Enclosure 1, the VEGP 3&4 UFSAR and VEGP 3&4 Tier 1 contain **Sensitive Unclassified Non-Safeguards Information (SUNSI), Security-Related Information and Proprietary information; therefore, SNC requests that these documents be withheld from public disclosure under 10 CFR 2.390(d).**

Enclosure 2 contains the list of VEGP 3&4 UFSAR and VEGP 3&4 Tier 1 figures and sections that contain Security-Related Information or Proprietary information.

Enclosure 3 contains the public version of the VEGP 3&4 UFSAR and VEGP 3&4 Tier 1. The public version of the VEGP UFSAR and VEGP 3&4 Tier 1 is redacted and withholds the Security-Related Information and Proprietary information provided in Enclosure 1 as identified by Enclosure 2. Enclosure 3 also contains the Vogtle Units 3 and 4 TRM and the Vogtle Units 3 and 4 TS Bases, which do not contain Security-Related Information or Proprietary information.

Enclosure 4 provides the SNC affidavit for withholding additional proprietary information contained in UFSAR Appendix 7B of Enclosure 1. SNC requests that the proprietary information contained in VEGP 3&4 UFSAR Appendix 7B continue to be withheld from public disclosure pursuant to 10 CFR 2.390.

Enclosure 5 provides the Westinghouse affidavit CAW-19-4876 for withholding proprietary information contained in Appendix 7B of Enclosure 1.

Enclosure 6 contains the IBR Document, APP-GW-J0R-012, "Protection and Safety Monitoring System Computer Security Plan," Revision 5, in PDF. Enclosure 6 contains **Security-Related Information; therefore, SNC requests that this document be withheld from public disclosure under 10 CFR 2.390(d).** Enclosure 6 is requested to be withheld in its entirety due to

Security-Related information, therefore there is no public version of Enclosure 6. The information contained in Enclosure 6 is owned by Westinghouse Electric Company; therefore, Enclosure 7 provides Affidavit CAW-20-5089, executed by Westinghouse Electric Company for withholding proprietary information contained in Enclosure 6, APP-GW-J0R-012, Revision 5. The Affidavit sets forth the basis on which the identified proprietary information in Enclosure 6 may be withheld from public disclosure by the Nuclear Regulatory Commission ("Commission") and addresses with specificity the considerations listed in paragraph (b)(4) of Section 2.390 of the Commission's regulations. Accordingly, it is respectfully requested that the information that is proprietary to Westinghouse be withheld from public disclosure in accordance with 10 CFR Section 2.390 of the Commission's regulations. Correspondence with respect to the copyright or proprietary aspects of the items listed above or the supporting Westinghouse Affidavit should reference CAW-20-5089 and should be addressed to Michael M. Corletti, Adv Analysis & Risk App, Westinghouse Electric Company, 1000 Westinghouse Drive, Suite 165, Cranberry Township, Pennsylvania 16066.

Enclosure 8 contains the IBR Document, WCAP-15775, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report," Revision 8, in PDF. WCAP-15775 does not include proprietary or security-related information and may be made available to the public.

Enclosure 9 contains the IBR Document, WCAP-15871, "AP1000 Assessment Against NFPA 804," Revision 7, in PDF. WCAP-15871 does not include proprietary or security-related information and may be made available to the public.

Enclosure 10 contains the IBR document, WCAP-15927-P, "Design Process for AP1000 Common Q Safety Systems," Revision 8, in PDF. Enclosure 10 contains **Proprietary information; therefore, SNC requests that this document be withheld from public disclosure under 10 CFR 2.390(d)**. Enclosure 11 contains the public version of WCAP-15927-P (WCAP-15927-NP) in PDF. The information contained in Enclosure 10 is owned by Westinghouse Electric Company; therefore, Enclosure 12 provides Affidavit CAW-20-5088, executed by Westinghouse Electric Company for withholding proprietary information contained in Enclosure 10, WCAP-15927-P, Revision 8. The Affidavit sets forth the basis on which the identified proprietary information in Enclosure 10 may be withheld from public disclosure by the Nuclear Regulatory Commission ("Commission") and addresses with specificity the considerations listed in paragraph (b)(4) of Section 2.390 of the Commission's regulations. Accordingly, it is respectfully requested that the information that is proprietary to Westinghouse be withheld from public disclosure in accordance with 10 CFR Section 2.390 of the Commission's regulations. Correspondence with respect to the copyright or proprietary aspects of the items listed above or the supporting Westinghouse Affidavit should reference CAW-20-5088 and should be addressed to Michael M. Corletti, Adv Analysis & Risk App, Westinghouse Electric Company, 1000 Westinghouse Drive, Suite 165, Cranberry Township, Pennsylvania 16066.

Enclosure 13 contains the IBR document, WCAP-16674-P, "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components," Revision 9, in PDF. Enclosure 13 contains **Proprietary information; therefore, SNC requests that this document be withheld from public disclosure under 10 CFR 2.390(d)**. Enclosure 14 contains the public version of WCAP-16674-P (WCAP-16674-NP) in PDF. The information contained in Enclosure 13 is owned by Westinghouse Electric Company; therefore, Enclosure 15 provides Affidavit CAW-19-4950, executed by Westinghouse Electric Company for withholding proprietary information contained in Enclosure 13, WCAP-16674-P, Revision 9. The Affidavit sets forth the basis on which the identified proprietary information in Enclosure 13 may be withheld from public disclosure by the Nuclear Regulatory Commission ("Commission") and addresses with specificity the considerations listed in paragraph (b)(4) of Section 2.390 of the Commission's regulations.

Accordingly, it is respectfully requested that the information that is proprietary to Westinghouse be withheld from public disclosure in accordance with 10 CFR Section 2.390 of the Commission's regulations. Correspondence with respect to the copyright or proprietary aspects of the items listed above or the supporting Westinghouse Affidavit should reference CAW-19-4950 and should be addressed to Michael M. Corletti, Adv Analysis & Risk App, Westinghouse Electric Company, 1000 Westinghouse Drive, Suite 165, Cranberry Township, Pennsylvania 16066.

Enclosure 16 contains the IBR document, WCAP-16675-P, "AP1000 Protection and Safety Monitoring System Architecture Technical Report," Revision 10, in PDF. Enclosure 16 contains **Proprietary information; therefore, SNC requests that this document be withheld from public disclosure under 10 CFR 2.390(d)**. Enclosure 17 contains the public version of WCAP-16675-P (WCAP-16675-NP) in PDF. The information contained in Enclosure 16 is owned by Westinghouse Electric Company; therefore, Enclosure 12 provides Affidavit CAW-20-5088, executed by Westinghouse Electric Company for withholding proprietary information contained in Enclosure 16, WCAP-16675-P, Revision 10. The Affidavit sets forth the basis on which the identified proprietary information in Enclosure 16 may be withheld from public disclosure by the Nuclear Regulatory Commission ("Commission") and addresses with specificity the considerations listed in paragraph (b)(4) of Section 2.390 of the Commission's regulations. Accordingly, it is respectfully requested that the information that is proprietary to Westinghouse be withheld from public disclosure in accordance with 10 CFR Section 2.390 of the Commission's regulations. Correspondence with respect to the copyright or proprietary aspects of the items listed above or the supporting Westinghouse Affidavit should reference CAW-20-5088 and should be addressed to Michael M. Corletti, Adv Analysis & Risk App, Westinghouse Electric Company, 1000 Westinghouse Drive, Suite 165, Cranberry Township, Pennsylvania 16066.

Enclosure 18 contains the IBR document, WCAP-17179-P, "AP1000 Component Interface Module Technical Report," Revision 6, in PDF. Enclosure 18 contains **Proprietary information; therefore, SNC requests that this document be withheld from public disclosure under 10 CFR 2.390(d)**. Enclosure 19 contains the public version of WCAP-17179-P (WCAP-17179-NP) in PDF. The information contained in Enclosure 18 is owned by Westinghouse Electric Company; therefore, Enclosure 20 provides Affidavit CAW-20-5095, executed by Westinghouse Electric Company for withholding proprietary information contained in Enclosure 18, WCAP-17179-P, Revision 6. The Affidavit sets forth the basis on which the identified proprietary information in Enclosure 18 may be withheld from public disclosure by the Nuclear Regulatory Commission ("Commission") and addresses with specificity the considerations listed in paragraph (b)(4) of Section 2.390 of the Commission's regulations. Accordingly, it is respectfully requested that the information that is proprietary to Westinghouse be withheld from public disclosure in accordance with 10 CFR Section 2.390 of the Commission's regulations. Correspondence with respect to the copyright or proprietary aspects of the items listed above or the supporting Westinghouse Affidavit should reference CAW-20-5095 and should be addressed to Michael M. Corletti, Adv Analysis & Risk App, Westinghouse Electric Company, 1000 Westinghouse Drive, Suite 165, Cranberry Township, Pennsylvania 16066.

U.S. Nuclear Regulatory Commission
ND-21-0486
Page 5 of 9

This letter contains no NRC commitments.

If you have any questions regarding this letter, please contact Ms. Amy Chamberlain at (205) 992- 6361.

I declare under penalty of perjury that the foregoing is true and correct. Executed on the 15th of June, 2021.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Brian H. Whitley", is written over a solid horizontal line.

Brian H. Whitley
Regulatory Affairs Director
Southern Nuclear Operating Company

Enclosures:

1. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, DVD containing:
VEGP 3&4 UFSAR, Revision 10
VEGP 3&4 Tier 1, Revision 9
[Note: VEGP 3&4 UFSAR and VEGP 3&4 Tier 1 Contain SUNSI Security-Related Information and Proprietary Information – Withhold from Public Disclosure Under 10 CFR 2.390(d)]
2. Vogtle Electric Generating Plant (VEGP) Units 3 and 4,
List of VEGP 3&4 UFSAR and VEGP 3&4 Tier 1 Figures and Sections Containing
Security-Related Information or Proprietary Information
3. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, DVD containing:
VEGP 3&4 UFSAR, Revision 10 (Public Version)
VEGP 3&4 Tier 1, Revision 9 (Public Version)
Vogtle Units 3 and 4 TRM, Revision 18
Vogtle Units 3 and 4 TS Bases, Revision 68
4. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, Affidavit from Southern Nuclear
Operating Company for Withholding Under 10 CFR 2.390
(Updated Final Safety Analysis Report, Tier 1, Technical Requirements Manual and
Technical Specifications Bases Annual Submittal)
5. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, Westinghouse Electric Company
Application for Withholding Proprietary Information from Public Disclosure and
Accompanying Affidavit CAW-19-4876
6. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, APP-GW-J0R-012, “Protection and
Safety Monitoring System Computer Security Plan,” Revision 5
**[Note: APP-GW-J0R-012 contains Security-Related Information – Withhold from Public
Disclosure Under 10 CFR 2.390(d)]**
7. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, Westinghouse Electric Company
Application for Withholding Proprietary Information from Public Disclosure and
Accompanying Affidavit CAW-20-5089.
8. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, WCAP-15775, “AP1000
Instrumentation and Control Defense-in-Depth and Diversity Report,” Revision 8
9. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, WCAP-15871, “AP1000 Assessment
Against NFPA 804,” Revision 7
10. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, WCAP-15927-P, “Design Process
for AP1000 Common Q Safety Systems,” Revision 8
**[Note: WCAP-15927-P contains Proprietary Information – Withhold from Public
Disclosure Under 10 CFR 2.390(d)]**

11. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, WCAP-15927-NP, "Design Process for AP1000 Common Q Safety Systems," Revision 8
[Non-proprietary version of WCAP-15927-P, Revision 8]
12. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, Westinghouse Electric Company Application for Withholding Proprietary Information from Public Disclosure and Accompanying Affidavit CAW-20-5088.
13. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, WCAP-16674-P, "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components," Revision 9
[Note: WCAP-16674-P contains Proprietary Information – Withhold from Public Disclosure Under 10 CFR 2.390(d)]
14. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, WCAP-16674-NP, "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components," Revision 9
[Non-proprietary version of WCAP-16674-P, Revision 9]
15. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, Westinghouse Electric Company Application for Withholding Proprietary Information from Public Disclosure and Accompanying Affidavit CAW-19-4950.
16. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, WCAP-16675-P, "AP1000 Protection and Safety Monitoring System Architecture Technical Report," Revision 10
[Note: WCAP-16675-P contains Proprietary Information – Withhold from Public Disclosure Under 10 CFR 2.390(d)]
17. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, WCAP-16675-NP, "AP1000 Protection and Safety Monitoring System Architecture Technical Report," Revision 10
[Non-proprietary version of WCAP-16675-P, Revision 10]
18. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, WCAP-17179-P, "AP1000 Component Interface Module Technical Report," Revision 6
[Note: WCAP-17179-P contains Proprietary Information – Withhold from Public Disclosure Under 10 CFR 2.390(d)]
19. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, WCAP-17179-NP, "AP1000 Component Interface Module Technical Report," Revision 6
[Non-proprietary version of WCAP-17179-P, Revision 6]
20. Vogtle Electric Generating Plant (VEGP) Units 3 and 4, Westinghouse Electric Company Application for Withholding Proprietary Information from Public Disclosure and Accompanying Affidavit CAW-20-5095.

cc: (All without enclosures, except as noted)

Southern Nuclear Operating Company / Georgia Power Company

Mr. S. E. Kuczynski

Mr. P. P. Sena III

Mr. M. D. Meier

Mr. G. Chick

Mr. S. Stimac

Mr. P. Martino

Mr. D. L. McKinney

Mr. T. W. Yelverton

Mr. B. Whitley

Mr. W. Levis

Ms. C. A. Gayheart

Ms. M. Ronnlund

Mr. J. DeLano

Mr. M. J. Yox

Mr. C. T. Defnall

Ms. A. C. Chamberlain

Mr. S. Leighty

Ms. K. Roberts

Mr. J. Haswell

Mr. K. Warren

Mr. A. S. Parton

Document Services RTYPE: VND.LI.L00 (with enclosures, without DVDs)

File AR.01.02.06

Nuclear Regulatory Commission

Mr. M. King

Mr. G. Bowman

Ms. M. Bailey

Ms. A. Veil

Mr. G. Khouri

Mr. B. Armstrong

Mr. C. Patel

Mr. C. Santos (with enclosures)

Mr. B. Kemker (with enclosures)

Mr. J. Eargle

Mr. C. J. Even

Ms. N. C. Coovert

Mr. C. Welch

Mr. J. Gaslevic

Mr. M. Webb

Mr. B. Gleaves

Mr. T. Fredette

Ms. K. McCurry

Mr. B. Davis

Mr. J. Parent

Mr. B. Grimman

U.S. Nuclear Regulatory Commission
ND-21-0486
Page 9 of 9

State of Georgia
Mr. R. Dunn

Oglethorpe Power Corporation
Mr. B. Brinkman
Mr. E. Rasmussen

Municipal Electric Authority of Georgia
Mr. J. E. Fuller
Mr. S. M. Jackson

Dalton Utilities
Mr. T. Bundros

Westinghouse Electric Company, LLC
Mr. L. Oriani
Mr. Z. Harper
Mr. M. Corletti

Other
Mr. S. W. Kline, Bechtel Power Corporation
Ms. L. A. Matis, Tetra Tech NUS, Inc.
Dr. W. R. Jacobs, Jr., Ph.D., GDS Associates, Inc.
Mr. S. Roetger, Georgia Public Service Commission
Mr. R. L. Trokey, Georgia Public Service Commission
Mr. K. C. Greene, Troutman Sanders
Mr. S. Blanton, Balch Bingham

Southern Nuclear Operating Company

ND-21-0486

Enclosure 1

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

DVD containing:

**VEGP 3&4 UFSAR, Revision 10
VEGP 3&4 Tier 1, Revision 9**

[Note: VEGP 3&4 UFSAR and VEGP 3&4 Tier 1 Contain SUNSI Security-Related Information and Proprietary Information - Withhold Under 10 CFR 2.390(d)]

List of Files Contained in DVD

VEGP3&4_UFSAR_CHAP01
VEGP3&4_UFSAR_CHAP02_SEC02.00-02.04
VEGP3&4_UFSAR_CHAP02_SEC02.04A
VEGP3&4_UFSAR_CHAP02_SEC02.04B
VEGP3&4_UFSAR_CHAP02_SEC02.05 PART 1
VEGP3&4_UFSAR_CHAP02_SEC02.05 PART 2
VEGP3&4_UFSAR_CHAP02_SEC02.05 PART 3
VEGP3&4_UFSAR_CHAP02_SEC02.05A-02.05E
VEGP3&4_UFSAR_CHAP03_SEC03.01-03.07
VEGP3&4_UFSAR_CHAP03_SEC03.08
VEGP3&4_UFSAR_CHAP03_SEC03.09-03F
VEGP3&4_UFSAR_CHAP03_SEC03G-03GG
VEGP3&4_UFSAR_CHAP03_SEC03H-03I
VEGP3&4_UFSAR_CHAP04
VEGP3&4_UFSAR_CHAP05
VEGP3&4_UFSAR_CHAP06
VEGP3&4_UFSAR_CHAP07
VEGP3&4_UFSAR_CHAP08
VEGP3&4_UFSAR_CHAP09
VEGP3&4_UFSAR_CHAP10
VEGP3&4_UFSAR_CHAP11
VEGP3&4_UFSAR_CHAP12
VEGP3&4_UFSAR_CHAP13
VEGP3&4_UFSAR_CHAP14
VEGP3&4_UFSAR_CHAP15
VEGP3&4_UFSAR_CHAP16
VEGP3&4_UFSAR_CHAP17
VEGP3&4_UFSAR_CHAP18
VEGP3&4_UFSAR_CHAP19
VEGP3&4_TIER1

Total Files Listed: 30 File(s)

Southern Nuclear Operating Company

ND-21-0486

Enclosure 2

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

**List of VEGP 3&4 UFSAR and VEGP 3&4 Tier 1 Figures and Sections
Containing Security-Related Information or Proprietary Information**

(Enclosure 2 consists of 6 pages, including this cover page)

Document	Basis for Withholding
UFSAR Figure 1.2-2	Security-Related Information
UFSAR Figure 1.2-4	Security-Related Information
UFSAR Figure 1.2-5	Security-Related Information
UFSAR Figure 1.2-6	Security-Related Information
UFSAR Figure 1.2-7	Security-Related Information
UFSAR Figure 1.2-8	Security-Related Information
UFSAR Figure 1.2-9	Security-Related Information
UFSAR Figure 1.2-10	Security-Related Information
UFSAR Figure 1.2-11	Security-Related Information
UFSAR Figure 1.2-12	Security-Related Information
UFSAR Figure 1.2-13	Security-Related Information
UFSAR Figure 1.2-14	Security-Related Information
UFSAR Figure 1.2-15	Security-Related Information
UFSAR Figure 1.2-16	Security-Related Information
UFSAR Figure 1.2-17	Security-Related Information
UFSAR Figure 1.2-201	Security-Related Information
UFSAR Figure 1.2-19	Security-Related Information
UFSAR Figure 1.2-20	Security-Related Information
UFSAR Figure 1.2-21	Security-Related Information
UFSAR Figure 1.2-22	Security-Related Information
UFSAR Figure 1.2-23	Security-Related Information
UFSAR Figure 1.2-24	Security-Related Information
UFSAR Figure 1.2-25	Security-Related Information
UFSAR Figure 1.2-26	Security-Related Information
UFSAR Figure 1.2-27	Security-Related Information
UFSAR Figure 1.2-28	Security-Related Information
UFSAR Figure 1.2-29	Security-Related Information
UFSAR Figure 1.2-30	Security-Related Information
UFSAR Figure 3.7.2-12 (Sheet 1 of 12)	Security-Related Information
UFSAR Figure 3.7.2-12 (Sheet 2 of 12)	Security-Related Information
UFSAR Figure 3.7.2-12 (Sheet 3 of 12)	Security-Related Information
UFSAR Figure 3.7.2-12 (Sheet 4 of 12)	Security-Related Information
UFSAR Figure 3.7.2-12 (Sheet 5 of 12)	Security-Related Information
UFSAR Figure 3.7.2-12 (Sheet 6 of 12)	Security-Related Information
UFSAR Figure 3.7.2-12 (Sheet 7 of 12)	Security-Related Information
UFSAR Figure 3.7.2-12 (Sheet 8 of 12)	Security-Related Information
UFSAR Figure 3.7.2-12 (Sheet 9 of 12)	Security-Related Information
UFSAR Figure 3.7.2-12 (Sheet 10 of 12)	Security-Related Information
UFSAR Figure 3.7.2-12 (Sheet 11 of 12)	Security-Related Information
UFSAR Figure 3.7.2-12 (Sheet 12 of 12)	Security-Related Information
UFSAR Figure 3.7.2-19 (Sheet 1 of 10)	Security-Related Information
UFSAR Figure 3.7.2-19 (Sheet 2 of 10)	Security-Related Information
UFSAR Figure 3.7.2-19 (Sheet 3 of 10)	Security-Related Information

Document	Basis for Withholding
UFSAR Figure 3.7.2-19 (Sheet 4 of 10)	Security-Related Information
UFSAR Figure 3.7.2-19 (Sheet 5 of 10)	Security-Related Information
UFSAR Figure 3.7.2-19 (Sheet 6 of 10)	Security-Related Information
UFSAR Figure 3.7.2-19 (Sheet 7 of 10)	Security-Related Information
UFSAR Figure 3.7.2-19 (Sheet 8 of 10)	Security-Related Information
UFSAR Figure 3.7.2-19 (Sheet 9 of 10)	Security-Related Information
UFSAR Figure 3.7.2-19 (Sheet 10 of 10)	Security-Related Information
UFSAR Figure 3.8.3-1 (Sheet 2 of 7)	Security-Related Information
UFSAR Figure 3.8.3-1 (Sheet 4 of 7)	Security-Related Information
UFSAR Figure 3H.5-1 (Sheet 3 of 3)	Security-Related Information
UFSAR Figure 3H.5-11 (Sheet 1 of 6)	Security-Related Information
UFSAR Figure 3H.5-11 (Sheet 2 of 6)	Security-Related Information
UFSAR Figure 3H.5-11 (Sheet 3 of 6)	Security-Related Information
UFSAR Figure 3H.5-11 (Sheet 4 of 6)	Security-Related Information
UFSAR Figure 3H.5-11 (Sheet 5 of 6)	Security-Related Information
UFSAR Figure 3H.5-16 (Sheet 1 of 2)	Security-Related Information
UFSAR Figure 3H.5-16 (Sheet 2 of 2)	Security-Related Information
UFSAR Figure 6.2.4-5	Security-Related Information
UFSAR Figure 6.2.4-6	Security-Related Information
UFSAR Figure 6.2.4-7	Security-Related Information
UFSAR Figure 6.2.4-8	Security-Related Information
UFSAR Figure 6.2.4-9	Security-Related Information
UFSAR Figure 6.2.4-10	Security-Related Information
UFSAR Figure 6.2.4-11	Security-Related Information
UFSAR Figure 6.2.4-12	Security-Related Information
UFSAR Figure 6.2.4-13	Security-Related Information
UFSAR Figure 6.4-1	Security-Related Information
UFSAR Appendix 7B, Table 7B-1, Page 7B-1	Proprietary Information
UFSAR Appendix 7B, Table 7B-2, Page 7B-2	Proprietary Information
UFSAR Appendix 7B, Section 7B.1, Page 7B-3	Proprietary Information
UFSAR Appendix 7B, Section 7B.1, Page 7B-4	Proprietary Information
UFSAR Appendix 7B, Section 7B.1, Page 7B-5	Proprietary Information
UFSAR Appendix 7B, Section 7B.1, Page 7B-6	Proprietary Information
UFSAR Appendix 7B, Section 7B.2, Page 7B-7	Proprietary Information
UFSAR Appendix 7B, Section 7B.2, Page 7B-8	Proprietary Information
UFSAR Appendix 7B, Section 7B.2, Page 7B-9	Proprietary Information
UFSAR Appendix 7B, Section 7B.2, Page 7B-10	Proprietary Information
UFSAR Appendix 7B, Section 7B.2, Page 7B-11	Proprietary Information
UFSAR Appendix 7B, Section 7B.3, Page 7B-12	Proprietary Information
UFSAR Appendix 7B, Section 7B.4, Page 7B-13	Proprietary Information
UFSAR Appendix 7B, Section 7B.4, Page 7B-14	Proprietary Information
UFSAR Appendix 7B, Section 7B.4, Page 7B-15	Proprietary Information
UFSAR Appendix 7B, Section 7B.4, Page 7B-16	Proprietary Information

Document	Basis for Withholding
UFSAR Appendix 7B, Section 7B.5, Page 7B-17	Proprietary Information
UFSAR Appendix 7B, Section 7B.5, Page 7B-18	Proprietary Information
UFSAR Appendix 7B, Section 7B.6, Page 7B-19	Proprietary Information
UFSAR Appendix 7B, Section 7B.6, Page 7B-20	Proprietary Information
UFSAR Appendix 7B, Section 7B.7, Page 7B-21	Proprietary Information
UFSAR Appendix 7B, Section 7B.7, Page 7B-22	Proprietary Information
UFSAR Appendix 7B, Section 7B.7, Page 7B-23	Proprietary Information
UFSAR Appendix 7B, Section 7B.8, Page 7B-24	Proprietary Information
UFSAR Appendix 7B, Section 7B.9, Page 7B-25	Proprietary Information
UFSAR Appendix 7B, Section 7B.10, Page 7B-26	Proprietary Information
UFSAR Appendix 7B, Section 7B.10, Page 7B-27	Proprietary Information
UFSAR Appendix 7B, Section 7B.11, Page 7B-28	Proprietary Information
UFSAR Appendix 7B, Section 7B.11, Page 7B-29	Proprietary Information
UFSAR Appendix 7B, Section 7B.11, Page 7B-30	Proprietary Information
UFSAR Appendix 7B, Section 7B.11, Page 7B-31	Proprietary Information
UFSAR Appendix 7B, Section 7B.11, Page 7B-32	Proprietary Information
UFSAR Appendix 7B, Section 7B.12, Page 7B-33	Proprietary Information
UFSAR Appendix 7B, Section 7B.13, Page 7B-34	Proprietary Information
UFSAR Figure 9A-1 (Sheet 2 of 16)	Security-Related Information
UFSAR Figure 9A-1 (Sheet 3 of 16)	Security-Related Information
UFSAR Figure 9A-1 (Sheet 4 of 16)	Security-Related Information
UFSAR Figure 9A-1 (Sheet 5 of 16)	Security-Related Information
UFSAR Figure 9A-1 (Sheet 6 of 16)	Security-Related Information
UFSAR Figure 9A-1 (Sheet 7 of 16)	Security-Related Information
UFSAR Figure 9A-1 (Sheet 8 of 16)	Security-Related Information
UFSAR Figure 9A-1 (Sheet 9 of 16)	Security-Related Information
UFSAR Figure 9A-1 (Sheet 10 of 16)	Security-Related Information
UFSAR Figure 9A-1 (Sheet 11 of 16)	Security-Related Information
UFSAR Figure 9A-1 (Sheet 12 of 16)	Security-Related Information
UFSAR Figure 9A-1 (Sheet 13 of 16)	Security-Related Information
UFSAR Figure 9A-1 (Sheet 14 of 16)	Security-Related Information
UFSAR Figure 9A-1 (Sheet 15 of 16)	Security-Related Information
UFSAR Figure 9A-1 (Sheet 16 of 16)	Security-Related Information
UFSAR Figure 9A-2 (Sheet 1 of 5)	Security-Related Information
UFSAR Figure 9A-2 (Sheet 2 of 5)	Security-Related Information
UFSAR Figure 9A-2 (Sheet 3 of 5)	Security-Related Information
UFSAR Figure 9A-2 (Sheet 4 of 5)	Security-Related Information
UFSAR Figure 9A-2 (Sheet 5 of 5)	Security-Related Information
UFSAR Figure 9A-201	Security-Related Information
UFSAR Figure 9A-3 (Sheet 2 of 3)	Security-Related Information
UFSAR Figure 9A-3 (Sheet 3 of 3)	Security-Related Information
UFSAR Figure 9A-4	Security-Related Information
UFSAR Figure 9A-5	Security-Related Information

Document	Basis for Withholding
UFSAR Figure 12.3-1 (Sheet 2 of 16)	Security-Related Information
UFSAR Figure 12.3-1 (Sheet 3 of 16)	Security-Related Information
UFSAR Figure 12.3-1 (Sheet 4 of 16)	Security-Related Information
UFSAR Figure 12.3-1 (Sheet 5 of 16)	Security-Related Information
UFSAR Figure 12.3-1 (Sheet 6 of 16)	Security-Related Information
UFSAR Figure 12.3-1 (Sheet 7 of 16)	Security-Related Information
UFSAR Figure 12.3-1 (Sheet 8 of 16)	Security-Related Information
UFSAR Figure 12.3-1 (Sheet 9 of 16)	Security-Related Information
UFSAR Figure 12.3-1 (Sheet 10 of 16)	Security-Related Information
UFSAR Figure 12.3-201	Security-Related Information
UFSAR Figure 12.3-1 (Sheet 12 of 16)	Security-Related Information
UFSAR Figure 12.3-1 (Sheet 13 of 16)	Security-Related Information
UFSAR Figure 12.3-1 (Sheet 14 of 16)	Security-Related Information
UFSAR Figure 12.3-1 (Sheet 15 of 16)	Security-Related Information
UFSAR Figure 12.3-1 (Sheet 16 of 16)	Security-Related Information
UFSAR Figure 12.3-2 (Sheet 2 of 15)	Security-Related Information
UFSAR Figure 12.3-2 (Sheet 3 of 15)	Security-Related Information
UFSAR Figure 12.3-2 (Sheet 4 of 15)	Security-Related Information
UFSAR Figure 12.3-2 (Sheet 5 of 15)	Security-Related Information
UFSAR Figure 12.3-2 (Sheet 6 of 15)	Security-Related Information
UFSAR Figure 12.3-2 (Sheet 7 of 15)	Security-Related Information
UFSAR Figure 12.3-2 (Sheet 8 of 15)	Security-Related Information
UFSAR Figure 12.3-2 (Sheet 9 of 15)	Security-Related Information
UFSAR Figure 12.3-2 (Sheet 10 of 15)	Security-Related Information
UFSAR Figure 12.3-202	Security-Related Information
UFSAR Figure 12.3-2 (Sheet 12 of 15)	Security-Related Information
UFSAR Figure 12.3-2 (Sheet 13 of 15)	Security-Related Information
UFSAR Figure 12.3-2 (Sheet 14 of 15)	Security-Related Information
UFSAR Figure 12.3-2 (Sheet 15 of 15)	Security-Related Information
UFSAR Figure 12.3-3 (Sheet 2 of 16)	Security-Related Information
UFSAR Figure 12.3-3 (Sheet 3 of 16)	Security-Related Information
UFSAR Figure 12.3-3 (Sheet 4 of 16)	Security-Related Information
UFSAR Figure 12.3-3 (Sheet 5 of 16)	Security-Related Information
UFSAR Figure 12.3-3 (Sheet 6 of 16)	Security-Related Information
UFSAR Figure 12.3-3 (Sheet 7 of 16)	Security-Related Information
UFSAR Figure 12.3-3 (Sheet 8 of 16)	Security-Related Information
UFSAR Figure 12.3-3 (Sheet 9 of 16)	Security-Related Information
UFSAR Figure 12.3-3 (Sheet 10 of 16)	Security-Related Information
UFSAR Figure 12.3-203	Security-Related Information
UFSAR Figure 12.3-3 (Sheet 12 of 16)	Security-Related Information
UFSAR Figure 12.3-3 (Sheet 13 of 16)	Security-Related Information
UFSAR Figure 12.3-3 (Sheet 14 of 16)	Security-Related Information
UFSAR Figure 12.3-3 (Sheet 15 of 16)	Security-Related Information

Document	Basis for Withholding
UFSAR Figure 12.3-3 (Sheet 16 of 16)	Security-Related Information
UFSAR Appendix 19F, Section 19F.4.2, Page 19F-3	Security-Related Information
UFSAR Appendix 19F, Section 19F.4.3, Page 19F-4	Security-Related Information
Tier 1 Figure 3.3-1	Security-Related Information
Tier 1 Figure 3.3-2	Security-Related Information
Tier 1 Figure 3.3-3	Security-Related Information
Tier 1 Figure 3.3-4	Security-Related Information
Tier 1 Figure 3.3-5	Security-Related Information
Tier 1 Figure 3.3-6	Security-Related Information
Tier 1 Figure 3.3-7	Security-Related Information
Tier 1 Figure 3.3-8	Security-Related Information
Tier 1 Figure 3.3-9	Security-Related Information
Tier 1 Figure 3.3-10	Security-Related Information
Tier 1 Figure 3.3-11A	Security-Related Information
Tier 1 Figure 3.3-11B	Security-Related Information
Tier 1 Figure 3.3-12	Security-Related Information
Tier 1 Figure 3.3-13	Security-Related Information
Tier 1 Figure 3.3-14	Security-Related Information

Southern Nuclear Operating Company

ND-21-0486

Enclosure 3

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

**DVD containing:
VEGP 3&4 UFSAR, Revision 10 (Public Version)
VEGP 3&4 Tier 1, Revision 9 (Public Version)
Vogtle Units 3 and 4 TRM, Revision 18
Vogtle Units 3 and 4 TS Bases, Revision 68**

List of Files Contained in DVD

VEGP3&4_UFSAR_CHAP01
VEGP3&4_UFSAR_CHAP02_SEC02.00-02.04
VEGP3&4_UFSAR_CHAP02_SEC02.04A
VEGP3&4_UFSAR_CHAP02_SEC02.04B
VEGP3&4_UFSAR_CHAP02_SEC02.05 PART 1
VEGP3&4_UFSAR_CHAP02_SEC02.05 PART 2
VEGP3&4_UFSAR_CHAP02_SEC02.05 PART 3
VEGP3&4_UFSAR_CHAP02_SEC02.05A-02.05E
VEGP3&4_UFSAR_CHAP03_SEC03.01-03.07
VEGP3&4_UFSAR_CHAP03_SEC03.08
VEGP3&4_UFSAR_CHAP03_SEC03.09-03F
VEGP3&4_UFSAR_CHAP03_SEC03G-03GG
VEGP3&4_UFSAR_CHAP03_SEC03H-03I
VEGP3&4_UFSAR_CHAP04
VEGP3&4_UFSAR_CHAP05
VEGP3&4_UFSAR_CHAP06
VEGP3&4_UFSAR_CHAP07
VEGP3&4_UFSAR_CHAP08
VEGP3&4_UFSAR_CHAP09
VEGP3&4_UFSAR_CHAP10
VEGP3&4_UFSAR_CHAP11
VEGP3&4_UFSAR_CHAP12
VEGP3&4_UFSAR_CHAP13
VEGP3&4_UFSAR_CHAP14
VEGP3&4_UFSAR_CHAP15
VEGP3&4_UFSAR_CHAP16
VEGP3&4_UFSAR_CHAP17
VEGP3&4_UFSAR_CHAP18
VEGP3&4_UFSAR_CHAP19

VEGP3&4_TIER1_PUBLIC

VEGP3&4_TRM

VEGP3&4_TSBASES

Total Files Listed: 32 File(s)

Southern Nuclear Operating Company

ND-21-0486

Enclosure 4

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

**Affidavit from Southern Nuclear Operating Company for Withholding
Under 10 CFR 2.390**

**(Updated Final Safety Analysis Report, Tier 1, Technical Requirements Manual and
Technical Specifications Bases Annual Submittal)**

(Enclosure 4 consists of 2 pages, plus this cover page)

ND-21-0486

Enclosure 4

Affidavit from Southern Nuclear Operating Company for Withholding Under 10 CFR 2.390 (Updated Final Safety Analysis Report, Tier 1, Technical Requirements Manual and Technical Specifications Bases Annual Submittal)

Affidavit of Brian H. Whitley

1. My name is Brian H. Whitley. I am the Regulatory Affairs Director of Southern Nuclear Operating Company (SNC). I have been delegated the function of reviewing proprietary information sought to be withheld from public disclosure and am authorized to apply for its withholding on behalf of SNC.
2. I am making this affidavit on personal knowledge, in conformance with the provisions of 10 CFR Section 2.390 of the Commission's regulations, and in conjunction with SNC's filing on dockets 52-025 and 52-026, Vogtle Electric Generating Plant Units 3 and 4, Updated Final Safety Analysis Report, Tier 1, Technical Requirements Manual and Technical Specifications Bases Annual Submittal. I have personal knowledge of the criteria and procedures used by SNC to designate information as a trade secret, privileged or as confidential commercial or financial information.
3. Based on the reason(s) at 10 CFR 2.390(a)(4), this affidavit seeks to withhold from public disclosure Enclosure 1 of SNC letter ND-21-0486 for Vogtle Electric Generating Plant Units 3 and 4, Updated Final Safety Analysis Report, Tier 1, Technical Requirements Manual and Technical Specifications Bases Annual Submittal. Note that separate affidavits executed by Westinghouse seek withholding of Enclosure 6, Enclosure 10, Enclosure 13, Enclosure 16, and Enclosure 18.
4. The following is furnished for consideration by the Commission in determining whether the information sought to be withheld from public disclosure should be withheld.
 - a. The information sought to be withheld from public disclosure has been held in confidence by SNC and Westinghouse Electric Company.
 - b. The information is of a type customarily held in confidence by SNC and Westinghouse Electric Company and not customarily disclosed to the public.
 - c. The release of the information might result in the loss of an existing or potential competitive advantage to SNC and/or Westinghouse Electric Company.
 - d. Other reasons identified in Enclosure 5 of SNC letter ND-21-0486 for Vogtle Electric Generating Plant Units 3 and 4, Updated Final Safety Analysis Report, Tier 1, Technical Requirements Manual and Technical Specifications Bases Annual Submittal, and those reasons are incorporated here by reference.

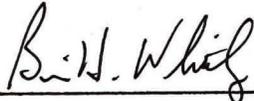
ND-21-0486

Enclosure 4

Affidavit from Southern Nuclear Operating Company for Withholding Under 10 CFR 2.390
(Updated Final Safety Analysis Report, Tier 1, Technical Requirements Manual and
Technical Specifications Bases Annual Submittal)

5. Additionally, release of the information may harm SNC because SNC has a contractual relationship with the Westinghouse Electric Company regarding proprietary information. SNC is contractually obligated to seek confidential and proprietary treatment of the information.
6. 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.
7. To the best of my knowledge and belief, 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.

I declare under penalty of perjury that the foregoing is true and correct.



Brian H. Whitley

Executed on 6/15/21
Date

Southern Nuclear Operating Company

ND-21-0486

Enclosure 5

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

**Westinghouse Electric Company Application for Withholding Proprietary Information
from Public Disclosure and Accompanying Affidavit CAW-19-4876**

(Enclosure 5 consists of 7 pages, plus this cover page)



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

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

Direct tel: (412) 374-5093
Direct fax: (724) 940-8505
e-mail: harperzs@westinghouse.com

CAW-19- 4876

March 21, 2019

APPLICATION FOR WITHHOLDING PROPRIETARY
INFORMATION FROM PUBLIC DISCLOSURE

Subject: Transmittal of APP-FSAR-GEF-008 (NL-1345)

The Application for Withholding Proprietary Information from Public Disclosure is submitted by Westinghouse Electric Company LLC (“Westinghouse”), pursuant to the provisions of paragraph (b)(1) of Section 2.390 of the Nuclear Regulatory Commission’s (“Commission’s”) regulations. It contains commercial strategic information proprietary to Westinghouse and customarily held in confidence.

The proprietary information for which withholding is being requested in the above-referenced report is further identified in Affidavit CAW-19-4876 signed by the owner of the proprietary information, Westinghouse. The Affidavit, which accompanies this letter, sets forth the basis on which the information may be withheld from public disclosure by the Commission and addresses with specificity the considerations listed in paragraph (b)(4) of 10 CFR Section 2.390 of the Commission’s regulations.

Accordingly, this letter authorizes the utilization of the accompanying Affidavit by Southern Nuclear Company.

Correspondence with respect to the proprietary aspects of the Application for Withholding or the Westinghouse Affidavit should reference CAW-19-4876, and should be addressed to Camille T. Zozula, Manager, Infrastructure & Facilities Licensing, Westinghouse Electric Company, 1000 Westinghouse Drive, Building 2, Suite 259, Cranberry Township, Pennsylvania 16066.

Zachary S. Harper, Manager
AP1000 Licensing

Enclosures:

1. Affidavit CAW-19-4876
2. Proprietary Information Notice and Copyright Notice
3. APP-FSAR-GEF-008 (NL-1345)

Enclosure 1 - AFFIDAVIT

COMMONWEALTH OF PENNSYLVANIA:

ss

COUNTY OF BUTLER:

I, Zachary S. Harper, am authorized to execute this Affidavit on behalf of Westinghouse Electric Company LLC (“Westinghouse”) and declare that the averments of fact set forth in this Affidavit are true and correct to the best of my knowledge, information, and belief.

Executed on: 03/21/2019



Zachary S. Harper, Manager
AP1000 Licensing

- (1) I am Manager, AP1000 Licensing, 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 Nuclear Regulatory Commission’s (“Commission’s”) regulations and in conjunction with the Westinghouse Application for Withholding Proprietary Information from Public Disclosure accompanying this Affidavit.
- (3) I have personal knowledge of the criteria and procedures utilized by Westinghouse in designating information as a trade secret, privileged or as confidential commercial or financial information.
- (4) Pursuant to the provisions of paragraph (b)(4) of Section 2.390 of the Commission’s regulations, the following is furnished for consideration by the Commission in determining whether the information sought to be withheld from public disclosure should be withheld.
 - (i) The information sought to be withheld from public disclosure is owned and has been held in confidence by Westinghouse.
 - (ii) The information is of a type customarily held in confidence by Westinghouse and not customarily disclosed to the public. Westinghouse has a rational basis for determining the types of information customarily held in confidence by it and, in that connection, utilizes a system to determine when and whether to hold certain types of information in confidence. The application of that system and the substance of that system constitute Westinghouse policy and provide 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.
- (iii) 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.
- (iv) The information is being transmitted to the Commission in confidence and, under the provisions of 10 CFR Section 2.390, is to be received in confidence by the Commission.
- (v) 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.
- (vi) The proprietary information sought to be withheld in this submittal is that which is appropriately marked in APP-FSAR-GEF-008, "PMS Changes Related to the MTP DVD Drive, Cable Access Control, the FMEA, Component Level Control, and Nonsafety-related Interfaces" (Proprietary), for submittal to the Commission, being transmitted by Southern Nuclear Company letter. The proprietary information as submitted by Westinghouse is that associated with the NL-1345 licensing basis markups which describe the Protection and Safety Monitoring System (PMS) design and Failure Modes and Effects Analysis, and may be used only for that purpose.
- (a) This information is part of that which will enable Westinghouse to manufacture and deliver products to utilities based on proprietary designs.
 - (b) Further, this information has substantial commercial value as follows:

- (i) Westinghouse plans to sell the use of similar information to its customers for the purpose of licensing of new nuclear power stations.
- (ii) Westinghouse can sell support and defense of industry guidelines and acceptance criteria for plant-specific applications.
- (iii) The information requested to be withheld reveals the distinguishing aspects of a methodology which was developed by Westinghouse.

Public disclosure of this proprietary information is likely to cause substantial harm to the competitive position of Westinghouse because it would enhance the ability of competitors to provide similar technical evaluation justifications 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.

Enclosure 2 - Proprietary Information Notice and Copyright Notice

PROPRIETARY INFORMATION NOTICE

Transmitted herewith are proprietary and non-proprietary versions of a document, 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.

Southern Nuclear Operating Company

ND-21-0486

Enclosure 7

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

**Westinghouse Electric Company Application for Withholding Proprietary Information
from Public Disclosure and Accompanying Affidavit CAW-20-5089**

(Enclosure 7 consists of 3 pages, plus this cover page)

Westinghouse Non-Proprietary Class 3

CAW-20-5089
Page 1 of 3AFFIDAVIT

COMMONWEALTH OF PENNSYLVANIA:

COUNTY OF BUTLER:

- (1) I, Zachary S. Harper, have been specifically delegated and authorized to apply for withholding and execute this Affidavit on behalf of Westinghouse Electric Company LLC (Westinghouse).
- (2) I am requesting the proprietary portions of APP-GW-J0R-012, Revision 5 be withheld from public disclosure under 10 CFR 2.390.
- (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 10 CFR 2.390, 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 and is not customarily disclosed to the public.
 - (ii) 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 technical evaluation justifications 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.

Westinghouse Non-Proprietary Class 3

CAW-20-5089
Page 2 of 3AFFIDAVIT

- (5) Westinghouse has policies in place to identify proprietary information. 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.
- (6) The attached submittal contains proprietary information throughout, for the reasons set forth in Sections 5, (a) and (c) of this Affidavit. Accordingly, a redacted version would be of no value to the public.

Westinghouse Non-Proprietary Class 3

CAW-20-5089
Page 3 of 3

AFFIDAVIT

I declare that the averments of fact set forth in this Affidavit are true and correct to the best of my knowledge, information, and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: 9/11/2020



Zachary S. Harper, Manager
Licensing Engineering

Southern Nuclear Operating Company

ND-21-0486

Enclosure 8

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

WCAP-15775, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report," Revision 8

(Enclosure 8 consists of 41 pages, plus this cover page)

WCAP-15775
APP-GW-J1R-004
Revision 8

May 2017

AP1000[®]

Instrumentation and Control Defense-in-Depth and Diversity Report

REVISION HISTORY
RECORD OF CHANGES

Revision	Author	Description
Rev 0	T. P. Hayes	Original issue
Rev 1	T. P. Hayes	Technical updates due to progression of the design
Rev 2	T. P. Hayes	Technical updates due to progression of the design
Rev 3	J. G. Ewald	Technical updates due to progression of the design
Rev 4	J. G. Ewald	Updates to reflect answers to RAIs
Rev. 5	Seth. A. Peasley	<p>Editorial changes throughout:</p> <ul style="list-style-type: none"> • Alphabetized and removed duplicates from the List of Acronyms and Abbreviations. (Not shown as change to highlight added acronyms, see below). • Page <i>viii</i>: Added Trademark Paragraph. • Paragraph 4.2, Item 3: Updated DCD Figure references to match latest revision of AP1000 DCD. • Section 5.5.4 changed “Subsection 5.4 discusses...” to “Section 5.4 discusses...” <p>Per DCP APP-GW-GEE-3892, changed List of Acronyms, Abbreviations, And Trademarks:</p> <ul style="list-style-type: none"> • Added “ALS”, “CIM”, and “FPGA” <p>Per DCP 3892, changed Paragraph 3.3, bullet 1:</p> <ul style="list-style-type: none"> • Deleted references to WCAP-13383 and CE-CES-195 as these references are obsolete. • Added reference to WCAP-16096 (Reference 10) • Added reference to WCAP-16675 (Reference 11)

REVISION HISTORY (cont.)

RECORD OF CHANGES (cont.)

Revision	Author	Description
Rev. 5 (cont.)		<p>Per DCP 3892, changed Paragraph 4.2, Item 4:</p> <ul style="list-style-type: none"> • First Paragraph: changed reference WCAP-13383 to WCAP-16096-NP and changed Reference 3 to Reference 10 • First Paragraph: deleted reference to CE-CES-195 (Reference 4) • First Paragraph, Deleted the sentence: “It is a requirement of the DAS that different people will be responsible for its design and fabrication, including verification and validation.” • First Paragraph, Added “At the system level, different design and IV&V teams are used on the DAS and PMS systems.” • Added the following after the first paragraph: “<i>The AP1000 Component Interface Module (CIM), provides the priority logic between PMS and plant control for component control. The AP1000 CIM Technical Report (Reference 9), identifies how diversity is maintained between the ALS-based DAS and the CIM.</i> The functionality of the CIM and DAS are different, and this reduces the chances that a common cause failure can be made in both designs. The FPGA Logic used in the DAS, as compared to the FPGA logic used in the CIM, is humanly diverse with respect to the following lifecycle activities: <ul style="list-style-type: none"> • Design Activities (i.e., different FPGA logic design teams for activities such as the preparation of design specifications and development of the application logic in the hardware descriptive language) • Implementation Activities (i.e., different FPGA logic design teams for activities required to physically program the FPGA chip such as simulation, synthesis and “place and route” tasks) • Black Box Test Activities (i.e., different IV&V test teams). Black Box Testing is the testing of a component or system in the target hardware without reference to the internal structure of the component or system. Testing focuses solely on the outputs generated in response to selected inputs and execution conditions.”

REVISION HISTORY (cont.)

RECORD OF CHANGES (cont.)

Revision	Author	Description
Rev. 5 (cont.)		<p>Per DCP 3892, changed Paragraph 4.2, Item 6:</p> <ul style="list-style-type: none"> • Revised entire paragraph on Software Diversity. Deleted “The DAS contains redundant signal processing units that use hardware that is different (diverse) from the hardware and software used in the PMS. The DAS uses no software for its control functions.” • Replaced with “The DAS contains redundant signal processing units that use hardware that is different (diverse) from the hardware used in the PMS. The PMS uses a combination of hardware and executable software to achieve its function. The DAS uses no operating system or executable software loops for its control functions. However, software-based tools are used to configure and test the DAS platform. These software tools are unique and diverse as compared to PMS software.”
		<p>Per DCP 3892, Section 6:</p> <ul style="list-style-type: none"> • Deleted Reference 3, WCAP-13383 “AP600 Instrumentation and Control Hardware and Software Design, Verification, and Validation Process Report”. Obsolete reference. • Deleted Reference 4, CE-CES-194, ‘Software Program Manual for Common Q Systems’. Obsolete reference. • Added Reference 9, WCAP-17179, “ AP1000 Component Interface Module Technical Report” • Added Reference 10, WCAP-16096-NP, “Software Program Manual for Common Q Systems” • Added Reference 11, WCAP-16675, “AP1000® Protection and Safety Monitoring System Architecture Technical Report”
Rev. 6	Seth A. Peasley	<p>Made the following changes per DCP APP-GW-GEE-4578:</p> <ul style="list-style-type: none"> • Editorial: Added ® to Document Title. • Editorial: Per trademark guidelines, all usage of term AP1000 is bold, and followed by word “plant” as appropriate. • Editorial: capitalized first letter in acronym list of HIS. • Editorial: italicized bullet list in Glossary section ‘Diversity’. • Figure 2-1 revised to remove arrow from DAS block. • Editorial: Section 2-2, second paragraph, changed “shutdown” to “shut down”. • Section 3.3, first bullet item, clarified Reference 10 is non-proprietary version.

REVISION HISTORY (cont.)

RECORD OF CHANGES (cont.)

Revision	Author	Description
Rev. 6 (cont.)		<ul style="list-style-type: none"> • Section 3.3, first bullet item, corrected document number in Reference 11. Correct reference is WCAP-15927. • Section 4.2, List Item 4, first paragraph, removed duplicate phrase “described in”. • Section 4.2, List Item 4, added “and WCAP-15927 (Reference 11).” • Section 4.2, List Item 4, replaced “The FPGA Logic used in the DAS, as compared to the FPGA logic used in the CIM, is humanly diverse with respect to the following lifecycle activities:” with “The FPGA Logic used in the DAS maintains human diversity with respect to the FPGA logic used in the CIM for the following lifecycle activities:” • Figure 5-1 re-drawn because previous version was too blurry to read effectively. • Figure 5-1 re-drawn to reflect current AP1000 plant I&C diversity architecture. • Figure 5-2 re-drawn because previous version was too blurry to read effectively. • Figure 5-2 re-drawn to reflect current AP1000 plant diverse I&C structure. • Figure 5-2 re-drawn to remove multiplexers from the layout • Section 5.4.10: Added to clarify DAS operations. • Section 5.7.2: Clarified that the DAS actuates key containment isolation valves. • References Section, Item 9, clarified the proprietary version is used. • References Section, Item 10, clarified the proprietary version is used. • References Section, Item 11, removed incorrect reference to WCAP-16675, and replaced with WCAP-15927, “Design Process for AP1000 Common Q Safety Systems.” • Editorial: added revision number to all Westinghouse documents.
Rev. 7	L. Scott Foster	<p>Made the following changes per DCP APP-GW-GEE-4380:</p> <ul style="list-style-type: none"> • Section 3.3 correct references used for V&V • Section 4.2 correct references used for V&V • Section 6 correct reference list to match Sections 3.3 and 4.2

REVISION HISTORY (cont.)

RECORD OF CHANGES (cont.)

Revision	Author	Description
Rev. 8	L. Scott Foster	<p>These changes address DCP-5489 to match WCAP-15775 (APP-GW-J1R-004) to the PMS design.</p> <p>Section 2.2: clarify that not all functions are four-way redundant. The instrumentation and control (I&C) equipment performing reactor trip and ESF actuation functions, their related sensors, and the reactor trip switchgear are, <i>for the most part</i>, four-way redundant.</p> <p>Section 4.4: add “hardwired connections” The control echelon is provided by the PLS, with certain inputs provided from the PMS by means of <i>hardwired connections or</i> isolated data links.</p> <p>Section 4.10.2: fix typo Additionally, the PMS provides both system-level and component-level manual means of actuating ESF functions, and DAS provides manual means of actuating selected <i>ESF</i> functions.</p> <p>Section 6: References updates</p> <p>9. WCAP-17179-P, Rev. 2(as modified by changes provided in Appendix 7A), “AP1000 Component Interface Module Technical Report,” Westinghouse Electric Company LLC. <i>Is now Rev.6.</i></p> <p>11. WCAP-15927, Rev. 4, “Design Process for AP1000 Common Q Safety Systems,” Westinghouse Electric Company LLC. <i>Is now Rev.6.</i></p> <p>CAPAL 100404337 is addressed by the following change to incorporate DCP-4993. Section 4.10.3: delete first sentence Isolated, independent interconnections exist between the reactor trip and ESF actuation functions. Failure of the reactor trip function will not prevent the ESF actuation function from responding to other inputs, nor will failure of the ESF actuation function prevent the reactor trip function from responding to other inputs.</p> <p>CAPAL 100408211 is addressed by the following changes to incorporate DCP-854. Section 5.4.1: “In the event of a small RCS leak, the CVS makeup pumps automatically start on a low pressurizer level signal.” - change <i>“low” to “Low-2”</i> Section 5.4.9: “The PMS automatically opens these valves [“discharge isolation valves”] to initiate IRWST injection on a low-low RCS hot leg level.” – change <i>“low-low” to “Low-4”</i> Section 5.5.6: The IRWST will automatically actuate on low-low RCS hot leg level. – change <i>“low-low” to “Low-4”</i></p>

TABLE OF CONTENTS

REVISION HISTORY	iv
RECORD OF CHANGES	iv
LIST OF TABLES	xi
LIST OF FIGURES	xii
LIST OF ACRONYMS, ABBREVIATIONS, AND TRADEMARKS	xiii
GLOSSARY OF TERMS	xiv
1 INTRODUCTION	1-1
1.1 PREFACE	1-1
1.2 ARCHITECTURE OVERVIEW	1-1
1.3 SCOPE	1-2
1.4 SUMMARY AND CONCLUSIONS	1-2
2 <i>AP1000</i> PLANT INSTRUMENTATION AND CONTROL ARCHITECTURE/ SYSTEMS DESCRIPTION	2-1
2.1 ARCHITECTURE DESCRIPTION	2-1
2.2 PROTECTION AND SAFETY MONITORING SYSTEM OVERVIEW	2-2
2.3 PLANT CONTROL SYSTEM OVERVIEW	2-3
2.4 DIVERSE ACTUATION SYSTEM OVERVIEW	2-3
2.5 DATA DISPLAY AND PROCESSING SYSTEM OVERVIEW	2-3
2.6 CONFORMANCE TO THE NUREG/CR-6303 ECHELON OF DEFENSE STRUCTURE AND TO THE NUREG/CR-6303 BLOCK STRUCTURE.....	2-4
3 DEFENSE-IN-DEPTH FEATURES OF THE <i>AP1000</i> PLANT INSTRUMENTATION AND CONTROL ARCHITECTURE.....	3-1
3.1 INTRODUCTION	3-1
3.2 DEFINITION OF COMMON-MODE FAILURES (CMFS)	3-1
3.3 OVERALL INSTRUMENTATION AND CONTROL FAULT TOLERANT DESIGN FEATURES.....	3-1
4 EVALUATION OF NUREG/CR-6303 GUIDELINES	4-1
4.1 IDENTIFYING SYSTEM BLOCKS – GUIDELINES 1 AND 5	4-1
4.2 DETERMINING DIVERSITY – GUIDELINE 2	4-1
4.3 SYSTEM FAILURE TYPES – GUIDELINE 3.....	4-3
4.3.1 Type 1 Failure.....	4-3
4.3.2 Type 2 Failure.....	4-3
4.3.3 Type 3 Failure.....	4-4
4.4 ECHELONS OF DEFENSE – GUIDELINE 4.....	4-4
4.5 POSTULATED COMMON-MODE FAILURE OF BLOCKS – GUIDELINE 6.....	4-5
4.6 USE OF IDENTICAL HARDWARE AND SOFTWARE MODULES – GUIDELINE 7.....	4-5
4.7 EFFECT OF OTHER BLOCKS – GUIDELINE 8	4-5
4.8 OUTPUT SIGNALS – GUIDELINE 9	4-5
4.9 DIVERSITY FOR ANTICIPATED OPERATIONAL OCCURRENCES AND ACCIDENTS – GUIDELINES 10 AND 11	4-5
4.10 DIVERSITY AMONG ECHELONS OF DEFENSE – GUIDELINE 12.....	4-6

4.10.1	Control/Reactor Trip.....	4-6
4.10.2	Control/ESFAS	4-6
4.10.3	Reactor Trip/ESFAS	4-6
4.11	PLANT MONITORING – GUIDELINE 13.....	4-6
4.12	MANUAL OPERATOR ACTION – GUIDELINE 14	4-7
5	EVALUATION OF DIVERSITY WITHIN THE <i>AP1000</i> PLANT INSTRUMENTATION AND CONTROL ARCHITECTURE.....	5-1
5.1	INTRODUCTION	5-1
5.2	DIVERSITY OVERVIEW OF THE <i>AP1000</i> PLANT INSTRUMENTATION AND CONTROL ARCHITECTURE.....	5-1
5.3	REACTOR SHUTDOWN	5-2
5.4	REACTOR COOLANT SYSTEM INVENTORY CONTROL.....	5-2
5.5	CORE DECAY HEAT REMOVAL	5-6
5.6	CONTAINMENT COOLING.....	5-7
5.7	CONTAINMENT ISOLATION.....	5-7
5.8	EVENT SCENARIOS	5-7
6	REFERENCES	6-1

LIST OF TABLES

Table 2-1. *API000* Plant Instrumentation and Control Echelons of Defense Echelons.....2-5
Table 2-2. Assignment of Instrumentation and Control Equipment to Defense-in-Depth Echelons2-6

LIST OF FIGURES

Figure 2-1. <i>AP1000</i> Plant Instrumentation and Control Systems Interactions	2-2
Figure 5-1. <i>AP1000</i> Plant Instrumentation and Control Systems Diversity Architecture.....	5-3
Figure 5-2. <i>AP1000</i> Plant Diverse Instrumentation and Control Structure.....	5-4

LIST OF ACRONYMS, ABBREVIATIONS, AND TRADEMARKS

ADS	Automatic Depressurization System
ALS	Advanced Logic System
ALWR	Advanced Light Water Reactor
AMSAC	Anticipated Transient Without Trip Mitigation System Actuation Cabinet
CIM	Component Interface Module
CMF	Common-Mode Failure
CMT	Core Makeup Tank
CRDM	Control Rod Drive Mechanism
CVS	Chemical and Volume Control System
DAS	Diverse Actuation System
DCD	Design Control Document
DDS	Data Display and Processing System
EMI/RFI	Electromagnetic Interference/Radio Frequency Interference
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
FPGA	Field Programmable Gate Array
HSI	Human-System Interface
I&C	Instrumentation & Control
IRWST	In-containment Refueling Water Storage Tank
PCS	Passive Containment Cooling System
PLC	Programmable Logic Controller
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
PRA	Probabilistic Risk Assessment
PRHR	Passive Residual Heat Removal
PXS	Passive Core Cooling System
QDPS	Qualified Data Processing Subsystem
RCS	Reactor Coolant System
RNS	Normal Residual Heat Removal System

AP1000 is a trademark or registered trademark of Westinghouse Electric Company LLC, its affiliates and/or its subsidiaries in the United States of America and may be registered in other countries throughout the world. All rights reserved. Unauthorized use is strictly prohibited. Other names may be trademarks of their respective owners.

GLOSSARY OF TERMS

This section contains clarifications of terms used in this report that are defined in NUREG/CR-6303 (Reference 2). These definitions are provided to aid in understanding of the report text, instrumentation and control architecture, and conformance to guidelines. The definitions and clarifications may vary from corresponding definitions in NUREG/CR-6303 because of development and evolution of the **AP1000**[®] plant instrumentation and control architecture. *Definitions as stated in NUREG/CR-6303 are in Italics.*

Anticipated Operational Occurrences:

“...those conditions of normal operation which are expected to occur one or more times during the life of the nuclear power unit and include but are not limited to loss power to all recirculation pumps, tripping of the turbine generator set, isolation of the main condenser and loss of offsite power.” (10CRF50, Appendix A, Definition and Explanations)

Section 15.0.1 of the **AP1000** plant DCD (Reference 6), “Classification of Plant Conditions,” provides the definition and discussion of Anticipated Operational Occurrences.

Accidents:

“Accidents are defined as those conditions of abnormal operation that result in limiting faults...” (Standard Format, Section 15, “Accident Analysis,” USNRC Reg. Guide 1.70)

Section 15.0.1 of the **AP1000** plant DCD (Reference 6), “Classification of Plant Conditions,” provides the definition and discussion of Accidents.

Block:

“Generally, a system is described as an arrangement of components or black boxes interconnected by communication, electrical connections, pipes, or physical effects. This kind of description, often called a ‘system architecture,’ may be too complex or may not be partitioned conveniently for diversity and defense-in-depth analysis. A more convenient description may be obtained by restricting the portion of the system under consideration to instrumentation and control equipment and partitioning the restricted portion into ‘blocks.’ A ‘block’ is the smallest portion of the system under analysis for which it can be credibly assumed that internal failures, including the effects of software errors, will not propagate to other equipment. The objective of choosing blocks is to eliminate the need for detailed examination of internal failure mechanisms while examining system behavior under reasonable assumptions of failure containment.

“Examples of typical software-containing blocks are computers, local area networks or programmable logic controllers (PLCs). A block can be solely hardware, but there are no solely software blocks; software-containing blocks suffer the distinction that both hardware or software faults (and sometimes both acting together) can cause block failure. Consequently, it is difficult to separate the effects of software from the machine that executes that software. For example, a software defect in one small routine can cause an entire computer to fail by corruption of other data or software...”

GLOSSARY OF TERMS (cont.)

Channel:

“A channel is defined as a set of interconnected hardware and software components that processes an identifiable sensor signal to produce a single protective action signal in a single division when required by a generating station condition. A channel includes the sensor, data acquisition, signal conditioning, data transmission, bypasses, and logic up to voters or actuating device inputs. The objective of the channel definition is to define subsets of a reactor protection system that can be unambiguously tested or analyzed from an input to an output.”

Common-Mode (or -Cause) Failure:

“Common-mode failures (CMFs) are causally related failures of redundant or separate equipment; for example, (1) CMF of identical subsystems across redundant divisions, defeating the purpose of redundancy, or (2) CMF of different subsystems or echelons of defense, defeating the use of diversity. CMF embraces all causal relations, including severe environments, design errors, calibration and maintenance errors, and consequential failures...”

For this report, a distinction is made between CMFs and multiple failures. CMFs are further discussed in subsection 3.2. Multiple failures are addressed in the **AP1000** plant Probabilistic Risk Assessment (PRA).

Defense-in-Depth

“Defense-in-depth is a principle of long standing for the design, construction and operation of nuclear reactors, and may be thought of as requiring a concentric arrangement of protective barriers or means, all of which must be breached before a hazardous material or dangerous energy can adversely affect human beings or the environment. The classic three physical barriers to radiation release in a reactor – cladding, reactor pressure vessel, and containment – are an example of defense-in-depth.”

Diversity:

“Diversity is a principle in instrumentation systems of sensing different parameters, using different technologies, using different logic or algorithms, or using different actuation means to provide several ways of detecting and responding to a significant event. Diversity is complementary to the principle of defense-in-depth and increases the chances that defenses at a particular level or depth will be actuated when needed. Defenses at different levels of depth may also be diverse from each other. There are six important types of diversity to consider:

- *Human diversity*
- *Design diversity*
- *Software diversity*
- *Functional diversity*
- *Signal diversity*
- *Equipment diversity...”*

GLOSSARY OF TERMS (cont.)

Echelons of Defense:

NUREG/CR-6303 provides definitions of four echelons of defense. The definition of each level is reproduced in the following along with a brief description of the **AP1000** plant instrumentation and control systems that accomplish the task.

1. Control system:

“The control echelon is that non-Class 1E manual or automatic equipment that routinely prevents reactor excursions toward unsafe regimes of operation and is generally used to operate the reactor in the safe power production operating region. Indicators, annunciators, and alarms may be included in the control echelon. Reactor control systems typically contain some equipment to satisfy the ATWS rule (10 CFR 50.62) or the requirement for a remote shutdown panel. Examples of such equipment include high-quality non-Class 1E equipment for which credit may be taken solely for compensating rare common-mode failures of Class 1E reactor protection equipment.”

The functions performed by the control system echelon of defense are included in the nonsafety Plant Control System (PLS). The PLS normally functions to maintain the plant within operating limits to avoid the need for a reactor trip or engineered safety features (ESF) actuation.

2. Reactor Trip or Scram System:

“The reactor trip echelon is that safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion. It consists of instrumentation for detecting potential or actual excursions, means for rapidly and completely inserting the reactor control rods, and may also include certain chemical neutron moderation systems (e.g., boron injection).”

The automatic reactor trip functions performed by the reactor trip echelon of defense are included in the safety Protection and Safety Monitoring System (PMS). The nonsafety Diverse Actuation System (DAS) also provides automatic reactor trip capabilities.

3. ESF Actuation System (ESFAS):

“The ESFAS echelon is that safety equipment that removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel, and containment). This echelon detects the need for and performs such functions as emergency cooling, pressure relief or depressurization, isolation, and control of various support systems (e.g., emergency generators) or devices (valves, motors, pumps) required for ESF equipment to operate.”

GLOSSARY OF TERMS (cont.)

The automatic ESF actuation functions performed by the ESFAS echelon of defense are included in the safety PMS. The nonsafety DAS also provides automatic actuation capability for a subset of ESF component actuations. The **AP1000** plant is a passive plant and does not require emergency generators, motors, or pumps to perform the ESF functions.

4. Monitoring and Indication System:

“The monitoring and indication echelon is the slowest and also the most flexible echelon of defense. Like the other three echelons, operators are dependent upon accurate sensor information to perform their tasks, but, given information, time, and means, can perform previously unspecified logical computations to react to unexpected events. The monitoring and indication echelon includes both Class 1E and non-Class 1E manual controls, monitors, and indicators required to operate nominally assigned to the other three echelons.”

Monitoring and indication functions are provided by the nonsafety data display and processing system (DDS) and by the safety PMS. The safety manual reactor trip and manual ESF actuation functions performed by the monitoring and indication echelon of defense are included in the PMS. The nonsafety DAS also provides manual reactor trip and manual ESF actuation capabilities.

Instrumentation System:

“A reactor instrumentation system is that set of equipment that senses various reactor parameters and transmits appropriate signals to control systems, to the reactor trip system, to the engineered safety features actuation system, and to the monitoring and indicator system for use in determining the actions these systems or reactor operators will take. Independence is required between control systems, safety-related monitoring and display systems, the two safety systems, and between redundant divisions of the safety systems.”

In this report, the instrumentation system includes the following systems in the instrumentation and control architecture:

- Protection and Safety Monitoring System (PMS)
- Plant Control System (PLS)
- Data Display and Processing System (DDS)
- Diverse Actuation System (DAS)

1 INTRODUCTION

1.1 PREFACE

Since January 1979 when NUREG-0493 (Reference 1) was issued, the instrumentation and control architecture for Westinghouse Pressurized Water Reactors has undergone refinement in both the systems architecture aspects of the overall design, and the detailed design of the instrumentation and control cabinets. Experience gained from the AP600 design, upgrading the instrumentation and control of domestic plants, providing instrumentation and control systems for international plants, and providing plant instrumentation and control for non-nuclear applications has been incorporated into the **AP1000**[®] plant instrumentation and control design. The Advanced Light Water Reactor (ALWR) Utility Requirements Document has provided valuable industry guidance that has also been incorporated into the design. Also, modern statistical tools have been applied to analyze the instrumentation and control design within the context of overall plant risk assessment, and these results have provided insight into design performance considerations. Because of these factors, the **AP1000** plant instrumentation and control design has evolved beyond the RESAR-414 design that was evaluated in NUREG-0493.

Changes beyond the RESAR-414 design have been incorporated into the AP600 and **AP1000** plant instrumentation and control architectures that must be considered in the diversity assessment:

1. Probabilistic risk assessment (PRA) methods were used to consider the role of both safety and nonsafety equipment in the prevention and mitigation of transients and faults. For the **AP1000** plant, this consideration has been reflected in the overall design of the **AP1000** plant's systems.
2. The nonsafety diverse actuation system (DAS) provides a reactor trip and engineered safety features (ESF) actuations diverse from the protection and safety monitoring system (PMS). The DAS is included to support the aggressive **AP1000** plant risk goals by reducing the probability of a severe accident that potentially results from the unlikely coincidence of postulated transients and postulated common-mode failures (CMFs).

In October 1994, the Nuclear Regulatory Commission published NUREG/CR-6303 (Reference 2) which described a deterministic method of analyzing computer-based nuclear reactor protection systems that identifies and evaluates design vulnerabilities to CMF. The **AP1000** plant instrumentation and control systems follow closely the AP600 instrumentation and control systems, which were designed and analyzed before NUREG/CR-6303 was published. As with the AP600 design, PRA methods were used for the analysis of diversity and defense-in-depth analysis for the **AP1000** plant, rather than the deterministic methods described in NUREG/CR-6303. These PRA methods are consistent with NUREG/CR-6303 and allow the designers to concentrate on situations that are the largest contributors to the predicted core melt frequency.

1.2 ARCHITECTURE OVERVIEW

The PMS is a Class 1E instrumentation and control system that is included in the **AP1000** plant instrumentation and control architecture to address the anticipated operational occurrences and accidents outlined and described in Chapter 15 of the **AP1000** plant Design Control Document (DCD) (Reference 6). The PMS is designed to meet plant licensing requirements by including design features

such as: redundancy, functional diversity, failsafe design, continuous self-diagnostics, periodic surveillance test capability, circuit isolation, and a design, verification, and validation process. Section 3.3 describes the fault tolerant features of the PMS.

The DAS is a nonsafety instrumentation and control system that is an enhanced version of the Anticipated Transient Without Trip Mitigation System Actuation Cabinet (AMSAC) in operating Westinghouse nuclear power plants. The DAS is included to enable the **AP1000** plant instrumentation and control architecture to meet reliability goals in the **AP1000** plant PRA, where the PMS is assumed to fail as a result of postulated failures beyond design basis, such as CMF.

1.3 SCOPE

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. NUREG/CR-6303 defines echelons of defense as:

“...specific applications of the principle of defense-in-depth to the arrangement of instrumentation and control systems attached to a nuclear reactor for the purpose of operating the reactor or shutting it down and cooling it. Specifically, the echelons are the control system, the reactor trip or scram system, the engineered safety features (ESF) actuation system, and the monitoring and indicator system.”

This **AP1000** plant Instrumentation and Control Defense-in-Depth and Diversity Report describes the type of diversity that exists among the four echelons of defense for the **AP1000** plant and identifies dependencies among the echelons.

1.4 SUMMARY AND CONCLUSIONS

- 1.4.1 The **AP1000** plant Instrumentation and Control Architecture complies with NUREG-0493. The Architecture pays special attention to Section 2, “Technical Discussion,” and Section 3.3 “Guidelines,” which contain guidelines, requirements, and recommendations for mitigating or preventing potential Common Mode Failures.
- 1.4.2 The **AP1000** plant Instrumentation and Control Architecture complies with NUREG/CR-6303, in particular, Section 3 “Guidelines,” which contains guidelines, requirements, and recommendations for mitigating or preventing potential Common Mode Failures.
- 1.4.3 The analysis to protect against CMF in the **AP1000** plant instrumentation and control architecture was done as part of the PRA. In the PRA, failures of the instrumentation and control architecture, including common cause failures, were analyzed. The PRA report (Reference 7) describes this analysis of the **AP1000** plant instrumentation and control systems. Chapter 26 of the PRA report describes the PMS model; Chapter 27 describes the DAS model; and Chapter 28 describes the Plant Control System (PLS) model. The conclusion is that the **AP1000** plant instrumentation and control architecture is, as calculated by PRA analysis, sufficient to meet probabilistic safety goals.

2 AP1000 PLANT INSTRUMENTATION AND CONTROL ARCHITECTURE/ SYSTEMS DESCRIPTION

2.1 ARCHITECTURE DESCRIPTION

The instrumentation and control systems and functions have been structured into the architecture shown in Figure 2-1 and in DCD Figure 7.1-1 (Reference 6). Figure 2-1 is a simplified representation of the **AP1000** plant instrumentation and control architecture that illustrates the interactions between the instrumentation and control systems. DCD Figure 7.1-1 shows the same instrumentation and control systems and their interfaces in detail. In this architecture, related functions are grouped into cabinets and then these cabinets are connected into systems by means of hardwired conductors, data links, and data highways. The cabinets communicate plant data between systems through a real-time data network.

The instrumentation and control architecture is arranged in a hierarchical manner. Above the real-time data network are the systems whose purpose is to facilitate the interaction between the plant operators and the instrumentation and control systems. These are the operations and control centers system and the data display and processing system (DDS). Below the real-time data network are the systems and functions that perform the protective, control, and data monitoring functions. These are the PMS, the PLS, the InCore instrument system, the special monitoring system, and the DAS.

The special monitoring and InCore instrumentation systems do not provide any functions directly related to the control or protection of the plant and are therefore not discussed in this document.

The operations and control centers system defines the arrangement of the main control room, the layout of the main control room workstations, the remote shutdown workstation, and contains the design process for the layout, and content of operating and safety displays, alarms, controls, and procedures for the preceding human-system interface (HSI). The HSI functions, developed under the operations and control centers system, are covered in the appropriate instrumentation and control systems such as the PMS, PLS, DAS, and DDS.

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 DDS (plant computer) is implemented using 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 input from the real-time data network and delivers output over the network to other users.

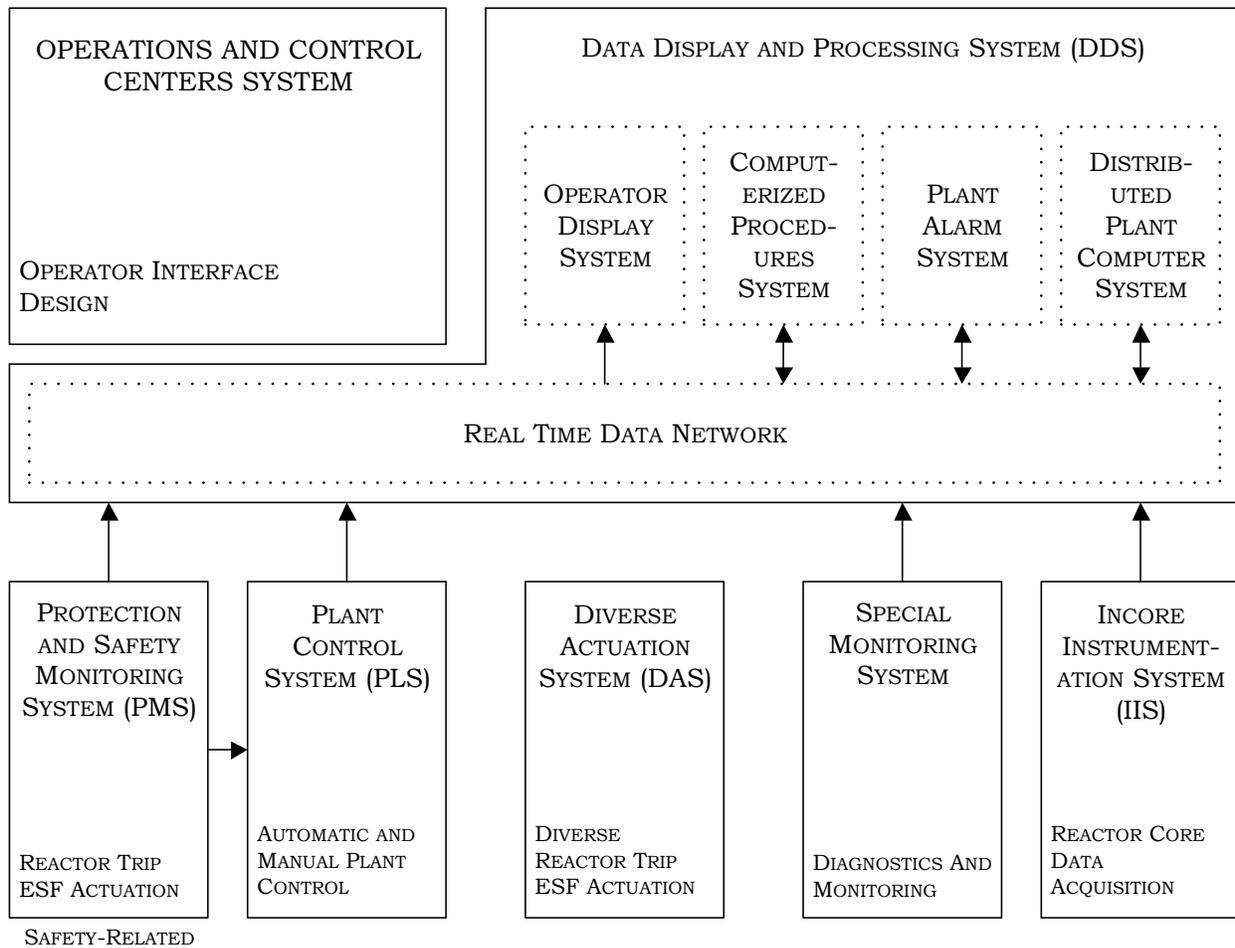


Figure 2-1. AP1000 Plant Instrumentation and Control Systems Interactions

2.2 PROTECTION AND SAFETY MONITORING SYSTEM OVERVIEW

Located in the lower left of Figure 2-1 is the safety PMS. The PMS performs the reactor trip functions, the ESF actuation functions, and the Qualified Data Processing Subsystem (QDPS) functions. The instrumentation and control (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.

The PMS provides the safety functions necessary to monitor the plant during normal operation, to shut down the plant, and to maintain the plant in a safe shutdown condition. The PMS controls safety components in the plant that are operated from the main control room or remote shutdown workstation.

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

Further description of the PMS is contained in Chapter 7 of the AP1000 plant DCD.

2.3 PLANT CONTROL SYSTEM OVERVIEW

The nonsafety PLS is located to the right of the PMS in Figure 2-1. The PLS provides the functions necessary for normal operation of the plant from cold shutdown through full power. The PLS controls nonsafety components in the plant that are operated from the main control room or remote shutdown workstation.

The PLS contains nonsafety control and instrumentation equipment to control reactor power, control pressurizer pressure and level, control feedwater flow, and perform other plant functions associated with power generation.

The PLS provides margins to plant safety limits and the plant's transient performance. The PLS maintains the plant conditions within operating limits. The PLS provides the instrumentation and control to support defense-in-depth automatic and manual functions. The PLS also provides sensors for nonsafety plant monitoring functions.

The PLS is described further in Chapter 7 of the **AP1000** plant DCD.

2.4 DIVERSE ACTUATION SYSTEM OVERVIEW

The DAS is located to the right of the PLS in Figure 2-1. The DAS is a nonsafety, 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 DAS receives signals directly from dedicated sensors. The DAS contains redundant signal processing units that use hardware that is different (diverse) from the hardware and software used in the PMS.

The DAS is described further in Chapter 7 of the **AP1000** plant DCD.

2.5 DATA DISPLAY AND PROCESSING SYSTEM OVERVIEW

The nonsafety DDS is in the upper right of Figure 2-1. The DDS provides the equipment used for processing data that will result in nonsafety 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 DDS also contains the real-time data network, which is a redundant data network that links the elements of the **AP1000** plant instrumentation and control architecture.

2.6 CONFORMANCE TO THE NUREG/CR-6303 ECHELON OF DEFENSE STRUCTURE AND TO THE NUREG/CR-6303 BLOCK STRUCTURE

The **AP1000** plant instrumentation and control architecture conforms to the echelon of defense structure defined in Section 2.2 of NUREG/CR-6303 and the block structure described in Section 2.5 of NUREG/CR-6303. The four echelons are divided into three levels containing the nonsafety systems, safety systems, and nonsafety diverse systems that provide automatically and manually actuated functions to support these echelons.

The functions assigned to the instrumentation and control systems are implemented by processor-based subsystems, which are placed within a structure of cabinets. Table 2-1 maps the echelons of defense to the instrumentation and control architecture. The echelons are divided into a nonsafety layer, a safety layer, and a diverse layer to reflect the means provided by the systems to implement the functions of each echelon. Table 2-2 illustrates the relationships between these subsystems and cabinets and the block structure described in NUREG/CR-6303. This table shows the assignment of equipment to the blocks for each level within the echelons of defense.

Due to the nature of the processor implementation, the demarcation between measured variable blocks and derived variable blocks lies within the software structure of a channel or function. These blocks are combined into a single column for purposes of defining hardware assignments.

Indications to support manual actions to maintain the plant within operating limits, trip the reactor, and actuate ESF functions are provided within the three layers of the instrumentation and control architecture. The DDS provides nonsafety operator displays and alarms. Plant data for the nonsafety displays and alarms is obtained from across the instrumentation and control architecture by means of the real-time data network. The QDPS within the PMS provides safety operator displays. In addition, the DAS provides nonsafety, operator indications which are diverse from PMS. Figure 5-2 shows the integration of indication functions into the instrumentation and control architecture.

Table 2-1. AP1000 Plant Instrumentation and Control Echelons of Defense Echelons

	LAYER 1 NONSAFETY SYSTEMS	LAYER 2 SAFETY SYSTEMS	LAYER 3 DIVERSE NONSAFETY SYSTEMS
CONTROL ECHELON	PLANT CONTROL SYSTEM (PLS) NOTES 1 & 2		
REACTOR TRIP ECHELON		PROTECTION AND SAFETY MONITORING SYSTEM (PMS) NOTE 2	DIVERSE ACTUATION SYSTEM (DAS) NOTE 2
ESF ACTUATION ECHELON		PROTECTION AND SAFETY MONITORING SYSTEM (PMS) NOTE 2	DIVERSE ACTUATION SYSTEM (DAS) NOTE 2
MONITORING AND INDICATION ECHELON	DATA DISPLAY AND PROCESSING SYSTEM (DDS)	PROTECTION AND SAFETY MONITORING SYSTEM (PMS) NOTE 2	DIVERSE ACTUATION SYSTEM (DAS) NOTE 2
		CLASS 1E SYSTEMS	

Notes:

1. The PLS enables the plant to maintain conditions within operating limits and also provides automatic and manual actuations of the nonsafety defense-in-depth systems.
2. Automatic and manual actions are provided in the PLS, PMS, and DAS.

Table 2-2. Assignment of Instrumentation and Control Equipment to Defense-in-Depth Echelons

Echelon	AP1000 Plant Function	Measured and Derived Variable Blocks	Command Block	Manual Actions(2)
Plant Control	nonsafety	sensors, signal conditioning, (communication functions in PMS) ⁽¹⁾	real-time data network, output signal conditioning, output driver	system level soft control as determined by HSI design; component level soft control
	safety	NONE	NONE	NONE
	diverse	NONE	NONE	NONE
Reactor Trip	nonsafety	not applicable	not applicable	not applicable
	safety	sensors, signal conditioning, plant protection subsystem	voting logic, reactor trip switchgear	hardwired manual reactor trip to reactor trip breakers
	diverse	sensors, signal conditioning, diverse control logic	output driver, rod drive M/G set field breaker	hardwired manual reactor trip to rod drive M/G set field breaker
Engineered Safety Features Actuation	nonsafety	not applicable	not applicable	component level soft control
	safety	sensors, signal conditioning, plant protection subsystem	ESF coincidence logic, logic bus, ESF actuation subsystem	system level to ESF coincidence logic
	diverse	sensors, signal conditioning, diverse control logic	output driver	hardwired component level
Monitoring and Indication	nonsafety	sensors, signal conditioning, (communication functions in PMS)	real-time data network, alarm processors, operator workstations	see other three echelons
	safety	sensors, signal conditioning, QDPS	qualified operator displays	see other three echelons
	diverse	sensors, signal conditioning	diverse display devices	see other three echelons

Notes:

1. Used for safety sensors that provide isolated information to nonsafety systems.
2. See Section 4.11 for supplemental information.

3 DEFENSE-IN-DEPTH FEATURES OF THE AP1000 PLANT INSTRUMENTATION AND CONTROL ARCHITECTURE

3.1 INTRODUCTION

This section describes features of the instrumentation and control architecture that provide redundant design, fail-safe design, and failure detection and repair. Section 5 of this document discusses design diversity.

3.2 DEFINITION OF COMMON-MODE FAILURES (CMFS)

For the purpose of this report, CMFs are considered to be sets of causally related failures that occur within a limited time, and fall outside of system design capabilities for detection or mitigation of failures. The failures that meet this definition exhibit the following characteristics:

- The failures occur in a sufficient number of places in the instrumentation and control architecture such that redundant design is ineffective in enabling the system to tolerate the failure.
- The failures are such that fail-safe design is ineffective in enabling the system to tolerate the failure.
- The failures are undetectable, or they occur within a sufficiently short time that neither automatic nor manual responses are possible to enable the system to tolerate the failures.

An instrumentation and control system, or portion of a system, can be capable of tolerating some combinations of CMFs because:

1. Diverse design exists within the system.
2. Redundant design exists within the system.
3. Fail-safe design exists within the system.
4. The failure is detectable and sufficient time exists between instances of failure that automatic or manual response to the failure occurs.

In this evaluation, CMFs are postulated to cause complete failure of similar or identical equipment. This failure mode is assumed to cause complete loss of function of the PMS, but not loss of function of the DAS.

3.3 OVERALL INSTRUMENTATION AND CONTROL FAULT TOLERANT DESIGN FEATURES

The instrumentation and control architecture contains design features whose primary intent is to meet licensing requirements and to enhance plant reliability and availability. However, these features also

provide a degree of protection against CMFs, and, as a result, decrease the probability that a CMF will render a portion of the **AP1000** plant instrumentation and control architecture unable to respond to a transient or plant fault. Among these design features that protect against failures, including CMF, are:

- The Design, Verification, and Validation Process – The design of the instrumentation and control systems hardware and software elements are controlled by a design, verification, and validation process that is described in DCD Section 7.1.2.14. These processes are formal, rigorous means to detect and correct design errors before they can result in common-mode errors in the plant.
- Use of a Distributed Processing Architecture – Instrumentation and control functions are divided among multiple subsystems so that diverse functions are separated into different subsystems. This, in conjunction with other design features such as division independence, has the effect of localizing certain CMFs to a single subsystem. For instances where functional diversity exists in the instrumentation and control architecture, complete system failure may not occur as a result of CMF.
- Redundancy – While redundant design of itself does not prevent CMFs, use of redundant subsystems can enable the plant to detect and respond to failures, including CMFs in those instances where sufficient time exists between occurrences of the individual failures.
- Modular Design – Modular design enhances the rapid isolation and repair of failures. For instances where failures, including CMFs, occur, but sufficient time between failure instances exists for detection and repair, modular design enables the redundant subsystems to be available for response to events.
- Fail-Safe/Fault Tolerant Design – Fail-safe design features in the instrumentation and control architecture, such as de-energizing to trip or actuate, provide the capability to, automatically or manually, put the plant into a safe condition following single failures and certain types of multiple failures. Fault tolerant design features, such as functional diversity and redundancy, also provide the capability to, automatically or manually, put the plant into a safe condition following single failures and certain types of multiple failures.
- Alarm System – The **AP1000** plant alarm system is capable of alerting the operator to failures, including multiple failures, in other parts of the instrumentation and control systems. The main **AP1000** plant alarm system is part of the DDS, which uses different hardware and software from the PMS.
- Continuous Self-Diagnostics – In the **AP1000** plant instrumentation and control architecture, the subsystems continuously execute self-diagnostic software routines. Other self-diagnostic features, such as read-backs and watchdog timers continuously monitor operation of critical subsystems. These self-diagnostic features are designed to detect and report hardware failures, enabling the operator to act.
- Test Subsystem – The test subsystem rapidly and consistently verifies system operation. The use of the test subsystem enhances the timely detection of all failures, including CMF. The test

subsystem also enhances the ability of plant personnel to quickly diagnose and repair failures detected by the continuous self-diagnostic features.

- **Circuit Isolation** – Circuit isolation is used to electrically isolate segments of the instrumentation and control architecture and to prevent propagation of electrical faults. This feature helps to limit the propagation of faults caused by failures, including CMF.
- **Control of Setpoint and Tuning Adjustments** – The instrumentation and control architecture has physical and administrative controls and multiple levels of security for access to setpoint and tuning adjustments. This helps to prevent CMF due to incorrect constants entered as a result of a maintenance error.
- **Use of Engineering Units for Setpoints and Tuning Constants** – Setpoints and tuning constants in the instrumentation and control architecture are entered in engineering units rather than as scaled values. This eliminates a potential common-mode error by removing scaling calculations.
- **Signal Selector Algorithm in the Plant Control System** – The signal selector algorithm in the PLS protects against failure, including CMF, of sensor signals shared by the protection and control systems. The signal selector algorithm alerts the operator to differences in output signals from redundant sensors.
- **Physical Separation** – Physical separation is provided between the four redundant divisions of equipment for the safety PMS, which in turn, are separated from nonsafety systems such as the PLS. Equivalent physical separation is also provided for supporting systems, such as electrical power. Physical separation meets the requirements of IEEE-384 (Reference 8). This physical separation provides protection from CMF induced by physical phenomena.
- **Equipment Qualification** – Equipment in the instrumentation and control architecture is qualified to environmental requirements, including temperature, humidity, vibration/seismic, electromagnetic interference/radio frequency interference (EMI/RFI), and surge withstand criteria commensurate with its safety classification and intended usage. The environmental qualification program provides assurance that physical phenomena will not introduce CMF until design requirements are exceeded.
- **Other Features** – The instrumentation and control architecture also contains other design features, such as ac power line protection and filtering, EMI/RFI design, and surge withstand networks at signal conditioning board inputs, which will prevent failure from specific causes. Due to these features, the causes that would induce multiple failures must be in excess of design and qualification test limits.

4 EVALUATION OF NUREG/CR-6303 GUIDELINES

NUREG/CR-6303 (Reference 2) describes a method for analyzing computer-based reactor protection system vulnerability to postulated software CMFs. NUREG/CR-6303 provides fourteen guidelines for performing a diversity and defense-in-depth analysis. The following sections describe the results of applying these guidelines to the **AP1000** plant.

Section	Title	NUREG Guideline
4.1	Identifying System Blocks	1, 5
4.2	Determining Diversity	2
4.3	System Failure Types	3
4.4	Echelons of Defense	4
4.5	Postulated Common-Mode Failure of Blocks	6
4.6	Use of Identical Hardware and Software Modules	7
4.7	Effect of Other Blocks	8
4.8	Output Signals	9
4.9	Diversity for Anticipated Operational Occurrences and Accidents	10, 11
4.10	Diversity among Echelons of Defense	12
4.11	Plant Monitoring	13
4.12	Manual Operator Action	14

4.1 IDENTIFYING SYSTEM BLOCKS – GUIDELINES 1 AND 5

The safety instrumentation that provides the protective functions is divided into four redundant divisions. Table 2-2 shows how the cabinets and subsystems within each division can be mapped into blocks.

The nonsafety PLS uses redundant sensors and redundant subsystems to provide defense-in-depth functions. The nonsafety DAS uses redundant sensors and redundant subsystems to provide diverse actuation functions.

In this evaluation, however, CMFs are postulated to cause complete failure of similar or identical equipment. This failure mode is assumed to cause the complete loss of function of the PMS, but not loss of function of the DAS due to the diversity of implementation.

4.2 DETERMINING DIVERSITY – GUIDELINE 2

NUREG/CR-6303 identifies six aspects of diversity to address the issue of common-mode effects:

1. Design Diversity

In the nonsafety DAS, energize to trip or actuate logic is used. In the safety PMS, de-energize to trip or actuate logic is used, except where energize to trip is necessary to meet plant system design requirements.

2. Equipment Diversity

For the DAS, the hardware which is used to provide the signal input and conditioning and automatic actions will be diverse from the equipment used for related functions in the PMS. In addition, the DAS provides a reactor trip by tripping the nonsafety rod drive motor-generator set field breakers in the plant control system. This means is diverse from the reactor trip switchgear used in the PMS for reactor trip.

3. Functional Diversity

The **AP1000** plant is designed with multiple levels of defense for each anticipated operational occurrence and accident. These multiple levels of defense are described in WCAP-13793 (Reference 5). WCAP-13793 is an AP600 document that is applicable to the **AP1000** plant. The PMS is a Class 1E system with 4-way divisional separation. Two-out-of-four voting is used for the reactor trip function and most ESF actuation functions. Multiple reactor trip functions and ESF actuations are provided for each anticipated operational occurrence and accident, generally using diverse sensors, as described in DCD Chapter 15 (Reference 6). The DAS has two automatic logic racks that support two-out-of-two voting for reactor trip and ESF actuations. The functional logic for the automatic PMS functions is shown in DCD Figure 7.2-1, sheets 1-19. The functional logic for the automatic DAS functions is shown in DCD Figure 7.2-1, sheets 20 and 21.

4. Human Diversity

The design, verification, and validation programs for instrumentation and control systems, as described in WCAP-16096-P-A (Reference 10) and WCAP-15927 (Reference 11), require and specify the use of independent review. At the system level, different design and IV&V teams are used on the DAS and PMS systems.

The **AP1000** plant Component Interface Module (CIM), provides the priority logic between PMS and plant control for component control. The **AP1000** plant CIM Technical Report (Reference 9), identifies how diversity is maintained between the ALS-based DAS and the CIM.

The functionality of the CIM and DAS are different, and this reduces the chances that a common cause failure can be made in both designs. The Field Programmable Gate Array (FPGA) logic used in the DAS maintains human diversity with respect to the FPGA logic used in the CIM for the following lifecycle activities:

- Design Activities (i.e., different FPGA logic design teams for activities such as the preparation of design specifications and development of the application logic in the hardware descriptive language)
- Implementation Activities (i.e., different FPGA logic design teams for activities required to physically program the FPGA chip such as simulation, synthesis and “place and route” tasks)
- Black Box Test Activities (i.e., different IV&V test teams).

Black Box Testing is the testing of a component or system in the target hardware without reference to the internal structure of the component or system. Testing focuses solely on the outputs generated in response to selected inputs and execution conditions.

5. Signal Diversity

Signal diversity for specific events is provided within the safety level of the reactor trip and ESF actuation echelons. The signals used to produce reactor trips and ESF actuations within the PMS originate from different types of sensors as shown in DCD Tables 7.2-1 and 7.3-1. The DAS receives signals directly from its own dedicated sensors.

6. Software Diversity

The DAS contains redundant signal processing units that use hardware that is different (diverse) from the hardware used in the PMS. The PMS uses a combination of hardware and executable software to achieve its function. The DAS uses no operating system or executable software loops for its control functions. However, software-based tools are used to configure and test the DAS platform. These software tools are unique and diverse as compared to PMS software.

4.3 SYSTEM FAILURE TYPES – GUIDELINE 3

NUREG/CR-6303 describes three different instrumentation failure types that are applicable to the **AP1000** plant.

4.3.1 Type 1 Failure

Type 1 failures are postulated failures in one echelon that result in a plant transient that require a protection function to mitigate the transient. Generally, the postulated failure is assumed to occur in the control system echelon such that a plant transient occurs that results in an automatic reactor trip or ESF actuation. However, there are also postulated failures in the ESF that necessitate protective action.

Examples of Type 1 failures that are analyzed in the DCD Chapter 15 (Reference 6) accident analyses are described in WCAP-13793, “AP600 System/Event Matrix” (Reference 5). WCAP-13793 is an AP600 document that is applicable to the **AP1000** plant.

The primary defense against Type 1 failures is to ensure that a protection function exists to mitigate each postulated credible failure that can occur in plant control or protection systems and can result in a plant transient and requires protective action.

4.3.2 Type 2 Failure

Type 2 failures are undetected failures that are manifested only when a demand is received to actuate a component or system. Failure to respond is due to a postulated CMF of redundant divisions or trains. For example, a software CMF in all four divisions of the plant protection subsystem could potentially degrade the operation of all four process divisions. Another example would be a postulated software CMF in a

software module in the train-related ESF coincidence logic that could degrade the capability of the protection system to actuate ESF components or systems.

The primary defense against a Type 2 failure is to provide diversity within and between the four echelons of defense. The goal is to design a system in which all functions associated with an echelon of defense and the four echelons of defense are not susceptible to a postulated CMF.

4.3.3 Type 3 Failure

Type 3 failures are failures that occur because either the plant process does not respond in a predictable manner or the sensors measuring the plant process respond in an anomalous manner. An example of the first type of anomalous behavior was experienced during the Three Mile Island Unit 2 (TMI-2) event in 1979. A pressurizer relief valve stuck open resulting in the loss of reactor coolant. However, the pressurizer level sensors indicated acceptable pressurizer levels. The anomalous level indication occurred because coolant was being lost at the top of the pressurizer, which resulted in a high level indication due to the design of the delta-P level measurement circuit. An example of the second type of anomalous behavior is the response of the steam generator level measurement system following a high-energy line rupture inside containment. The delta-P measurement level transmitter is calibrated assuming the ambient reference leg temperature is at the normal containment operating temperature. If a high-energy line rupture occurs inside containment, the reference leg heats up to the elevated containment temperature, which results in an anomalous high, indicated level in the steam generator, since the transmitter was calibrated at a lower temperature.

The primary defense against a Type 3 failure is to provide diverse sensors for measuring the plant response to an initiating event, e.g., using turbine impulse pressure and neutron Excore detectors for measuring reactor power. Another example would be using reactor coolant system (RCS) subcooling and core-exit thermocouple temperature to measure core cooling.

4.4 ECHELONS OF DEFENSE – GUIDELINE 4

The instrumentation and control architecture is divided into four echelons of defense, as defined in NUREG/CR-6303. The control echelon is provided by the PLS, with certain inputs provided from the PMS by means of hardwired connections or isolated data links.

The PMS and the DAS provide the reactor trip echelon. The reactor trip function in the safety PMS is provided by: the plant protection subsystems, the voting logic, the dedicated datalinks, the reactor trip switchgear interface and the reactor trip switchgear. The nonsafety DAS and rod drive motor-generator set field breakers provide a diverse reactor trip function. In addition, the PLS will enable the plant to avoid the need to trip for certain events by maintaining the plant within acceptable limits.

The PMS and the DAS provide the ESF echelon. The ESF subsystems within the plant protection subsystems, the ESF coincidence logic, the ESF actuation subsystems, dedicated datalinks, and data highways provide the ESF function in the PMS. The DAS provides diverse means to actuate some ESF functions. In addition, the PLS actuates defense-in-depth plant systems to enable the plant to avoid the need for actuating the passive safety systems.

4.5 POSTULATED COMMON-MODE FAILURE OF BLOCKS – GUIDELINE 6

The CMF of processor-based subsystems postulated for this document is a failure that occurs in all similar subsystems. This postulated failure could be caused by failure of a common hardware element, or failure of a common software element. This failure mode is assumed to cause the complete loss of function of the PMS, but not loss of function of the DAS due to the diversity of the implementations. The result of this failure is that the entire system or systems fail to produce any protective actions. The evaluation of the instrumentation and control architecture based on this failure is contained in Section 5 of this document.

4.6 USE OF IDENTICAL HARDWARE AND SOFTWARE MODULES – GUIDELINE 7

The PRA postulated CMF within the instrumentation and control architecture, in conjunction with random failures. The PRA evaluated the contribution to core damage due to instrumentation and control CMF to be acceptably low. It is conservatively assumed in the PRA that all software modules or hardware modules of a type will fail simultaneously. The diversity between the PMS and DAS assures that the joint CMF probability is acceptably low.

4.7 EFFECT OF OTHER BLOCKS – GUIDELINE 8

In the **AP1000** plant instrumentation and control architecture, input signals are not shared between DAS and other systems.

For CMF within the PMS, the system is conservatively assumed to actuate no protective actions needed during an event.

4.8 OUTPUT SIGNALS – GUIDELINE 9

Optical or resistive isolation is provided between subsystems to prevent propagation of electrical failures in either direction. The four divisions of the PMS are physically separated. Since sensors are considered to be contained in a measured variable block for the purposes of the analyses in this report, failure of signal conditioning equipment influencing sensor performance is not considered. (Note that the instrumentation and control hardware contains features to minimize the occurrence of this failure mode.)

4.9 DIVERSITY FOR ANTICIPATED OPERATIONAL OCCURRENCES AND ACCIDENTS – GUIDELINES 10 AND 11

The frequency of a postulated accident occurring in conjunction with CMFs of the PMS and failures of the DAS is calculated in the **AP1000** plant PRA (Reference 7). Chapter 26 of the PRA report discusses the PMS modeling, and Chapter 27 presents the modeling of the DAS. Section 5 of this document provides a strategic evaluation of the ability of the instrumentation and control architecture to produce the following required protective actions to support the safety goals:

- Reactor shutdown
- Maintain reactor coolant inventory

- Initiate and maintain core decay heat removal
- Initiate and maintain containment cooling
- Initiate containment isolation

Note that the primary coolant system can be depressurized in a controlled fashion to mitigate certain events.

4.10 DIVERSITY AMONG ECHELONS OF DEFENSE – GUIDELINE 12

4.10.1 Control/Reactor Trip

For the low probability circumstance where an event that requires a reactor trip occurs coincident with a postulated CMF in the PMS, the DAS initiates the reactor trip in a diverse fashion. The specific functions performed by the DAS are selected based on the PRA evaluation. The DAS functional requirements are based on an assessment of the protection system instrumentation CMF probabilities combined with the event probability.

Additionally, both the PMS and DAS provide manual means of tripping the reactor. To support manual reactor trip, both the PMS and the DAS provide plant information to the operator. The PMS provides the Class 1E QDPS indications, while the DAS provides nonsafety diverse indications.

4.10.2 Control/ESFAS

For the low probability circumstance where an event that requires one or more ESF actuations occurs coincident with a postulated CMF in the PMS, the DAS initiates selected ESF actuations in a diverse fashion. The specific functions performed by the DAS are selected based on the PRA evaluation. The DAS functional requirements are based on an assessment of the protection system instrumentation CMF probabilities combined with the event probability.

Additionally, the PMS provides both system-level and component-level manual means of actuating ESF functions, and DAS provides manual means of actuating selected ESF functions. To support manual ESF actuation, both the PMS and the DAS provide plant information to the operator. The PMS provides the Class 1E QDPS indications, while the DAS provides nonsafety diverse indications.

4.10.3 Reactor Trip/ESFAS

Failure of the reactor trip function will not prevent the ESF actuation function from responding to other inputs, nor will failure of the ESF actuation function prevent the reactor trip function from responding to other inputs.

4.11 PLANT MONITORING – GUIDELINE 13

Indications to support manual actions to maintain the plant within operating limits, trip the reactor, and actuate ESF functions are provided within the three layers of the instrumentation and control architecture. The DDS provides nonsafety operator displays and alarms. Plant data for the nonsafety displays and alarms is obtained from across the instrumentation and control architecture by means of the real-time data

network. The QDPS within the PMS provides safety operator displays. In addition, the DAS provides nonsafety, diverse operator indications. No sensors are shared between the RTS/ESFAS and the DAS. Diverse and independent signal conditioning and data acquisition functions will be performed in the RTS/ESFAS and DAS such that a postulated software common mode failure in the PMS platform will not degrade the signal conditioning and data acquisition functions in the other platform.

Signals are transmitted from the PMS to the PLS and the DDS. The connections between the PMS and the PLS and DDS contain isolation devices to prevent failures in the PLS or DDS from affecting operation of the PMS. Once signals leave the PMS through the isolation devices, they are no longer safety-related, and are not used to provide any safety functions.

The signals from PMS to PLS and DDS meet the independence requirements of GDC-24, IEEE-603, IEEE-379, and IEEE-384.

No credible failure of the PLS or DDS will prevent the safety system from performing its safety function. The Gateway provides the connections used for plant monitoring and for surveillance of the reactor trip and ESF actuation subsystems. The DDS provides the software and hardware used for displaying plant parameters and monitoring system performance.

The automatic functions of the PMS are designed to protect the **AP1000** plant from potential operator-induced transients which may result from failures in the DDS or PLS.

4.12 MANUAL OPERATOR ACTION – GUIDELINE 14

The manual reactor trip and ESF actuation functions performed by the monitoring and indication echelon of defense is included in the safety PMS. The nonsafety DAS also provides manual reactor trip and selected ESF actuation capabilities.

Both the PMS and DAS provide manual means of tripping the reactor. The PMS provides a hardwired reactor trip to the reactor trip breakers. The DAS provides a diverse hardwired reactor trip to the rod drive motor-generator set field breaker.

The PMS provides both system-level and component-level manual means of actuating ESF functions. The DAS provides manual means of actuating selected ESF functions.

5 EVALUATION OF DIVERSITY WITHIN THE *AP1000* PLANT INSTRUMENTATION AND CONTROL ARCHITECTURE

5.1 INTRODUCTION

The **AP1000** plant fluid systems are designed with multiple levels of defense for a wide range of events. The designs of both the safety and the nonsafety systems support this multiple level design philosophy. The **AP1000** plant instrumentation and control systems architecture reflects this multiple level of defense approach by including safety and nonsafety instrumentation systems that provide safety and nonsafety means of initiating protective functions.

This section of the document discusses the functions provided to protect the core and limit the spread of radioactivity during an event by initiating:

- Reactor Shutdown
- RCS Inventory Control
- Core Decay Heat Removal
- Containment Cooling
- Containment Isolation

5.2 DIVERSITY OVERVIEW OF THE *AP1000* PLANT INSTRUMENTATION AND CONTROL ARCHITECTURE

For the purposes of discussing instrumentation and control diversity, the **AP1000** plant instrumentation and control systems can be organized into three layers. The first layer contains the nonsafety PLS and the DDS. The PLS provides the monitoring, and the automatic and manual control of nonsafety functions. The PLS contains sensors, rod control cabinets, control logic cabinets, the rod drive motor/generator set, the pressurizer heater controller, the rod position indication system, and operator controls. The DDS provides operator displays and alarms in the main control room and remote shutdown area. Dedicated functional processors perform display and alarm processing. The display and alarm processors acquire the information from the other plant instrumentation and control systems by means of the real-time data network, which is also part of the DDS.

The second layer contains the PMS. The PMS provides the safety reactor trip function, ESF actuation functions, and qualified plant monitoring function. In the PMS, both automatic and manual means are provided to trip the reactor and actuate the engineered safety features. The PMS contains sensors, plant protection subsystems, ESF coincidence logic, ESF actuation subsystems, logic buses, reactor trip switchgear, operator controls, QDPS, and qualified displays.

The third layer contains the DAS. The DAS provides nonsafety, reactor trip functions, actuation of engineered safety features, and operator displays. In the DAS, both automatic and manual means are provided to trip the reactor and actuate selected engineered safety features. The DAS also provides monitoring of plant parameters required to ascertain the state of the plant and provide guidance for manual actions by the operator. The DAS is implemented in hardware that is diverse from the PMS.

Figure 5-1 shows, on an overview basis, the relationships between components of the PLS, DAS, and PMS, and illustrates the means provided to accomplish the automatic and manual actions. This figure illustrates the sources of signals for automatic trips and actuations, and shows operator displays. It also shows the manual controls and operator displays that facilitate operator actions.

Figure 5-2 shows how diverse sensors, cabinets, and operator controls are integrated into the instrumentation and control architecture.

5.3 REACTOR SHUTDOWN

Reactor shutdown is the process of bringing the reactor to a subcritical state in a timely manner and maintaining an adequate shutdown margin. This function is normally provided by inserting the control rods into the core either in a controlled manner (stepping) or by dropping them.

- 5.3.1 The control rods can be automatically or manually stepped into the core. The PLS provides automatic insertion of the control rods using signals from various sensors in the PLS and PMS. The PLS also provides controls for manual insertion of the control rods. The final actuation devices for reactor shutdown via the PLS are the control rod drive mechanisms (CRDMs).
- 5.3.2 The PMS provides automatic reactor shutdown by dropping the rods using the reactor trip switchgear. When the reactor trip switchgear opens, the CRDMs are de-energized and the rods drop into the core by gravity. The PMS also provides a manual reactor shutdown by means of controls that directly interface with the reactor trip switchgear.
- 5.3.3 The DAS provides the capability for automatic reactor shutdown by de-energizing the rod drive motor/generator set that supplies power to the CRDMs. This is a diverse means of de-energizing the control rod drive mechanisms and has the same effect as opening the reactor trip switchgear. The DAS also provides the capability for manual reactor shutdown by de-energizing the rod drive motor/generator set.

5.4 REACTOR COOLANT SYSTEM INVENTORY CONTROL

RCS inventory control is the process of maintaining sufficient borated water in the RCS to maintain the heat removal capability.

- 5.4.1 During normal plant operation, the pressurizer level control function of the PLS automatically controls the operation of the nonsafety chemical and volume control system (CVS) to maintain RCS inventory. In the event of a small RCS leak, the CVS makeup pumps automatically start on a Low-2 pressurizer level signal. The makeup pumps also start automatically on a core makeup tank (CMT) actuation signal.

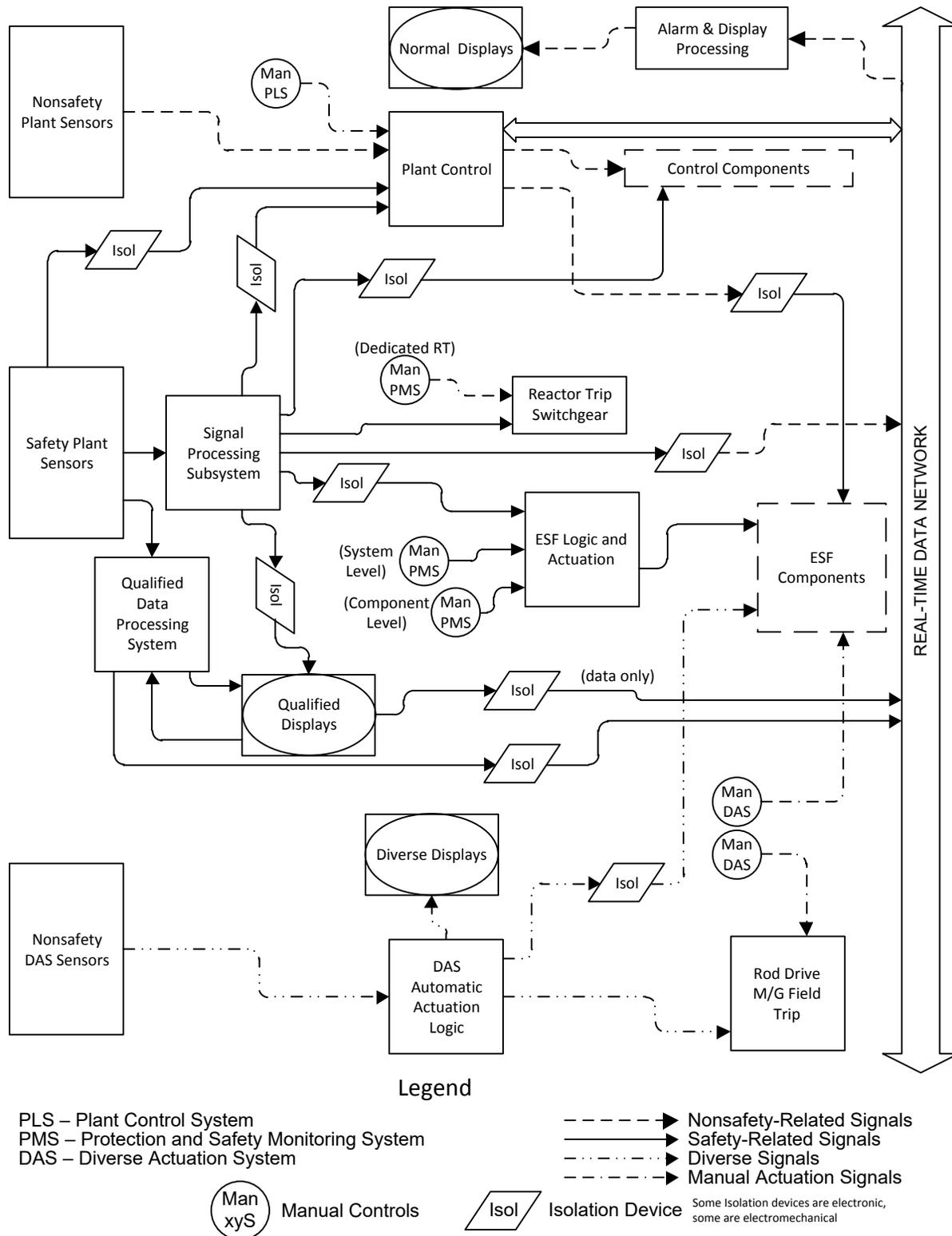


Figure 5-1. AP1000 Plant Instrumentation and Control Systems Diversity Architecture

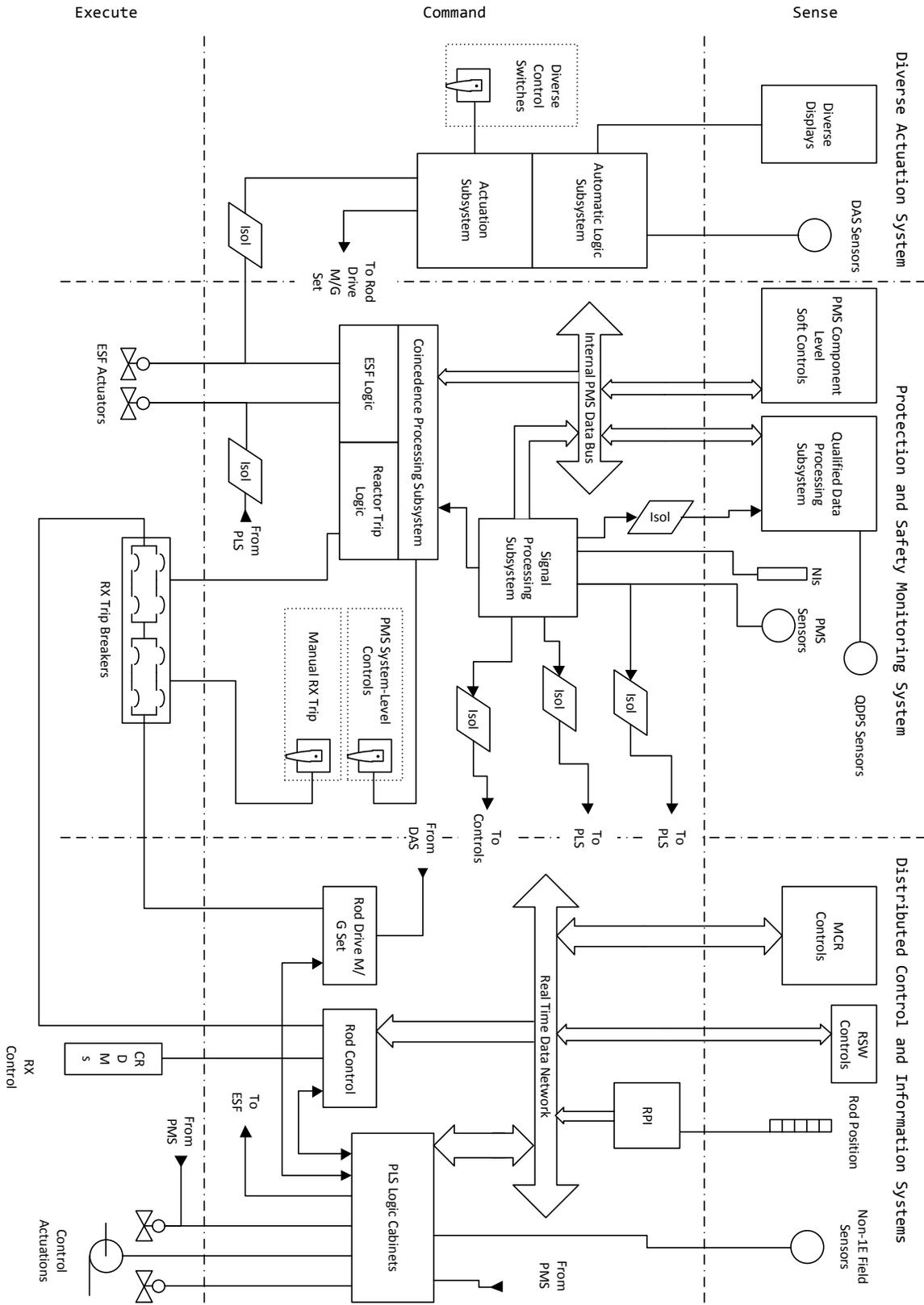


Figure 5-2. AP1000 Plant Diverse Instrumentation and Control Structure

- 5.4.2 The safety passive core cooling system (PXS) provides emergency core decay heat removal, RCS emergency makeup, boration, and safety injection. The PXS includes four sources of passive injection for RCS inventory control. These injection sources provide injection in a sequenced manner, based upon RCS pressure. The CMTs are normally the first injection source, providing makeup at any RCS pressure. The PMS automatically initiates CMT injection. The PMS also provides the capability for manual actuation of the CMTs using control devices, the logic buses, and the ESF actuation subsystem.
- 5.4.3 The DAS provides the capability for nonsafety automatic actuation of the CMT injection. The DAS also provides the capability for nonsafety manual actuation of CMT injection using dedicated, hardwired controls.
- 5.4.4 The other three PXS injection sources provide makeup once the RCS is depressurized. The automatic depressurization system (ADS) uses four valve stages to provide a controlled depressurization of the RCS. The PMS automatically initiates each ADS stage. The PMS provides the capability for manual actuation of the ADS using control devices, the logic buses, and the ESF actuation subsystem.
- 5.4.5 The DAS also provides the capability for manual actuation of the ADS using dedicated, hardwired controls for the valves in each stage.
- 5.4.6 The second PXS injection source is the accumulator tanks. Injection from the accumulators is initiated once RCS pressure is below the static pressure in the accumulators. The PMS actuates the accumulator discharge isolation valves, which are normally open, with actuation power removed, during plant power operation.
- 5.4.7 The nonsafety normal residual heat removal system (RNS) can be manually actuated to provide RCS injection once RCS pressure is reduced to within the capability of the RNS.
- 5.4.8 The third PXS makeup source is the in-containment refueling water storage tank (IRWST). During plant power operation, the PMS automatically initiates IRWST injection once RCS pressure is within the injection head capability of the IRWST.
- 5.4.9 During shutdown operations, the IRWST discharge isolation valves are normally closed with actuation power available. The PMS automatically opens these valves to initiate IRWST injection on a Low-4 RCS hot leg level. These valves can also be manually opened using the PMS.

The DAS also provides the capability for nonsafety manual actuation of the IRWST injection.

- 5.4.10 The fourth PXS makeup source is the containment recirculation volume of reactor coolant and makeup water that collects in the recirculation screen areas in containment following an event. The PMS automatically opens the containment recirculation valves. The PMS also provides the capability for manual actuation of the containment recirculation valves.

The DAS provides the capability for nonsafety manual actuation of containment recirculation valves.

5.5 CORE DECAY HEAT REMOVAL

Core decay heat removal is the process of maintaining a heat sink that is capable of cooling the reactor core after a reactor shutdown. A number of different systems can provide core decay heat removal. The system and components to be used for core heat removal will depend upon the plant operating mode. During some plant conditions, the same systems and components that maintain the RCS inventory provide core decay heat removal.

- 5.5.1 The nonsafety startup feedwater system supplies feedwater to the steam generators during non-power operation to provide core decay heat removal. The PLS automatically actuates the two nonsafety startup feedwater pumps and automatically controls feedwater flow to the steam generators. The startup feedwater pumps automatically start on either a low steam generator water level or low main feedwater flow signal. Startup feedwater flow control is based on the steam generator water level.
- 5.5.2 The PXS provides a safety core cooling process using the passive residual heat removal (PRHR) heat exchanger. The PMS automatically actuates the PRHR heat exchanger. The PMS also provides the capability for manual actuation of the PRHR heat exchanger using control devices, the logic buses, and the ESF actuation subsystem.
- 5.5.3 The DAS provides the capability for nonsafety automatic actuation of the PRHR heat exchanger. The DAS also provides the capability for manual actuation of the PRHR heat exchangers using dedicated, hardwired controls.
- 5.5.4 In addition to the startup feedwater system and the PRHR heat exchangers, core decay heat removal can also be automatically provided by the CMTs, accumulators, and IRWST, and manually provided by the nonsafety RNS, once RCS pressure has been reduced to within the capability of the RNS. Section 5.4 discusses the actuation of the components in these two systems.
- 5.5.5 During plant shutdown conditions before opening the RCS, core cooling is provided as discussed previously. During plant shutdown, some PXS components may not automatically actuate, but can be manually actuated, depending upon specific plant conditions. During these conditions, the RNS is normally operating and will automatically restart when power is restored following a loss of power to the RNS pumps.
- 5.5.6 During plant conditions when the RCS is not intact or with reduced RCS inventory (such as mid-loop operation), the RNS is normally operating and will automatically restart when power is restored following a loss of power to the RNS pumps. Various PXS components including the CMTs, accumulators, and PRHR heat exchangers are not available. The IRWST will automatically actuate on Low-4 RCS hot leg level. The IRWST can also be manually actuated.

5.6 CONTAINMENT COOLING

Containment cooling is the process of removing heat from the containment.

- 5.6.1 Nonsafety fan coolers normally provide containment cooling during power operation. The PLS is used to control the operation of the fan coolers.
- 5.6.2 If the fan coolers are unavailable or have insufficient capacity for the containment heat loads, the PMS automatically actuates the safety passive containment cooling system (PCS) to provide containment cooling. The PMS also provides the capability for manual control of the PCS using control devices, the logic buses, and the ESF actuation subsystem.
- 5.6.3 The DAS provides the capability for nonsafety automatic actuation of the PCS. The DAS also provides the capability for manual actuation of the PCS using dedicated, hardwired controls.

5.7 CONTAINMENT ISOLATION

Containment isolation is the process of closing safety valves in fluid lines that penetrate the containment to minimize the release of radioactivity from containment, following an event.

- 5.7.1 PMS provides automatic containment isolation by actuating the containment isolation valves on a safeguards actuation signal. The PMS also provides the capability for manual actuation of containment isolation valves using control devices, the logic buses, and the ESF actuation subsystem.
- 5.7.2 The DAS provides the capability for nonsafety automatic actuation of key containment isolation valves on high containment temperature. The DAS also provides the capability for manual containment isolation capability using dedicated, hardwired controls.

5.8 EVENT SCENARIOS

WCAP-13793, “AP600 System/Event Matrix” (Reference 5) contains a series of flowcharts and tables that illustrate these levels of defense, from an operational point of view, for a selected number of full power and shutdown events. WCAP-13793 is an AP600 document that is applicable to the **AP1000** plant.

6 REFERENCES

1. NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," March 1979.
2. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems," October 21, 1994.
3. Deleted.
4. Deleted
5. WCAP-13793, Rev.2, "AP600 System/Event Matrix," Westinghouse Electric Company LLC.
6. APP-GW-GL-700, Rev. 19, "**AP1000** Design Control Document," Westinghouse Electric Company LLC.
7. APP-GW-GL-022, Rev. 8, "**AP1000** Probabilistic Risk Assessment," Westinghouse Electric Company LLC.
8. IEEE 384-1981, "IEEE Criteria for Independence of Class 1E Equipment and Circuits."
9. WCAP-17179-P, Rev. 6, "**AP1000** Component Interface Module Technical Report," Westinghouse Electric Company LLC.
10. WCAP-16096-P-A, Rev. 4, "Software Program Manual for Common Q Systems," Westinghouse Electric Company LLC.
11. WCAP-15927, Rev. 6, "Design Process for **AP1000** Common Q Safety Systems," Westinghouse Electric Company LLC.

Southern Nuclear Operating Company

ND-21-0486

Enclosure 9

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

WCAP-15871, "AP1000 Assessment Against NFPA 804," Revision 7

(Enclosure 9 consists of 76 pages, plus this cover page)

WCAP-15871
Revision 7

August 2020

AP1000 Assessment Against NFPA 804



WCAP-15871
Revision 7

AP1000 Assessment Against NFPA 804

Thomas A. Runyan, Jr.*
Fire Protection Engineering

August 2020

Reviewer: Warren R. Odess-Gillett*
Structural & Mechanical Licensing
Advanced Analysis & Risk Applications

Approved: Lary J. Rosenbloom*, Manager
Fire Protection Engineering

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

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

© 2020 Westinghouse Electric Company LLC
All Rights Reserved

RECORD OF REVISIONS

Revision	Section	Description of Change
0	All	Initial Issue
1	2.4 (6)	Changed from: [NC. Not included in AP1000 fire protection analysis.], to: [Comply. Release of contamination. NC. Other areas not included in AP1000 fire protection analysis.].
	3.3.1.5	Changed from: [The AP1000 fire protection design criteria document applies NFPA 50A by reference to NFPA 803, it does not apply to NFPA 50B.], to: [Comply.].
	5.3.1.10.1	Changed from: [AC – The AP1000 fire hazards analysis assumes a single worst case spurious actuation regardless of cable failure mode except for valve motor operators.], to: [AC – The AP1000 fire hazards analysis assumes spurious actuations regardless of cable failure mode except for valve motor operators. The spurious actuations are postulated one at a time (except for high/low pressure interfaces). Spurious actuation of the redundant valves in any one high-low pressure interface line are postulated if the circuits for those valves are located in the fire area. The spurious actuations that are evaluated are those that could cause a breach in the reactor coolant boundary or defeat safety-related decay heat removal capability or cause an increase in shutdown reactivity of the reactor.].
	Chapter 9	Changed from: [Chapter 9: The AP1000 fire protection criteria document requires conformance to NFPA 803 requirements for the construction period. NFPA 804 Chapter 9 requirements are more prescriptive than those in NFPA 803. A detailed comparison of the NFPA 804 Chapter 9 requirements with the AP1000 construction plan has not been made.], to: [N/A – Heading].
2	6.4.10.4	Changed from: [N/A – AP1000 has no charcoal adsorber beds containing more than 100 lb (45.4 kg) of charcoal.], to: [Comply]; Change made per DCP No. APP-GW-GEE-483.
3	6.2.1	Changed from: [Comply], to: [NC. Deviations from the Life Safety Code's exit and egress requirements are identified and the degree of life safety justified in the Means of Egress Studies.]; Change made per DCP No. APP-GW-GEE-3037.
4	6.4.10.4	DCP No. APP-GW-GEE-4940 was reviewed and no changes were found that directly impacted this document. Changed from: [Comply] to: [AC - HVAC charcoal beds are provided with fixed water spray systems. The WGS charcoal adsorber beds are provided with a permanent connection from a nitrogen purge line to allow nitrogen to be injected into the enclosed space containing the charcoal to extinguish a fire.]; Change made per DCP No. APP-GW-GEE-4922.
	8.3.1	Changed from: [Comply - except AP1000 does not have automatic smoke dampers installed in the fire barrier walls between the main control room and the peripheral rooms.], to: [Comply - The MCR/Operator Work Area wall is not fire-rated based on other design criteria. Manual fire suppression is

Revision	Section	Description of Change
	8.3.5	provided for peripheral rooms. See Appendix 9A of the Design Control Document.]; Change made per DCP No. APP-GW-GEE-4977.
	6.3.2.1	Changed from: [Comply], to: [NC - Smoke detectors are not provided in cabinets and consoles. The control room is continuously occupied so that a fire is promptly detected and extinguished.]; Change made per DCP No. APP-GW-GEE-4977.
	6.3.2.2	Changed from: [Comply] to: [NC - Protective Coatings used as interior wall and ceiling finishes meet the criteria of noncombustible from the BTP CMEB 9.5-1 Regulatory Position C.5.(a).9.]; Change made per DCP No. APP-GW-GEE-5266.
5	6.1.2.2	Changed from: [Comply] to: [NC. Auxiliary building stairwells and elevator shafts, with exception of the exterior wall sections enclosing Stairwell S03 and the wall separating Stairwell S03 from the elevator shaft above the Auxiliary Building Roof as described in Section 9A of the DCD. For buildings outside of the Nuclear Island, exterior wall sections enclosing stairwells and elevator shafts do not have a fire resistance rating of 2 hours, only interior stairwell and elevator shaft wall sections are rated for the minimum 2 hour fire resistance rating.]; Change made per DCP No. APP-GW-GEE-5366.
	6.4.10.1	Changed from: [Comply] to: [AC - Filters will be listed for UL 900. As of May 2012, Class 1 filters are obsolete as UL no longer lists filters to the former Class 1 criteria.]; Change made per DCP No. APP-GW-GEE-4948.
6	6.1.2.2	Revised the AP1000 Compliance Statement to include additional clarification. The following clarification was added to the statement: [, are enclosed in towers constructed using both concrete structural walls and nonstructural walls]; Change made per E&DCR No. APP-FSAR-GEF-086. LID completed by reference.
	7.4.10.3	Changed from: [Comply] to: [AC - The seismic standpipe system is operated in the same manner during normal plant operation or following a safe shutdown earthquake. It is supplied with water from the safety related passive containment cooling system storage tank and normally operates independently of the rest of the fire protection system. The supply line draws water from a portion of the storage tank, using water allocated for fire protection. This volume of water is sufficient to supply two hose streams, each with a flow of 75 gallons per minute, for 2 hours as required by BTP CMEB 9.5-1, Revision 2 (July 1981).]; Change made per E&DCR No. APP-FSAR-GEF-086. LID completed by reference.
7	6.1.3.2.2	Changed from: [Comply] to: [AC. For temperature criteria for the unexposed side of the fire barrier, RG 1.189 Rev. 1, Section

Revision	Section	Description of Change
		4.2.1.5b.ii is used: “The temperature levels recorded for the unexposed side of the fire barrier are analyzed and demonstrate that the maximum temperature does not exceed 163 °C (325 °F) or 121 °C (250 °F) above the ambient temperature. Higher temperatures at through-penetrations may be permitted when justified in terms of cable insulation ignitability.”]; Change made per E&DCR No. APP-FSAR-GEF-172. LID completed by reference.

Trademark Note:

AP1000 is a trademark of Westinghouse Electric Company LLC.

TABLE OF CONTENTS

LIST OF TABLES		vii
LIST OF FIGURES		viii
WCAP INTRODUCTION AND LEGEND.....		Page 1
NFPA 804 Section	Title	Page
1	INTRODUCTION	2
1.1	Scope.....	2
1.2	Purpose	2
1.3	Equivalency Concepts.....	2
1.4	Definitions	2
2	FIRE PROTECTION PROGRAM	6
2.1	General.....	6
2.2	Management Policy Direction and Responsibility.....	7
2.3	Fire Prevention Program	7
2.4	Fire Hazards Analysis	7
2.5	Procedures.....	8
2.6	Quality Assurance	9
2.7	Fire Emergency Plan.....	9
2.8	Fire Brigade	10
3	FIRE PROTECTION AND ADMINISTRATIVE CONTROLS	10
3.1	General.....	10
3.2	Plant Inspections	10
3.3	Control of Combustible Materials	10
3.4	Control of Ignition Sources.....	13
3.5	Temporary Structures.....	14
3.6	Impairments	16
3.7	Testing and Maintenance.....	16
4	MANUAL FIRE FIGHTING.....	16
4.1	Prefire Plans	16
4.2	On-Site Fire-Fighting Capability	17
4.3	Training and Drills	17
4.4	Fire-Fighting Equipment.....	18
4.5	Off-Site Fire Department Interface	18
4.6	Water Drainage	19
4.7	Fire-Fighting Access	19
4.8	Radiation Shielding.....	19
4.9	Smoke and Heat Removal.....	19

TABLE OF CONTENTS (cont.)

NFPA 804 Section	Title	Page
5	NUCLEAR REACTOR SAFETY CONSIDERATIONS	19
5.1	General	19
5.2	Fire Hazards and Safe Shutdown Analysis (FSSA)	19
5.3	Design Basis Events and Requirements	20
5.4	Separation Criteria	24
5.5	Manual Actions	25
5.6	Alternative Shutdown Capability	26
6	GENERAL PLANT DESIGN	26
6.1	Plant Arrangement	26
6.2	Life Safety	29
6.3	Building and Construction Materials	30
6.4	Ventilation	31
6.5	Drainage	34
6.6	Emergency Lighting	36
6.7	Lightning Protection	36
6.8	Electrical Cabling	37
6.9	Exposure Protection	38
6.10	Electrical Systems for the Plant	38
6.11	Communications	38
7	GENERAL FIRE PROTECTION SYSTEMS AND EQUIPMENT	38
7.1	General	38
7.2	Water Supply	39
7.3	Valve Supervision	41
7.4	Yard Mains, Hydrants, and Building Standpipes	41
7.5	Portable Fire Extinguishers	43
7.6	Fire Suppression Systems	43
7.7	Fire Alarm Systems	44
7.8	Fire Detectors	45
8	IDENTIFICATION OF AND PROTECTION AGAINST HAZARDS	45
8.1	General	45
8.2	Primary and Secondary Containments	45
8.3	Control Room Complex	47
8.4	Cable Concentrations	48
8.5	Plant Computer and Communication Rooms	49
8.6	Switchgear Rooms and Relay Rooms	50
8.7	Battery Rooms	50
8.8	Turbine Building	50
8.9	Standby Emergency Diesel Generators and Combustion Turbines	53
8.10	Diesel Fuel Storage and Transfer Areas	54
8.11	Nuclear Safety-Related Pump Rooms	54

TABLE OF CONTENTS (cont.)

NFPA 804 Section	Title	Page
8.12	New Fuel Area	54
8.13	Spent Fuel Pool Area	54
8.14	Rad Waste and Decontamination Areas	55
8.15	Safety-Related Water Tanks	55
8.16	Record Storage Areas.....	55
8.17	Cooling Towers	55
8.18	Acetylene-Oxygen Fuel Gases.....	55
8.19	Storage Areas for Ion Exchange Resins.....	55
8.20	Storage Areas for Hazardous Chemicals.....	55
8.21	Warehouses	55
8.22	Fire Pump Room/House.....	55
8.23	Transformers	56
8.24	Auxiliary Boilers.....	56
8.25	Offices, Shops, and Storage Areas	57
8.26	Simulators	57
8.27	Technical Support and Emergency Response Centers	57
8.28	Intake Structures	57
9	FIRE PROTECTION FOR THE CONSTRUCTION SITE	57
9.1	General.....	57
9.2	Administration	57
9.3	Site Clearing and Construction Equipment.....	58
9.4	Construction Warehouses, Shops, and Offices.....	58
9.5	Construction Site Lay-Down Areas	60
9.6	Temporary Construction Materials	60
9.7	Water Supplies, Supply Mains, and Hydrants.....	60
9.8	Manual Fire-Fighting Equipment	61
10	REFERENCED PUBLICATIONS	62

LIST OF TABLES

NFPA 804 Table	Title	Page
3.5.1.2	Minimum Separation Distances	15
8.23.1	Transformer Spacing Separation Distances.....	56

LIST OF FIGURES*

NFPA 804 Figure	Title	Page
8.23.1(a)	Transformer Spacing.....	56
8.23.1(b)	Transformer Spacing.....	56

* The actual figures are not recreated in this WCAP. Only a compliance assessment appears.

WCAP INTRODUCTION AND LEGEND

The purpose of this WCAP is to compare the AP1000 fire protection design to the requirements of NFPA 804 (2001 Edition). The comparison that appears on the following pages is performed on a paragraph basis. The comparison is by Westinghouse to support the AP1000 Design Certification. Compliance promises are for Westinghouse as the plant designer, not for the combined license applicant or the owner/operator, who must comply separately. The only reference besides NFPA 804 is the AP1000 Design Control Document (DCD), APP-GW-GL-701, Rev. 19. The following legend is provided to assist in interpreting the results.

Legend	AP1000 Compliance Statement
N/A	The paragraph is not applicable to the AP1000 design
N/A - Heading	The paragraph is not applicable as it is only a section heading
N/A - See Below	The paragraph is a lead-in statement for the requirements that follow
N/A - General	The paragraph contains no requirements
Comply	The AP1000 design complies or intends to comply with this paragraph
AC	The AP1000 design complies with the requirement by alternate means or intent. The alternate means or design is provided in the compliance statement.
COL	The Combined License applicant (COL) will address this paragraph
O/O	The plant owner/operator will address this paragraph
NC	The AP1000 design does not comply with this paragraph

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
Chapter 1 Introduction	N/A - Heading
1.1* Scope. This standard applies only to advanced light water reactor electric generating plants, and provides minimum fire protection requirements to ensure safe shutdown of the reactor, minimize the release of radioactive materials to the environment, provide safety to life of on-site personnel, limit property damage, and protect continuity of plant operation. The fire protection is based upon the principle of defense in depth.	N/A - General
1.2 Purpose. This standard is prepared for the use and guidance of those charged with the design, construction, operation, and regulation of advanced light water reactor electric generating plants. This standard covers those requirements essential to ensure that the consequences of fire will have minimum impact on the safety of the public and on-site personnel, the physical integrity of plant components, and the continuity of plant operations.	N/A - General
1.3 Equivalency Concepts.	N/A - Heading
1.3.1 Nothing in this standard is intended to prevent the use of systems, methods, or devices of equivalent or superior quality, strength, fire resistance, effectiveness, durability, and safety over those prescribed by this standard. Technical documentation shall be submitted to the authority having jurisdiction to demonstrate equivalency. The system, method, or device shall be approved for the intended purpose by the authority having jurisdiction.	N/A - General
1.3.2 The specific requirements of this standard shall be permitted to be modified by the authority having jurisdiction to allow alternative arrangements that will secure as nearly as practical the level of fire protection intended by this document, but in no case shall the modification afford less fire protection than that which, in the judgment of the authority having jurisdiction, would be provided by compliance with the corresponding provisions contained in this standard.	N/A - General
1.3.3 Alternative fire protection methods accepted by the authority having jurisdiction shall be considered as conforming with this standard.	N/A - General
1.4 Definitions.	N/A - Heading
1.4.1* Advanced Light Water Reactors (ALWRs). ALWRs are next generation light water reactors.	N/A - General
1.4.2 Alternative Shutdown Capability. The ability to safely shut down the reactor and maintain shutdown using equipment and processes outside the normal reactor shutdown process.	N/A - General
1.4.3* Approved. Acceptable to the authority having jurisdiction.	N/A - General

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
1.4.4* Associated Circuits of Concern. Safety-related and non-safety-related circuits that are not directly required to perform a safe shutdown function and that do not have a required physical separation.	N/A - General
1.4.5* Authority Having Jurisdiction. The organization, office, or individual responsible for approving equipment, materials, an installation, or a procedure.	N/A - General
1.4.6 Cable Tray Fire Break. A noncombustible or limited-combustible material installed in vertical or horizontal cable trays to limit fire spread.	N/A - General
1.4.7 Cold Shutdown. A stable nuclear power plant condition in which the affected reactor is subcritical and the average reactor coolant system temperature is less than or equal to 200°F (93°C).	N/A - General
1.4.8* Combustible. Capable of undergoing combustion.	N/A - General
1.4.9 Combustible Liquid. A liquid that has a closed-cup flash point at or above 100°F (37.8°C).	N/A - General
1.4.10* Defense in Depth. A principle aimed at providing a high degree of fire protection by achieving a balance of preventing fires from starting; detecting fires quickly and suppressing those fires that occur, thereby limiting damage; and designing a nuclear power plant to limit the loss of life, property, and environment to fire and to ensure continuity of nuclear power plant operation and safe shutdown capability.	N/A - General
1.4.11* Fire Area. An area that is physically separated from other areas by space, barriers, walls, or other means in order to contain fire within that area.	N/A - General
1.4.12* Fire Area Subdivision. A portion of a fire area that is separated from the remainder of the fire area by substantive barriers, which are not necessarily fire rated; by physical features, such as pipe tunnels; by spatial separation.	N/A - General
1.4.13 Fire Barrier. A continuous vertical or horizontal construction assembly designed and constructed to limit the spread of heat and fire and to restrict the movement of smoke.	N/A - General
1.4.14* Fire Brigade. As used in this standard, refers to those on-site persons trained in plant fire-fighting operations.	N/A - General
1.4.15 Fire Door. A door assembly rated in accordance with NFPA 252, <i>Standard Methods of Fire Tests of Door Assemblies</i> , and installed in accordance with NFPA 80, <i>Standard for Fire Doors and Fire Windows</i> .	N/A - General
1.4.16 Fire Hazards Analysis (FHA). An analysis to evaluate potential fire hazards and appropriate fire protection systems and features to mitigate the effects of fire in any plant location.	N/A - General
1.4.17 Fire Prevention. Measures directed toward avoiding the inception of fire.	N/A - General

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
1.4.18 Fire Protection. Methods of providing fire detection, control, and extinguishment.	N/A - General
1.4.19 Fire Protection Manager. The person directly responsible for the fire prevention and fire protection program at the plant.	N/A - General
1.4.20* Fire-Rated Cables. Cables with an hourly fire resistance rating based on maintaining functionality when exposed to fire tests in NFPA 251, <i>Standard Methods of Tests of Fire Endurance of Building Construction and Materials</i> .	N/A - General
1.4.21 Fire-Rated Internal Conduit Seal. A conduit seal that is a tested and approved hourly rated fire seal in accordance with ASTM E 814, <i>Fire Tests of Through-Penetration Fire Stops</i> .	N/A - General
1.4.22 Fire-Rated Penetration Seal. An assembly provided in a fire barrier opening for the passage of pipes, cable trays, and so forth, to maintain the fire resistance rating of the fire barrier.	N/A - General
1.4.23 Fire Resistance Rating. The time, in minutes or hours, that materials or assemblies have withstood a fire exposure as established in accordance with an approved test procedure appropriate for the component under consideration.	N/A - General
1.4.24 Fire Safe Shutdown. Actions, components, capabilities, and design features necessary to achieve and maintain safe shutdown of the reactor after a fire in a specific fire area.	N/A - General
1.4.25* Fire-Safe Shutdown Component (FSSD). Components (nuclear safety related and non-safety related), equipment, instrument-sensing line, or cable, including associated circuits of concern, that are required to safely shut down a nuclear plant in the event of fire.	N/A - General
1.4.26* First Break. The first place in a conduit run where the interior of the conduit is accessible to install a seal.	N/A - General
1.4.27 Flame Spread Rating. A relative measurement of the surface burning characteristics of building materials when tested in accordance with NFPA 255, <i>Standard Method of Test of Surface Burning Characteristics of Building Materials</i> .	N/A - General
1.4.28 Flammable Liquid. A liquid that has a closed-cup flash point that is below 100°F (37.8°C) and a maximum vapor pressure of 40 psia (2068 mm Hg) at 100°F (37.8°C).	N/A - General
1.4.29 Free of Fire Damage. The structure, system, or component under consideration is capable of performing its intended function during and after the postulated fire, as needed.	N/A - General

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
1.4.30 High Impedance Faults. Fire-induced faults on non-safe shutdown essential circuits routed through a common fire area that are assumed to occur simultaneously and have a current magnitude below the trip point for the individual circuits and the sum of the currents generated by the simultaneous occurrence of such faults could trip the main circuit breaker and cause the loss of a safe shutdown power supply.	N/A - General
1.4.31* High-Low Pressure Interface. A valve or set of valves that separates a high-pressure primary coolant system from a low-pressure system.	N/A - General
1.4.32 Labeled. Equipment or materials to which has been attached a label, symbol, or other identifying mark of an organization that is acceptable to the authority having jurisdiction and concerned with product evaluation, that maintains periodic inspection of production of labeled equipment or materials, and by whose labeling the manufacturer indicates compliance with appropriate standards or performance in a specified manner.	N/A - General
1.4.33 Limited-Combustible. A building construction material not complying with the definition of noncombustible material that, in the form in which it is used, has a potential heat value not exceeding 3500 Btu/lb (8141 kJ/kg), where tested in accordance with NFPA 259, <i>Standard Test Method for Potential Heat of Building Materials</i> , and complies with (a) or (b) below. Materials subject to increase in combustibility or flame spread index beyond the limits herein established through the effects of age, moisture, or other atmospheric condition shall be considered combustible. (a) Materials having a structural base of noncombustible material, with a surfacing not exceeding a thickness of 1/8 in. (3.2 mm) that has a flame spread index not greater than 50. (b) Materials, in the form and thickness used, other than as described in (a), having neither a flame spread index greater than 25 nor evidence of continued progressive combustion and of such composition that surfaces that would be exposed by cutting through the material on any plane would have neither a flame spread index greater than 25 nor evidence of continued progressive combustion.	N/A - General
1.4.34* Listed. Equipment, materials, or services included in a list published by an organization that is acceptable to the authority having jurisdiction and concerned with evaluation of products or services, that maintains periodic inspection of production of listed equipment or materials or periodic evaluation of services, and whose listing states that either the equipment, material, or service meets appropriate designated standards or has been tested and found suitable for a specified purpose.	N/A - General
1.4.35 Noncombustible. Not capable of supporting combustion.	N/A - General
1.4.36 Normal Operations. All modes of non-emergency nuclear power plant operation, ranging from 0 percent to 100 percent power, which include refueling outages but do not include extended outages when fuel is removed from the reactor.	N/A - General

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
1.4.37* Nuclear Safety Function. Any function that is necessary to ensure the integrity of the reactor coolant pressure boundary; the capability to shut down the reactor and maintain it in a safe shutdown condition; or the capability to prevent or mitigate the consequences of nuclear power plant conditions that could result in the potential for a significant fraction of allowable off-site releases.	N/A - General
1.4.38* Nuclear Safety Related. Structures, systems, or components that are required to remain functional to ensure the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition, or the capability to prevent or mitigate the consequences of accidents that could result in potential off-site exposures comparable to regulatory guideline exposures.	N/A - General
1.4.39 Postulated Fire. A fire that is assumed to occur in a specific area of a nuclear plant.	N/A - General
1.4.40* Power Block. Structures that have equipment required for nuclear plant operations.	N/A - General
1.4.41 Redundant Component, System, or Subsystem. A component, system, or subsystem that independently duplicates the essential function of another component, system, or subsystem.	N/A - General
1.4.42 Safe Shutdown. A shutdown with the reactivity of the reactor kept subcritical as specified by the technical specifications for the unit.	N/A - General
1.4.43* Safety Division. The designation applied to a given system or set of nuclear-safety-related components that enable the establishment and maintenance of physical, electrical, and functional independence from other redundant systems or sets of components.	N/A - General
1.4.44 Shall. Indicates a mandatory requirement.	N/A - General
1.4.45 Should. Indicates a recommendation or that which is advised but not required.	N/A - General
1.4.46* Spurious Operation. An unwanted change in state of equipment due to fire-induced faults (e.g., hot shorts, open circuits, or shorts to ground) on its power or control circuitry.	N/A - General
1.4.47 Spurious Signal. A fire-induced signal that could cause the spurious operation of components or equipment, which would adversely affect the safe shutdown capability.	N/A - General
Chapter 2 Fire Protection Program	N/A - Heading
<p>2.1* General. All elements of the site fire protection program shall be reviewed every two years, and updated as necessary.</p> <p><i>Exception: Other review frequencies are acceptable where specified in site administrative procedures and approved by the authority having jurisdiction.</i></p>	O/O

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
2.2 Management Policy Direction and Responsibility.	N/A - Heading
2.2.1 A policy document shall be prepared that defines management authorities and responsibilities and establishes the general policy for the site fire protection program.	COL
2.2.2 The policy document shall designate the senior management person with immediate authority and responsibility for the fire protection program.	COL
2.2.3 The policy document shall define the fire protection interfaces with other organizations and assign responsibilities for the coordination activities.	COL
2.2.4 The policy document shall include the authority for conflict resolution.	COL
2.3 Fire Prevention Program. A fire prevention program shall be established and documented to include all of the following: (1) Fire safety information for all employees and contractors, including as a minimum familiarization with plant fire prevention procedures, fire reporting, and plant emergency alarms, including evacuation (2) Documented plant inspections, including provisions for handling of remedial actions to correct conditions that increase fire hazards (3) A procedure for the control of general housekeeping practices and the control of transient combustibles (4) Procedures for the control of flammable and combustible gases in accordance with NFPA standards (5) Procedures for the control of ignition sources, such as smoking, welding, cutting, and grinding (<i>see NFPA 51B, Standard for Fire Prevention During Welding, Cutting, and Other Hot Work</i>) (6) A fire prevention surveillance plan (<i>see NFPA 601, Standard for Security Service in Fire Loss Prevention</i>) (7) A fire reporting procedure, including investigation requirements and corrective action requirements	COL
2.4* Fire Hazards Analysis. A documented fire hazards analysis shall be made for each site. The analysis shall document all of the following: (1) The physical construction and layout of the buildings and equipment, including fire areas and the fire ratings of area boundaries (2) *An inventory of the principal combustibles within each fire subdivision (3) A description of the fire protection equipment, including alarm systems and manual and automatic extinguishing systems	N/A - See Below Comply Comply Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
(4) A description of any equipment necessary to ensure a safe shutdown, including cabling and piping between equipment, and the location of such equipment	Comply
(5) An analysis of the postulated fire in each fire area, including its effect on safe shutdown equipment, assuming automatic and manual fire protection equipment does not function	Comply
(6) An analysis of the potential effects of a fire on life safety, release of contamination, impairment of operations, and property loss, assuming the operation of installed fire extinguishing equipment	Comply. Release of contamination. NC. Other areas not included in AP1000 fire protection analysis.
(7) An analysis of the potential effects of other hazards, such as earthquakes, storms, and floods, on fire protection	AC. Not included in AP1000 fire protection analysis, but is included in other sections of the AP1000 DCD.
(8) An analysis of the potential effects of an uncontained fire in causing other problems not related to safe shut-down, such as a release of contamination and impairment of operations	NC. Not included in AP1000 fire protection analysis
(9) An analysis of the postfire recovery potential	NC. Not included in AP1000 fire protection analysis
(10) An analysis for the protection of nuclear-safety-related systems and components from the inadvertent actuation or breaks in a fire protection system	Comply
(11) An analysis of the smoke control system, and the impact smoke can have on nuclear safety and operation for each fire area	Comply
(12) An analysis of the emergency planning and coordination requirements necessary for effective loss control. This shall include any necessary compensatory measures to compensate for the failure or inoperability of any active or passive fire protection system or feature.	COL
2.5 Procedures. A formal procedure system for all actions pertaining to the fire protection program shall be established. This shall include all of the following:	N/A - See Below
(1) Inspection, testing, maintenance, and operation of fire protection systems and equipment, both manual and automatic, such as detection and suppression systems	COL
(2) Inspection, testing, and maintenance of passive fire protection features, such as fire barriers and penetration seals	COL
(3) Trend analysis requirements	COL
(4) Provisions for entering areas with access restrictions	COL
(5) Training requirements	COL

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
2.6 Quality Assurance.	N/A - Heading
<p>2.6.1 A quality assurance program shall be established in accordance with ASME NQA-1, <i>Quality Assurance Program Requirements for Nuclear Facilities</i>, for all of these aspects of the fire protection program related to nuclear safety:</p> <p>(1) Design and procurement document control</p> <p>(2)* Instructions, procedures, and drawings</p> <p>(3)* Control of purchased material, equipment, and services</p> <p>(4)* Inspection</p> <p>(5)* Test and test control</p> <p>(6)* Inspection, test, and operating status</p> <p>(7)* Nonconforming items</p> <p>(8)* Corrective action</p> <p>(9)* Records</p> <p>(10)* Audits</p>	<p>Comply</p> <p>Comply</p> <p>Comply</p> <p>Comply</p> <p>Comply, COL</p> <p>Comply, COL</p> <p>COL</p> <p>Comply</p> <p>Comply</p> <p>Comply</p> <p>Comply</p>
2.6.2 The quality assurance program shall be documented in sufficient detail to verify its scope and adequacy.	Comply, COL
<p>2.7 Fire Emergency Plan. A written fire emergency plan shall be established. As a minimum, this plan shall include the following:</p> <p>(1) Response to fire and supervisory alarms</p> <p>(2) Notification of plant and public emergency forces</p> <p>(3) Evacuation of personnel</p> <p>(4) Coordination with security, maintenance, operations, and public information personnel</p> <p>(5) Fire extinguishment activities</p>	COL

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
(6) Postfire recovery and contamination control activities (7) Control room operations during an emergency (8) Prefire plan (9) A description of interfaces with emergency response organizations, security, safety, and others having a role in the fire protection program, including agreements with outside assistance agencies such as fire departments and rescue services	
2.8 Fire Brigade. A plant fire brigade shall be established as indicated in Chapter 4.	N/A -COL
Chapter 3 Fire Protection and Administrative Controls	N/A - Heading
3.1* General.	N/A - Heading
3.2 Plant Inspections.	N/A - Heading
3.2.1 The owner or his or her designated manager shall develop, implement, and update as necessary a fire prevention surveillance plan integrated with recorded rounds to all accessible sections of the plant.	O/O
3.2.2 Inspections of the plant shall be conducted in accordance with NFPA 601, <i>Standard for Security Services in Fire Loss Prevention</i> . A prepared checklist shall be used for the inspection. Areas of primary containment and high radiation areas normally inaccessible during plant operation shall be inspected as plant conditions permit but at least during each refueling outage. The results of each inspection shall be documented and retained for two years. <i>Exception: For those plant areas inaccessible for periods greater than two years, the most recent inspection shall be retained.</i>	O/O
3.3 Control of Combustible Materials.	N/A - Heading
3.3.1* Plant administrative procedures shall specify appropriate requirements governing the storage, use, and handling of flammable and combustible liquids and flammable gases.	COL
3.3.1.1* An inventory of all temporary flammable and combustible materials shall be made for each fire area, identifying the location, type, quantity, and form of the materials.	O/O
3.3.1.2* Temporary but predictable and repetitive concentrations of flammable and combustible materials shall be considered.	COL

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
3.3.1.3 Combustibles, other than those that are an inherent part of the operation, shall be restricted to designated storage compartments or spaces.	O/O
3.3.1.4 Consideration shall be given to reducing the fire hazard by limiting the amount of combustible materials.	Comply
3.3.1.5 The storage and use of hydrogen shall be in accordance with NFPA 50A, <i>Standard for Gaseous Hydrogen Systems at Consumer Sites</i> , and NFPA 50B, <i>Standard for Liquefied Hydrogen Systems at Consumer Sites</i> .	Comply
3.3.1.6 The temporary use of wood shall be minimized. Plant administrative procedures shall specify that if wood must be used in the power block, it shall be listed pressure-impregnated fire-retardant lumber.	O/O
3.3.2 Housekeeping.	N/A - Heading
3.3.2.1 Housekeeping shall be performed in such a manner as to minimize the probability of fire.	O/O
3.3.2.2 Accumulations of combustible waste material, dust, and debris shall be removed from the plant and its immediate vicinity at the end of each work shift or more frequently as necessary for safe operations.	O/O
3.3.3 Transient Combustible Loading.	N/A - Heading
3.3.3.1* Plant administrative procedures shall require that the total fire loads, including temporary and permanent combustible loading, will not exceed those quantities established for extinguishment by permanently installed fire protection systems and equipment. <i>Exception: Where limits are temporarily exceeded, the plant fire protection manager shall assure that appropriate fire protection measures are provided.</i>	O/O
3.3.3.2 The fire protection manager or his or her designated representative shall conduct weekly walk-through inspections to ensure implementation of required controls. During major maintenance operations, the frequency of these walk-throughs shall be increased to daily. The results of these inspections shall be documented and the documentation retained for a minimum of two years.	O/O
3.3.3.3 When the work is completed, the plant fire protection manager shall have the area inspected to confirm that transient combustible loadings have been removed from the area. Extra equipment shall then be returned to its proper location. The results of this inspection shall be documented and retained for two years.	O/O

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
<p>3.3.3.4* Only noncombustible panels or flame-retardant tarpaulins or approved materials of equivalent fire-retardant characteristics shall be used. Any other fabrics or plastic films used shall be certified to conform to the large-scale fire test described in NFPA 701, <i>Standard Methods of Fire Tests for Flame Propagation of Textiles and Films</i>.</p>	COL
<p>3.3.4 Flammable and Combustible Liquids.</p>	N/A - Heading
<p>3.3.4.1 Flammable and combustible liquid storage and use shall be in accordance with NFPA 30, <i>Flammable and Combustible Liquids Code</i>. Where oil-burning equipment, stationary combustion engines, or gas turbines are used, they shall be installed and used in accordance with NFPA 31, <i>Standard for the Installation of Oil-Burning Equipment</i>, or NFPA 37, <i>Standard for the Installation and Use of Stationary Combustion Engines and Gas Turbines</i>, as appropriate.</p>	Comply
<p>3.3.4.2 Flammable and combustible liquid and gas piping shall be in accordance with ANSI B31.1, <i>Code for Power Piping</i>, or ASME <i>Boiler and Pressure Vessel Code</i>, Section III, as applicable.</p>	Comply
<p>3.3.4.3 Hydraulic systems shall use only listed fire-resistant hydraulic fluids. <i>Exception: Where unlisted hydraulic fluids must be used, they shall be protected by a fire suppression system.</i></p>	NC - The AP1000 fire protection design criteria document does not explicitly invoke this requirement. Hydraulic fluids will be in accordance with equipment manufacturer recommendations.
<p>3.3.4.4 The ignition of leaked or spilled liquid shall be minimized by the following methods:</p> <ol style="list-style-type: none"> (1) * Keeping the liquid from contact with hot parts of the steam system (wall temperature greater than or equal to ignition temperature), such as steam pipes and ducts, entry valve, turbine casing, reheater, and bypass valve (2) Using suitable electrical equipment (3) Sealing the insulation of hot plant components to prevent liquid saturation 	<p>N/A - See Below</p> <p>AC - The AP1000 fire protection design criteria document does not explicitly invoke this requirement. The layout has been designed to pass flammable and combustible liquids below hot piping.</p> <p>NC - The AP1000 fire protection design criteria document does not explicitly invoke this requirement.</p> <p>AC - The AP1000 fire protection design criteria document does not explicitly invoke this requirement.</p>

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
(4) Using concentric piping (5) Using liquid collection systems	AC - The AP1000 fire protection design criteria document does not explicitly invoke this requirement. Piping for distribution of fuel oils is concentric. Comply
3.4 Control of Ignition Sources. Plant administrative procedures shall require an in-plant review and prior approval of all work plans to assess potential fire hazard situations. Where such conditions are determined to exist, special precautions shall be taken to define appropriate conditions under which the work is authorized.	O/O
3.4.1 Hot Work.	N/A - Heading
3.4.1.1 The owner or his or her designated manager shall develop, implement, and update as necessary a welding and cutting safety procedure using NFPA 51B, <i>Standard for Fire Prevention During Welding, Cutting, and Other Hot Work</i> , and NFPA 241, <i>Standard for Safeguarding Construction, Alteration, and Demolition Operations</i> , as a guide.	O/O
3.4.1.2 Written permission from the fire protection manager or a designated alternate shall be obtained before starting activities involving cutting, welding, grinding, or other potential ignition sources.	O/O
3.4.1.3* A permit shall not be issued until all of the following are accomplished: (1) An inspection has determined that hot work can be safely conducted at the desired location. (2) Combustibles have been moved away or safely covered. (3) The atmosphere is nonflammable. (4) A trained fire watch (with equipment) is posted for the duration of the work, and for 30 minutes thereafter, to protect against sparks or hot metal starting fires.	N/A – See Below O/O O/O O/O O/O
3.4.1.4 All cracks or openings in floors shall be safely covered or closed.	O/O
3.4.2 Smoking.	N/A - Heading
3.4.2.1 Smoking shall be prohibited at or in the vicinity of hazardous operations or combustible and flammable materials. “No Smoking” signs shall be posted in these areas.	O/O
3.4.2.2 Smoking shall be permitted only in designated and supervised safe areas of the plant. Where smoking is permitted, safe receptacles shall be provided for smoking materials.	O/O

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
3.4.3 Temporary Electrical Wiring. The ignition of flammable materials shall be minimized by requiring that all temporary electrical wiring (1) Be kept to a minimum (2) Be suitable for the location (3) Be installed and maintained in accordance with NFPA 70, <i>National Electrical Code</i> ® , or ANSI C2, <i>National Electrical Safety Code</i> , as appropriate (4) Be arranged so that energy shall be isolated by a single switch (5) Be arranged so that energy shall be isolated when not needed	O/O
3.4.4 Temporary Heating Appliances.	N/A - Heading
3.4.4.1 Only safely installed, approved heating devices shall be used in all locations. Ample clearance shall be provided around stoves, heaters, and all chimney and vent connectors to prevent ignition of adjacent combustible materials in accordance with NFPA 211, <i>Standard for Chimneys, Fireplaces, Vents, and Solid Fuel-Burning Appliances</i> (connectors and solid fuel); NFPA 54, <i>National Fuel Gas Code</i> (fuel gas appliances); and NFPA 31, <i>Standard for the Installation of Oil-Burning Equipment</i> (liquid fuel appliances).	O/O
3.4.4.2 Refueling operations of heating equipment shall be conducted in an approved manner.	O/O
3.4.4.3 Heating devices shall be situated so that they are not likely to overturn.	O/O
3.4.4.4 Temporary heating equipment, when utilized, shall be monitored and maintained by properly trained personnel.	O/O
3.4.5 Open-flame or combustion-generated smoke shall not be used for leak testing.	O/O
3.4.6 Plant administrative procedures shall specify appropriate requirements governing the control of electrical appliances in all plant areas.	COL
3.5 Temporary Structures.	N/A - Heading
3.5.1 Exterior Buildings.	N/A - Heading
3.5.1.1* Temporary buildings, trailers, and sheds, whether individual or grouped, shall be constructed of noncombustible material and shall be separated from other structures.	O/O
3.5.1.2 Temporary buildings, trailers, and sheds and other structures constructed of combustible or limited-combustible material shall be separated from other structures by a minimum distance of 30 ft (9.1 m). <i>Exception: Where all portions of the exposed building (walls, roof) within 30 ft (9.1 m) of the exposure constitute a rated fire barrier, the minimum separation distance shall be permitted to be reduced in accordance with Table 3.5.1.2.</i>	O/O

NFPA 804 PARAGRAPH					AP1000 COMPLIANCE STATEMENT
Table 3.5.1.2 Minimum Separation Distances					O/O
Exposed Building Fire Barrier Rating	Minimum Distance Where Exposing building is Without Protection		Minimum distance Where Exposing Building has Automatic Sprinklers		
	Ft	m	Ft	m	
3 hr	5	1.5	0	0	
2 hr	10	3.0	5	1.5	
1 hr	20	3.1	10	3.0	
1 hr	30	9.1	15	4.6	
3.5.1.3 All exterior buildings, trailers, sheds, and other structures shall have the appropriate type and size of portable fire extinguishers.					
3.5.2 Exterior Temporary Coverings. Where coverings are utilized for protection of the outdoor storage of materials or equipment, the following shall apply: (1) Only approved fire-retardant tarpaulins or other acceptable materials shall be used. (2) All framing material used to support such coverings shall be either noncombustible or fire-retardant pressure-impregnated wood. (3) Covered storage shall not be located within 30 ft (9.1 m) of any building.					O/O
3.5.3 Interior Temporary Facilities.					N/A - Heading
3.5.3.1 All interior temporary structures shall be constructed of noncombustible, limited-combustible, or fire-retardant pressure-impregnated wood. Structures constructed of noncombustible or limited-combustible materials shall be protected by an automatic fire suppression system unless the fire hazard analysis determines that automatic suppression is not required. The structure shall be protected by an automatic fire suppression system if the structure is constructed of fire-retardant pressure-impregnated wood.					O/O
3.5.3.2 This use of interior temporary coverings shall be limited to special conditions where interior temporary coverings are necessary. They shall be constructed of approved fire-retardant tarpaulins.					O/O
3.5.3.3 Where framing is required, it shall be constructed of noncombustible, limited-combustible, or fire-retardant pressure-impregnated wood.					O/O
3.5.3.4 All interior temporary facilities shall have the appropriate type and size of portable fire extinguisher.					O/O

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
3.6 Impairments.	N/A - Heading
3.6.1* A written procedure shall be established to address impairments to fire protection systems and features and other plant systems that directly impact the level of fire risk (e.g., ventilation systems, plant emergency communication systems, etc.).	COL
3.6.2* Impairments to fire protection systems shall be as short in duration as practical.	O/O
3.6.3* Appropriate post-maintenance testing shall be performed on equipment that was impaired to ensure that the system will function properly. Any change to the design or function of the system after the impairment shall be considered in establishing the testing requirements and shall be reflected in the appropriate design documents and plant procedures.	O/O
3.7 Testing and Maintenance.	N/A - Heading
3.7.1 Upon installation, all new fire protection systems and passive fire protection features shall be preoperationally inspected and tested in accordance with applicable NFPA standards. Where appropriate test standards do not exist, inspections and test procedures described in the purchase and design specification shall be followed.	O/O
3.7.2* Fire protection systems and passive fire protection features shall be inspected, tested, and maintained in accordance with applicable NFPA standards, manufacturers' recommendations, and requirements established by those responsible for fire protection at the plant.	O/O
3.7.3 Inspection, testing, and maintenance shall be performed using established procedures with written documentation of results and a program of follow-up actions on discrepancies.	O/O
3.7.4* Consideration shall be given to the inspection, testing, and maintenance of nonfire protection systems and equipment that have a direct impact on the level of fire risk within the plant.	O/O
Chapter 4 Manual Fire Fighting	N/A - Heading
4.1 Prefire Plans.	N/A - Heading
4.1.1 Detailed prefire plans shall be developed for all site areas.	COL
4.1.2* The plans shall detail the fire area configurations and fire hazards to be encountered in the fire area along with any safety-related components and fire protection systems and features that are present.	COL
4.1.3 Prefire plans shall be reviewed and, if necessary, updated at least every two years.	COL

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
4.1.4* Prefire plans shall be available in the control room and made available to the plant fire brigade.	O/O
4.2* On-Site Fire-Fighting Capability.	N/A - Heading
4.2.1 General.	N/A - Heading
4.2.1.1 A minimum of five plant fire brigade members shall be available for response at all times.	O/O
4.2.1.2 Fire brigade members shall have no other assigned normal plant duties that would prevent immediate response to a fire or other emergency as required.	O/O
4.2.1.3 The brigade leader and at least two brigade members shall have sufficient training and knowledge of plant safety-related systems to understand the effects of fire and fire suppressants on safe shutdown capability.	O/O
4.2.1.4 The fire brigade shall be notified immediately upon verification of a fire or fire suppression system actuation.	O/O
4.2.2 Fire Fighter Qualifications and Requirements.	N/A - Heading
4.2.2.1 Plant fire brigade members shall be physically qualified to perform the duties assigned.	O/O
4.2.2.2 Each member shall pass an annual physical examination to determine that the fire brigade member can perform strenuous activity.	O/O
4.2.2.3 The physical examination shall determine each member's ability to use respiratory protection equipment.	O/O
4.2.3 Each fire brigade member shall meet training qualifications as specified in Section 4.3	O/O
4.3 Training and Drills.	N/A - Heading
4.3.1 Plant Fire Brigade Training.	N/A - Heading
4.3.1.1 Plant fire brigade members shall receive training consistent with the requirements contained in NFPA 600, <i>Standard on Industrial Fire Brigades</i> , or NFPA 1500, <i>Standard on Fire Department Occupational Safety and Health Program</i> , as appropriate.	O/O
4.3.1.2* Fire brigade members shall be given quarterly training and practice in fire fighting.	O/O
4.3.1.3 A written program shall detail the fire brigade training program.	O/O

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
4.3.1.4 Written records that include, but are not limited to, initial fire brigade classroom and hands-on training, refresher training, special training schools attended, drill attendance records, and leadership training for fire brigades shall be maintained for each fire brigade member.	O/O
4.3.2 Drills.	N/A - Heading
4.3.2.1 Drills shall be conducted quarterly for each shift to test the response capability of the fire brigade.	O/O
4.3.2.2 Fire brigade drills shall be developed to test and challenge fire brigade response including brigade performance as a team, proper use of equipment, effective use of prefire plans, and coordination with other groups.	O/O
4.3.2.3 Fire brigade drills shall be conducted in various plant areas, especially in those areas identified by the fire hazards analysis to be critical to plant operation and to contain significant fire hazards.	O/O
4.3.2.4 Drill records shall be maintained detailing the drill scenario, fire brigade member response, and ability of the fire brigade to perform the assigned duties.	O/O
4.3.2.5 A critique shall be held after each drill	O/O
4.4 Fire-Fighting Equipment.	N/A - Heading
4.4.1* The plant fire brigade shall be provided with equipment that will enable them to adequately perform their assigned tasks.	O/O
4.4.2 Fire brigade equipment shall be tested and maintained. Written records shall be retained for review.	O/O
4.5 Off-Site Fire Department Interface.	N/A - Heading
4.5.1 Mutual Aid Agreement.	N/A - Heading
4.5.1.1 A mutual aid agreement shall be offered to the local off-site fire department.	COL
4.5.1.2 Where possible, the plant fire protection manager and the off-site fire authorities shall develop a plan for their interface. The fire protection manager also shall consult with the off-site fire department to make plans for fire fighting and rescue, including assistance from other organizations, and to maintain these plans.	O/O
4.5.1.3 The local off-site fire department shall be invited to participate in an annual drill.	O/O
4.5.2 Site-Specific Training.	N/A - Heading
4.5.2.1 Fire fighters from the off-site fire department who are expected to respond to a fire at the plant shall be familiar with the plant layout.	O/O
4.5.2.2 The access routes to fires in the controlled area (to which access doors are locked) shall be planned in advance.	COL

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
4.5.2.3* The off-site fire department shall be offered instruction and training in radioactive materials, radiation, and hazardous materials that might be present.	O/O
4.5.3 Security and Health Physics.	N/A - Heading
4.5.3.1* Plant management shall designate a plant position to act as a liaison to the off-site fire department when they respond to a fire or other emergency at the plant.	O/O
4.5.3.2 Plant management shall ensure that the off-site fire department personnel are escorted at all times and emergency actions are not delayed.	O/O
4.6 Water Drainage. The fire brigade shall have at their disposal the necessary equipment to assist with routing water from the affected area.	O/O
4.7 Fire-Fighting Access.	N/A - Heading
4.7.1 All plant areas shall be accessible for fire-fighting purposes.	Comply
4.7.2 Prefire plans shall identify those areas of the plant that are locked and have limited access for either security or radiological control reasons. Provisions shall be made to allow access to these areas. If necessary, this shall include having security and health physics personnel respond to the fire area along with the fire brigade. Health physics personnel shall confer with the fire brigade leader to determine the safest method of access to any radiologically controlled area.	COL
4.8 Radiation Shielding.	N/A - Heading
4.8.1 Full advantage shall be taken of all fixed radiation shielding to protect personnel responding for fire suppression purposes.	O/O
4.8.2 Health physics personnel shall advise the fire brigade leader of the best method for affording radiological protection.	O/O
4.9* Smoke and Heat Removal. If fixed ventilation systems are not capable of removing smoke and heat, the fire brigade shall utilize portable ventilation equipment. (See Section 6.4.)	O/O
Chapter 5 Nuclear Reactor Safety Considerations	N/A - Heading
5.1* General.	N/A - Heading
<p>5.2 Fire Hazards and Safe Shutdown Analysis (FSSA). A fire safe shutdown analysis (FSSA) shall be prepared and maintained for the operating life of the reactor. The FSSA shall include as a minimum all of the following:</p> <p>(1) Fire hazards analysis (FHA)</p> <p>(2) Safe shutdown analysis (SSA)</p> <p>(3) Internal plant examination of external fire events for severe accident vulnerabilities</p>	<p>Comply, COL</p> <p>Comply</p> <p>Comply</p> <p>Comply, COL</p>

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
5.2.1 Fire Hazards Analysis. The fire hazards analysis shall include the criteria indicated in Section 2.4.	Comply
5.2.2 Safe Shutdown Analysis. A safe shutdown analysis of the effects of a fire on those essential structures, systems, and components required to safely shut down the plant and maintain it in a safe shutdown condition shall be performed. The analysis shall include as a minimum the requirements of this section.	AC - The AP1000 fire protection analysis exists, but does not include the shutdown logic diagram per paragraph 5.2.2.2.
5.2.2.1 A safe shutdown system available/unavailable calculation or table shall be prepared and maintained for each fire area. This document shall identify all safe shutdown equipment that is operable or inoperable due to the effects of a fire in that fire area. This document shall demonstrate compliance with the requirements of Sections 5.3 and 5.4.	Comply
5.2.2.2* A shutdown logic diagram shall be available that identifies the conditions necessary to achieve and maintain safe shutdown capability in the event of a fire and those plant features necessary to realize these conditions, including auxiliary and support features.	NC. The AP1000 fire protection analysis does not include a shutdown logic diagram.
5.2.3 Internal Plant Examination of External Fire Events for Severe Accident Vulnerabilities.	N/A - Heading
A risk assessment that estimates the potential risk from a fire in relation to the plant's core damage frequency shall be prepared.	Comply. Westinghouse has a fire PRA for AP1000. It is not, however, referenced by the fire protection analysis.
5.2.3.1* An industry-accepted examination process shall be used for the risk assessment.	Comply. The Westinghouse fire PRA is consistent with the EPRI FIVE process.
5.2.3.2* An acceptable risk assessment shall demonstrate that the probability of core damage as a result of an internal fire is less than 1×10^{-6} per reactor year.	Comply
5.2.3.3 The internal plant examination of external fire events for severe accident vulnerabilities shall be used to evaluate the level of safety of the plant and shall not be used to reduce the overall plant fire protection design basis.	Comply – In some fire areas the fire is assumed to progress through the area and operator action is necessary to assure no spurious ADS actuation.
5.3 Design Basis Events and Requirements.	N/A - Heading
5.3.1 Fire.	N/A - Heading
5.3.1.1 Only one fire is assumed to occur at a given time. For the purpose of a safe shutdown analysis, damage shall be assumed to occur immediately.	Comply
5.3.1.2* All components, including electrical cables, that are susceptible to fire damage in a single fire area (except primary containment and annulus areas) shall be assumed to be disabled or to be spuriously actuated, whichever is the worst case.	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
5.3.1.3* A fire shall not be assumed to impair safe shutdown capability inside primary containment or annulus areas.	Comply
5.3.1.4 The plant shall be assumed to be operating at 100 percent power, with all components in their normal configuration, when a postulated fire occurs. The analysis also shall consider changes in plant configurations during all normal modes of operation.	Comply
5.3.1.5 A concurrent single active component failure independent of the postulated fire shall not be assumed to occur.	Comply
5.3.1.6 Plant accidents or severe natural phenomena shall not be assumed to occur concurrently with a postulated fire. <i>Exception: For seismic/fire interaction, see 5.3.2.</i>	Comply
5.3.1.7 A loss of off-site power shall be assumed concurrent with the postulated fire only where the safe shutdown analysis (including alternative shutdown) indicates the fire could initiate the loss of off-site power.	Comply
<p>5.3.1.8 Fire safe shutdown components shall be capable of performing all of the following functions in the event of the postulated fire:</p> <ul style="list-style-type: none"> (1) Achieving and maintaining subcritical reactivity conditions in the reactor (2) Maintaining the reactor coolant inventory such that plant safety limits are not violated (3) *Establishing reactor decay heat removal to prevent fuel damage and achieve and maintain cold shutdown conditions (4) Providing support functions such as process cooling, lubrication, and so forth, necessary to permit operation of the FSSD components (5) Providing direct readings of the process variables necessary to perform and control the FSSD functions 	<p>N/A - See Below</p> <p>Comply</p> <p>Comply</p> <p>AC - AP1000 is a passive plant designed to establish reactor decay heat removal to prevent fuel damage and achieve and maintain safe shutdown conditions. Additional protection has been afforded to also protect cold shutdown equipment. This safe shutdown end state was accepted by NRC for AP600.</p> <p>Comply</p> <p>Comply</p>
5.3.1.9 Limiting Safety Conditions. During a postfire shut-down, the fission product boundary integrity shall be maintained within acceptable limits (e.g., fuel clad damage, rupture of any primary coolant boundary, or rupture of the primary containment boundary).	Comply - A fire near a containment electrical penetration may affect the leaktightness of the penetration.

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
5.3.1.10 Spurious Signals.	N/A - Heading
<p>5.3.1.10.1 An evaluation of spurious signals shall be performed based on these assumptions:</p> <p>(1) All potential spurious components shall be assumed to be in their normal operating positions for the particular mode of operation being considered by the spurious signal evaluation.</p> <p>(2) The fire-induced cable damage shall determine if any of the following cable failure modes are possible:</p> <p><i>a. Hot Short.</i> Individual conductors within a cable are shorted to individual conductors of a different cable such that a de-energized circuit might become energized by shorting to an external source of electrical power.</p> <p><i>b. Open Circuit.</i> The cable failure results in the loss of electrical continuity.</p> <p><i>c. Shorts to Ground.</i> Cable conductors short to grounded structures.</p> <p><i>d. Short Circuit.</i> Individual conductors within multi-conductor cable short to each other.</p>	<p>Comply</p> <p>Comply</p> <p>AC – The AP1000 fire hazards analysis assumes spurious actuations regardless of cable failure mode except for valve motor operators. The spurious actuations are postulated one at a time (except for high/low pressure interfaces). Spurious actuation of the redundant valves in any one high-low pressure interface line are postulated if the circuits for those valves are located in the fire area. The spurious actuations that are evaluated are those that could cause a breach in the reactor coolant boundary or defeat safety-related decay heat removal capability or cause an increase in shutdown reactivity of the reactor.</p> <p>AC</p> <p>AC</p> <p>AC</p> <p>AC</p>
5.3.1.10.2 Functional failure or damage modes of equipment and components that can spuriously operate shall be considered.	Comply
5.3.1.11 Fire-Induced Spurious Actuation. The following postulates shall be used when analyzing fire-induced spurious actuation of equipment.	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
5.3.1.11.1 FSSD capability shall not be adversely affected by simultaneous spurious actuation of all valves in a single high-to-low pressure interface line where the power or control circuits for the valves can be damaged by a postulated fire.	Comply
5.3.1.11.2 For other than high-to-low pressure boundaries, FSSD capability shall not be adversely affected by spurious actuation or signal.	Comply
5.3.1.11.3 Separate conditions shall be analyzed concurrent with the spurious actuation(s) or signal addressed in 5.3.1.10.1 and 5.3.1.10.2.	Comply
5.3.1.11.4 All automatic functions (signal, logic, etc.) from the circuits that can be damaged by the postulated fire shall be assumed lost or assumed to function as intended, whichever is the worst case.	Comply
5.3.1.11.5 All potential spurious signals shall be analyzed. However, only one spurious signal shall be postulated to occur at a time for purposes of analysis, except for high-low pressure interface valves.	AC – See 5.3.1.10.1 (2)
5.3.1.12* For the purpose of analysis for cases involving high-to-low pressure interface, hot shorts involving three-phase ac circuits shall be postulated.	Comply – See AP1000 DCD 9A.3.7.1.1
5.3.1.13 For ungrounded dc circuits, if it can be shown that only two hot shorts of the proper polarity without grounding could cause spurious operation, no further evaluation shall be necessary except for cases involving high-to-low pressure interfaces.	AC - See 5.3.1.10.1 (2)
5.3.1.14* All associated circuits of concern shall be isolated from FSSD circuits by coordinated circuit breakers or fuses.	Comply
5.3.1.15* Circuits Associated by Common Enclosure.	N/A - Heading
5.3.1.15.1 Protection for circuits associated by common enclosure shall be demonstrated by ensuring that suitable electrical overcurrent protection devices are provided for all cables. Appropriate measures to prevent the propagation of fire, such as rated fire stops and seals in the raceway or enclosure, shall be provided.	Comply
5.3.1.15.2 The overcurrent protection devices shall be located outside of the fire area containing the common enclosure.	Comply
5.3.1.16 High Impedance Faults.	N/A - Heading
5.3.1.16.1 A high impedance fault shall be assumed to occur as a result of a fire.	Comply
5.3.1.16.2 Evaluation of the impact of high impedance faults on the ability to achieve and maintain safe shutdown shall be performed. This evaluation shall demonstrate that there is sufficient capacity in the electrical protective system to preclude a trip of the main source breaker to the supply.	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
5.3.2* Seismic/Fire Interaction.	N/A - Heading
5.3.2.1 A risk assessment that demonstrates the potential risk from a seismically induced fire in relationship to the plant's core damage frequency shall be prepared.	NC. AP1000 has not prepared seismically induced fire PRA.
5.3.2.2* An industry-accepted examination process shall be used for the risk assessment.	N/A. AP1000 does not have a seismically induced fire PRA.
5.3.2.3 The assessment shall be used to evaluate the level of safety of the plant. This assessment shall not be used to reduce the overall plant fire protection design basis.	N/A. AP1000 does not have a seismically induced fire PRA.
5.4 Separation Criteria.	N/A - Heading
5.4.1 One safety division of systems that is necessary to achieve and maintain safe shutdown from either the control room or emergency control station(s) shall be maintained free of fire damage by a single fire, including an exposure fire.	Comply
5.4.2 One safety division of systems that is necessary to prevent the initiation of a design basis accident shall be maintained free of fire damage from a single fire that occurs outside the main control room.	Comply - At least one safety division remains available following any single fire anywhere outside the control room or the containment.
<p>5.4.3 Redundant cables, equipment, components, and associated circuits of nuclear-safety-related or safe shutdown systems shall be located in separate fire areas. The fire barrier forming these fire areas shall have a 3-hour fire rating and automatic area-wide detection shall be installed throughout these fire areas. Structural steel forming a part of or supporting such fire barriers shall be protected to provide fire resistance equivalent to that of the barrier.</p> <p><i>Exception No. 1: Where redundant system separation inside containment cannot be achieved, other measures shall be permitted in accordance with Section 5.6 to prevent a fire from causing the loss of function of nuclear-safety-related or safe shutdown systems.</i></p> <p><i>Exception No. 2: Redundant cables, equipment, components, and associated circuits of nuclear-safety-related or safe shutdown systems shall be located in separate fire areas. The fire barriers forming these fire areas shall have a minimum fire-resistive rating of 1 hour, and automatic area-wide detection and suppression shall be installed throughout these fire areas. Structural steel forming a part of or supporting such fire barriers shall be protected to provide fire resistance equivalent to that of the barrier.</i></p>	Comply – See AP1000 DCD 9A.2.7.1.
5.4.4 Fire areas separated by minimum 3-hour fire barriers shall be established to separate redundant safety divisions and safe shutdown functions from fire hazards in nonsafety or safe shutdown related areas of the plant.	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
<p>5.4.5 Within fire areas containing components of either a nuclear-safety-related or safe shutdown system, special attention shall be given to detecting and suppressing fire that can adversely affect the system. Measures that shall be taken to reduce the effects of a postulated fire in a given fire area include limiting the amount of combustible materials (<i>see Section 3.3</i>), providing fire-rated barriers between major components and equipment to limit fire spread within a fire area (<i>see Section 6.1</i>), or installing fire detection (<i>see Section 7.8</i>) and fixed suppression systems (<i>see Section 7.6</i>).</p>	Comply
<p>5.5 Manual Actions.</p>	N/A - Heading
<p>5.5.1 Shutdown Procedures. Procedures shall be developed for actions necessary to achieve FSSD.</p>	COL
<p>5.5.2 Operator Actions.</p>	N/A - Heading
<p>5.5.2.1 Operator actions necessary to achieve FSSD of the reactor shall be kept to a minimum.</p>	Comply
<p>5.5.2.2* No credit shall be taken for operator actions required to effect repairs to equipment in order to achieve FSSD of the reactor.</p>	Comply
<p>5.5.2.3 Personnel necessary to achieve and maintain the plant in FSSD following a fire shall be provided from the normal on-site staff, exclusive of the fire brigade.</p>	O/O
<p>5.5.2.4 The operator training program shall include performance-based simulator training on FSSD procedures.</p>	O/O
<p>5.5.2.5 Walk-through of operator actions necessary to achieve FSSD of the reactor shall be performed to verify that the actions are feasible and shall be integrated into the operator training program.</p>	O/O
<p>5.5.2.6 Postfire shutdown and recovery plans shall be included in the station emergency preparedness plan. Drills and operator requalification training shall ensure that operations personnel are familiar with and can accomplish the necessary actions.</p>	O/O
<p>5.5.3 Operator Access and Equipment Operation.</p>	N/A - Heading
<p>5.5.3.1 Operator Access.</p>	N/A - Heading
<p>5.5.3.1.1* Access routes to areas containing equipment necessary for safe shutdown of the reactor shall be protected from the effects of smoke and fire.</p>	Comply
<p>5.5.3.1.2 Two separate access routes shall be provided from the main control room to the remote shutdown location.</p>	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
5.5.3.1.3 Emergency lighting shall be provided for the access routes and the remote shutdown location (<i>see Section 6.6</i>).	Comply
5.5.3.2 Equipment Operation.	N/A - Heading
5.5.3.2.1* Operator safety shall not be threatened by fire conditions while implementing FSSD of the reactor.	Comply
5.5.3.2.2* Operation of equipment required to effect FSSD of the reactor shall not require any extraordinary actions by the operator.	Comply
5.5.3.2.3 Operators (e.g., handwheels of valves that require manual manipulation for FSSD) shall be readily accessible. If the handwheel is located more than 5 ft (1.5 m) above the floor, it shall be provided with either a chain operator or a permanent platform. The platform shall be of sufficient size to allow the operator to safely perform the manual action.	Comply.
5.6 Alternative Shutdown Capability.	N/A - Heading
5.6.1 Alternative shutdown capability provided for a specific fire area shall include achieving and maintaining subcritical reactivity conditions in the reactor, maintaining the reactor coolant inventory, achieving safe shutdown, and maintaining safe shutdown following the fire event.	AC – See AP1000 DCD Table 9.5.1-1 items 25 and 76, and section 9A.2.7.
5.6.2 During the postfire shutdown, the reactor coolant system process variables shall be maintained within those predicted for a loss of normal ac power, and the fission product boundary integrity shall not be affected.	Comply
5.6.3 Performance goals for reactor shutdown functions shall be the same as those required by 5.3.1.8.	Comply
5.6.4 The safe shutdown circuits for each fire area shall be known to be isolated from associated circuits in the fire area so the hot shorts, shorts to ground, open circuits, or short circuits will not prevent the operation of the safe shutdown equipment. Isolation of associated circuits from the safe shut-down equipment shall be such that a postulated fire involving the associated circuits will not prevent safe shutdown or damage the safe shutdown components.	Comply
Chapter 6 General Plant Design	N/A - Heading
6.1 Plant Arrangement.	N/A - Heading
6.1.1 Building Separation.	N/A - Heading
6.1.1.1 In multi-unit plants, each unit shall be separated from adjacent units by either an open space of at least 50 ft (15.2 m), or at least a 3-hour-rated fire barrier.	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
<p>6.1.1.2 Buildings or portions thereof containing nuclear-safety-related systems shall be separated from buildings or portions thereof not related to nuclear safety by barriers having a designated fire resistance rating of 3 hours.</p> <p><i>Exception: Buildings containing nuclear-safety-related systems shall be permitted to be separated from buildings not related to nuclear safety by an open space of at least 50 ft (15.2 m).</i></p>	Comply
<p>6.1.2 Fire Areas. Advanced light water reactor (ALWR) electric generating plants shall be subdivided into separate fire areas to minimize the risk of fire spread and the resultant consequential damage from fire gases, smoke, heat, radioactive contamination, and fire-fighting activities. In addition, the subdivision into fire areas shall allow adequate access for manual fire suppression activities.</p>	Comply
<p>6.1.2.1 A listed fire barrier having a fire resistance rating of at least 3 hours, and with listed 3-hour-rated penetration seals, shall be provided as follows:</p> <ol style="list-style-type: none"> (1) To separate all contiguous buildings or portions thereof serving different purposes, such as reactor containment, auxiliary, turbine, radwaste, control, service, administration, and other occupancy areas as dictated by reactor design (2) To separate safety-related standby emergency diesel generators and combustion turbines from each other and the rest of the plant (3) To separate the turbine generator lube oil conditioning system and lube oil storage from the turbine building and adjacent areas (4) To separate diesel fire pumps and associated equipment from other pumps in the same pump house (5) To separate all areas with heavy concentrations of cables, such as cable spreading rooms, cable tunnels, cable penetration areas, and cable shafts or chases, including those within the reactor containment, from adjacent areas (6) To separate auxiliary boiler rooms from adjacent areas (7) Wherever so determined by the fire hazards analysis 	<p>N/A - See Below</p> <p>Comply</p> <p>N/A. There are no safety-related standby emergency diesel generators and/or combustion turbines in AP1000.</p> <p>Comply</p> <p>Comply. No other pumps are in the diesel fire pump house.</p> <p>Comply</p> <p>Comply</p> <p>Comply</p>

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
<p>6.1.2.2 To prevent vertical spread of fire, stairways, elevator shafts, trash chutes, and other vertical shafts and plenums shall be enclosed with barriers having a fire resistance rating of at least 2 hours. Openings in such barriers shall be protected with listed automatic or self-closing fire doors having a fire protection rating of at least 1-1/2 hours.</p>	<p>NC. Auxiliary building stairwells and elevator shafts, with exception of the exterior wall sections enclosing Stairwell S03 and the wall separating Stairwell S03 from the elevator shaft above the Auxiliary Building Roof, are enclosed in towers constructed using both concrete structural walls and nonstructural walls as described in Section 9A of the DCD.</p> <p>For buildings outside of the Nuclear Island, exterior wall sections enclosing stairwells and elevator shafts do not have a fire resistance rating of 2 hours, only interior stairwell and elevator shaft wall sections are rated for the minimum 2 hour fire resistance rating.</p>
<p>6.1.3 Openings in Fire Barriers.</p>	<p>N/A - Heading</p>
<p>6.1.3.1 All openings in fire barriers shall be provided with fire door assemblies, fire dampers, penetration seals (fire stops), or other approved means having a fire protection rating consistent with the designated fire resistance rating of the barrier.</p> <p><i>Exception: The use of assemblies that are not listed or approved due to nuclear safety or security requirements shall be demonstrated to be equivalent.</i></p>	<p>Comply</p>
<p>6.1.3.2 Fire door assemblies, fire dampers, and fire shutters used in 2-hour-rated fire barriers shall be listed as not less than 1-1/2 hour rated and shall meet the requirements of NFPA 80, <i>Standard for Fire Doors and Fire Windows</i>, for fire door requirements and NFPA 90A, <i>Standard for the Installation of Air-Conditioning and Ventilating Systems</i>, for fire damper requirements.</p> <p><i>Exception: Where approved full-scale fire tests indicate that opening protection is not necessary, opening protection shall not be required.</i></p>	<p>Comply</p>
<p>6.1.3.2.1 Windows in fire barriers, such as for a control room or computer room, shall be provided with a listed or approved fire shutter or automatic wall curtain.</p>	<p>Comply</p>

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
<p>6.1.3.2.2 Cable openings, piping openings, and building joints shall be provided with fire-rated penetration seals. The sealing material shall be of limited-combustible or noncombustible material and shall meet the requirements of ASTM E 814, <i>Fire Tests of Through-Penetration Fire Stops</i>, or UL 1479, <i>Standard for Safety Fire Tests of Through-Penetration Firestops</i>.</p>	<p>AC. For temperature criteria for the unexposed side of the fire barrier, RG 1.189 Rev. 1, Section 4.2.1.5b.ii is used: "The temperature levels recorded for the unexposed side of the fire barrier are analyzed and demonstrate that the maximum temperature does not exceed 163 °C (325 °F) or 121 °C (250 °F) above the ambient temperature. Higher temperatures at through-penetrations may be permitted when justified in terms of cable insulation ignitability."</p>
<p>6.1.3.2.3 Internal Conduit Seals. All conduits shall be sealed at the barrier with a fire-rated seal, if accessible. Alternatively, internally sealing with a fire-rated seal at the first break in the conduit on both sides of the barrier shall be acceptable. For the above configuration, the fire rating of the internal conduit seal shall be equivalent to the rating of the fire barrier being penetrated.</p> <p><i>Exception: Where approved full-scale fire tests indicate that internal conduit seals are not necessary, internal conduit seals are not required.</i></p>	<p>Comply</p>
<p>6.1.3.2.4 All fire-rated assemblies shall be tested with a positive pressure in the furnace.</p>	<p>Comply</p>
<p>6.1.3.2.5 Normally closed fire doors in fire barriers shall be identified with a sign indicating "Fire Door - Keep Closed."</p>	<p>Comply, O/O</p>
<p>6.1.3.3 Design features that provide for monitoring and control of fire doors to assure fire door operability and fire barrier integrity shall be provided. <i>Exception: Administrative procedures instead of design features shall be permitted.</i></p>	<p>Comply</p>
<p>6.2 Life Safety.</p>	<p>N/A - Heading</p>
<p>6.2.1* NFPA 101®, <i>Life Safety Code</i>®, shall be the standard for life safety from fire in the design and operation of the ALWR, except where modified by this standard.</p>	<p>NC. Deviations from the Life Safety Code's exit and egress requirements are identified and the degree of the life safety justified in the Means of Egress Studies.</p>
<p>6.2.2* The majority of the areas involved in the transfer of nuclear energy to electrical energy shall be considered as special-purpose industrial occupancies and special structure, windowless buildings, as defined in NFPA 101, <i>Life Safety Code</i>.</p>	<p>Comply</p>

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
6.2.3 In determining the exits for an ALWR plant, the actual number of personnel and occupancy hazards during maintenance, refueling, and testing shall determine the exit requirements and occupant load based upon NFPA 101, <i>Life Safety Code</i> .	Comply
6.2.4 Cafeterias, lunchrooms, conference rooms, and assembly rooms having an occupant load greater than 50 shall conform to the new assembly occupancy requirements in NFPA 101, <i>Life Safety Code</i> .	Not part of the standard AP1000 certified design.
6.2.5 General office areas, office buildings, and training facilities shall conform to the business occupancy requirements in NFPA 101, <i>Life Safety Code</i> .	Not part of the standard AP1000 certified design.
6.2.6 Warehouses and storage areas shall conform to the storage occupancy requirements in NFPA 101, <i>Life Safety Code</i> .	Not part of the standard AP1000 certified design.
6.3 Building and Construction Materials.	N/A - Heading
<p>6.3.1 Construction materials for the ALWR plant shall be classified by at least one of the following test methods appropriate to the end-use configuration of the material:</p> <p>(1) NFPA 220, Standard on Types of Building Construction</p> <p>(2) ASTM E 136, Standard Test Method for Behavior of Materials in a Vertical Tube Furnace at 750°C</p> <p>(3) NFPA 251, Standard Methods of Tests of Fire Endurance of Building Construction and Materials (ASTM E 119, Standard Test Methods for Fire Tests of Building Construction and Materials)</p> <p>(4) NFPA 253, Standard Method of Test for Critical Radiant Flux of Floor Covering Systems Using a Radiant Heat Energy Source</p> <p>(5) NFPA 255, Standard Method of Test of Surface Burning Characteristics of Building Materials (ASTM E 84, Standard Test Method for Surface Burning Characteristics of Building Materials)</p> <p>(6) NFPA 256, Standard Methods of Fire Tests of Roof Coverings</p> <p>(7) NFPA 259, Standard Test Method for Potential Heat of Building Materials</p>	<p>Comply</p> <p>Comply</p> <p>Comply</p> <p>Comply</p> <p>Comply</p> <p>Comply</p> <p>Comply</p>
6.3.2* All walls, floors, and structural components, except interior finish materials, shall be of noncombustible construction.	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
6.3.2.1 Interior wall or ceiling finish classification shall be in accordance with NFPA 101, <i>Life Safety Code</i> , requirements for Class A material.	NC - Protective Coatings used as interior wall and ceiling finishes meet the criteria of noncombustible from the BTP CMEB 9.5-1 Regulatory Position C.5.(a).9.
6.3.2.2 Interior floor finish classification shall be in accordance with NFPA 101, <i>Life Safety Code</i> , requirements for Class I interior floor finish.	NC - Protective Coatings used as interior wall and ceiling finishes meet the criteria of noncombustible from the BTP CMEB 9.5-1 Regulatory Position C.5.(a).9.
6.3.3 Thermal insulation materials, radiation shielding materials, ventilation duct materials, soundproofing materials, and suspended ceilings, including light diffusers and their supports, shall be noncombustible or limited combustible.	Comply
6.3.4 Electrical wiring above suspended ceilings shall be kept to a minimum. Electrical wiring shall be listed for plenum use, or armor-metal-jacketed, or routed in metallic conduits, or trays having both solid metallic bottoms and covers.	Comply
6.3.5 Roof coverings shall be Class A as determined by tests described in NFPA 256, <i>Standard Methods of Fire Tests of Roof Coverings</i> .	Comply
6.3.6 Metal roof deck construction shall be Class I as listed by Factory Mutual or fire acceptable as listed by Underwriters Laboratories Inc.	Comply
6.3.7 Bulk flammable gas storage, either compressed or cryogenic, shall not be permitted inside structures housing safety-related systems.	Comply
6.3.7.1 Storage of flammable gas, such as hydrogen, shall be located outdoors or in separate detached buildings, so that a fire or explosion will not adversely affect any safety-related systems or equipment.	Comply
6.3.7.2* Outdoor high pressure flammable gas storage containers shall be located so that the long axis is not pointing at the building walls.	Comply
6.3.8 Bulk storage of flammable and combustible liquids shall not be permitted inside structures housing safety-related systems. As a minimum, the storage and use shall comply with the requirements of NFPA 30, <i>Flammable and Combustible Liquids Code</i> .	Comply
6.4* Ventilation.	N/A - Heading

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
<p>6.4.1* The design, installation, and operation of ventilation systems necessary for normal and emergency operation of the plant shall be in accordance with NFPA 90A, <i>Standard for the Installation of Air-Conditioning and Ventilating Systems</i>.</p>	<p>AC - The AP1000 fire protection design criteria document does not explicitly invoke this requirement. It does, however, meet the intent of this requirement.</p>
<p>6.4.2* Automatic damper closure or shutdown of ventilation systems shall be consistent with nuclear safety and safety of on-site personnel.</p>	<p>Comply</p>
<p>6.4.3 Smoke removal shall be provided for nuclear-safety-related areas of the plant. Equipment shall be suitable for removing smoke without damage to equipment. The release to the environment of smoke containing radioactive materials shall be monitored in accordance with emergency plans.</p> <p><i>Exception: For those plants provided with complete automatic sprinkler protection, fixed ventilation systems for the removal of smoke is not required.</i></p>	<p>Comply</p>
<p>6.4.3.1 Smoke and heat removal systems shall be provided for other fire areas based upon the fire hazards analysis.</p> <p><i>Exception: For those plants provided with complete automatic sprinkler protection, fixed ventilation systems for the removal of smoke is not required.</i></p>	<p>Comply</p>
<p>6.4.3.2 Smoke from nonnuclear areas shall be discharged directly outside to an area that will not adversely affect nuclear-safety-related areas.</p>	<p>Comply</p>
<p>6.4.3.3* Any ventilation system designed to exhaust potentially radioactive smoke or heat shall be evaluated to ensure that inadvertent operation or single failures will not violate the radiologically controlled areas of the plant.</p>	<p>Comply</p>
<p>6.4.4 To facilitate manual fire fighting, smoke control shall be provided in high-density cable-use areas, switchgear rooms, diesel fuel oil storage areas, turbine buildings, and other areas where potential exists for heavy smoke and heat conditions as determined by the fire hazards analysis.</p>	<p>Comply</p>
<p>6.4.5 The power supply and controls for mechanical ventilation systems used for smoke removal shall be routed outside the fire area served by the system or protected from fire damage.</p>	<p>AC - Some equipment is located in the area that it serves. Some fires may disable the system, requiring the use of portable smoke removal equipment.</p>
<p>6.4.6 The fresh air supply intakes to plant areas shall be located remote from the exhaust air outlets and smoke vents of other fire areas to minimize the possibility of contaminating the air intake with the products of combustion.</p>	<p>Comply</p>

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
6.4.7 Enclosed stairwells shall be designed to minimize smoke infiltration during a fire.	AC - See AP1000 DCD Table 9.5.1-1 item 55.
6.4.8 Where natural-convection ventilation is used, a minimum ratio of vent area to floor area shall be at least 1 to 200, except in oil hazard areas, where at least a 1-to-100 ratio shall be provided.	N/A
6.4.9 Duct Systems.	N/A - Heading
6.4.9.1 Combustible ducts, including fire-retardant types, shall not be used for ventilation systems.	Comply
6.4.9.2 Interconnections of individual fire areas via the ventilation system shall be kept to a minimum.	Comply
<p>6.4.9.3 Fire dampers shall be installed in accordance with NFPA 90A, <i>Standard for the Installation of Air-Conditioning and Ventilating Systems</i>. Consideration shall be given to the velocity in the duct.</p> <p><i>Exception No. 1: Where full-scale fire tests that are conducted by testing laboratories indicate that fire dampers are not necessary to prevent fire spread through a fire-rated barrier, fire dampers can be omitted from the fire barrier.</i></p> <p><i>Exception No. 2: * As an alternative to fire dampers, the duct system can be enclosed or constructed to provide the required fire barrier through adjacent areas. (Refer to Figure A.6.4.9.3 Exception No. 2.)</i></p>	Comply
6.4.9.4 Listed fire dampers having a rating of 1-1/2 hours shall be installed where ventilation ducts penetrate fire barriers having a required fire resistance rating of 2 hours. Where ventilation ducts penetrate required 3-hour fire barriers, approved fire dampers having a fire protection rating of 3 hours shall be installed.	AC - Portions of the auxiliary building are conservatively rated for 3-hours to provide exposure protection from a turbine building fire. Fire dampers are not provided for roof penetrations, which are adequately protected by housings of noncombustible construction.
6.4.9.5 Fire dampers shall be equipped for automatic closure by thermal release elements. The fire damper shall be mounted directly into the separating wall or the duct shall be protected between the wall and the damper according to the fire resistance of the separating wall structure.	Comply
6.4.9.6 Fire dampers shall be designed and installed so that the air velocity in the ducts assists in closing fire dampers and does not preclude proper damper closure.	Comply
6.4.9.7 Ventilation ducts containing fire dampers shall be provided with access ports for ease of inspection and for replacement of the thermal element.	Comply
6.4.10 Filters.	N/A - Heading

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
6.4.10.1 Air entry filters shall have approved noncombustible filter media that produce a minimum amount of smoke (UL Class 1) when subjected to heat.	AC - Filters will be listed for UL 900. As of May 2012, Class 1 filters are obsolete as UL no longer lists filters to the former Class 1 criteria.
6.4.10.2 In order to decrease the fire hazard of these filters and of oil-bath-type filters, only approved fire-resistive adhesives and oils with the Cleveland open-cup flash point (ASTM D 92, <i>Standard Test Method for Flash and Fire Points by Cleveland Open Cup</i>) equal to or greater than 464°F (240°C) and that do not produce appreciable smoke shall be used.	Comply
6.4.10.3 High-efficiency particulate air filters (HEPA) shall meet the requirements of UL 586, <i>Standard for Test Performance of High-Efficiency Particulate Air Filter Units</i> .	Comply
6.4.10.4 Fixed water spray systems shall be provided for charcoal adsorber beds containing more than 100 lb (45.4 kg) of charcoal.	AC - HVAC charcoal beds are provided with fixed water spray systems. The WGS charcoal adsorber beds are provided with a permanent connection from a nitrogen purge line to allow nitrogen to be injected into the enclosed space containing the charcoal to extinguish a fire.
6.4.10.5 Fire suppression systems shall be installed to protect filters that collect combustible material.	Comply
6.5 Drainage.	N/A - Heading
6.5.1* Drainage shall be provided in all areas of the plant for the removal of all liquids directly to safe areas, or for containment in the area without adverse flooding of equipment and without endangering other areas.	Comply
6.5.2 Drainage and the prevention of equipment water damage shall be accomplished by one or more of the following: (1) Floor drains (2) Floor trenches (3) Open doorways or other wall openings (4) Curbs for containing or directing drainage (5) Equipment pedestals	N/A – See Below Comply Comply Comply Comply Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
(6) Pits, sumps, and sump pumps	Comply
<p>6.5.3 Drainage and any associated drainage facilities for a given area shall be sized to accommodate the volume of liquid produced by all of the following:</p> <p>(1) The spill of the largest single container of any flammable or combustible liquids in the area</p> <p>(2) Where automatic suppression is provided throughout, the credible volume of discharge (as determined by the fire hazards analysis) for the suppression system operating for a period of 30 minutes</p> <p>(3) * Where automatic suppression is not provided throughout, the contents of piping systems and containers that are subject to failure in a fire</p> <p>(4) Where the installation is outside, credible environmental factors such as rain and snow</p> <p>(5) Where automatic suppression is not provided throughout, the volume shall be based on a manual fire-fighting flow rate of 500 gal/min (1892.5 L/min) for a duration of 30 minutes, unless the fire hazards analysis demonstrates a different flow rate and duration</p>	<p>N/A - See Below</p> <p>Comply</p> <p>Comply</p> <p>Comply</p> <p>Comply</p> <p>NC. The AP1000 drains are not designed for 500 gpm, nor does the present fire hazards analysis demonstrate a different flow rate and duration.</p>
6.5.4 Floor drainage from areas containing flammable or combustible liquids shall be trapped to prevent the spread of burning liquids beyond the fire area.	Comply
6.5.5 Where gaseous fire suppression systems are installed, floor drains shall be provided with adequate seals, or the fire suppression system shall be sized to compensate for the loss of fire suppression agent through the drains.	N/A - AP1000 has no gaseous fire suppression systems.
6.5.6 Drainage facilities shall be provided for outdoor oil-insulated transformers, or the ground shall be sloped such that oil spills flow away from buildings, structures, and adjacent transformers.	Comply
6.5.6.1 Unless drainage from oil spills is accommodated by sloping the ground around transformers away from structures or adjacent equipment, consideration shall be given to providing curbed areas or pits around transformers.	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
<p>6.5.6.2 If a layer of uniformly graded stone is provided in the bottom of the curbed area or pit as a means of minimizing ground fires, the following shall be assessed.</p> <p>(1) The sizing of the pit shall allow for the volume of the stone.</p> <p>(2) The design shall address the possible accumulation of sediment or fines in the stone.</p>	Comply
<p>6.5.7 For facilities consisting of more than one generating unit, a curb or trench drain shall be provided on solid floors where the potential exists for an oil spill, such that oil released from the incident on one unit will not expose an adjacent unit.</p>	Comply
<p>6.5.8 Water drainage from areas that might contain radioactivity shall be collected, sampled, and analyzed before discharge to the environment.</p>	Comply
<p>6.5.9 Water released during fire suppression operations in areas containing radioactivity shall be drained to a location that would be acceptable for the containment of radioactive materials.</p>	Comply
<p>6.6 Emergency Lighting.</p>	N/A - Heading
<p>6.6.1 Emergency lighting units shall provide adequate lighting levels. The lighting units shall be sized to provide a duration of operation that will adequately illuminate the egress and access routes to areas containing safe shutdown equipment and the equipment operation until normal or emergency plant lighting can be re-established.</p>	Comply
<p>6.6.2 The illumination of means of egress shall be in accordance with NFPA 101, <i>Life Safety Code</i>. The illumination shall include emergency lighting and marking of the means of egress.</p>	Comply
<p>6.6.3 The floor of the means of egress and the safe shutdown operations shall be illuminated at all points including angles, intersections of corridors, passageways, stairways, landings of stairways, exit doors, safe shutdown equipment, and access and egress routes to safe shutdown equipment to values of not less than 1 footcandle measured at the floor and at safe shut-down equipment.</p>	Comply
<p>6.6.4 The required illumination shall be so arranged that the failure of any single lighting unit, such as the burning out of a single light bulb, will not leave any area in darkness.</p>	Comply
<p>6.6.5 Suitable battery-powered hand lights shall be provided for emergency use by the fire brigade and other operations personnel required to achieve safe plant shutdown.</p>	Comply
<p>6.7 Lightning Protection. The plant shall be provided with a lightning protection system in accordance with NFPA 780, <i>Standard for the Installation of Lightning Protection Systems</i>.</p>	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
6.8 Electrical Cabling.	N/A - Heading
6.8.1 As a minimum, combustible cable insulation and jacketing material shall meet the fire and flame test requirements of IEEE 383, <i>Standard for Type Test of Class IE Electric Cables, Field Splices and Connections for Nuclear Power Generating Stations</i> . Meeting the requirements of IEEE 383 shall not eliminate the need for protection as specified in this standard and the fire hazards analysis.	Comply - The insulating and jacketing material for electrical cables are selected to meet the fire and flame test requirements of IEEE Standard 1202 or IEEE Standard 383 excluding the option to use flame source, oil, or burlap.
6.8.2 Fiber optic cable insulation and jacketing material shall meet the fire and flame test requirements of IEEE 383, <i>Standard for Type Test of Class IE Electric Cables, Field Splices and Connections for Nuclear Power Generating Stations</i> .	Comply - The insulating and jacketing material for electrical cables are selected to meet the fire and flame test requirements of IEEE Standard 1202 or IEEE Standard 383 excluding the option to use flame source, oil, or burlap.
6.8.3 Group cabling shall be routed away from exposure hazards or protected as specified in this standard. Specifically, group cabling shall not be routed near sources of ignition or flammable and combustible liquid hazards.	Comply
6.8.4 Cable raceways shall be used only for cables.	Comply
6.8.5 Only metal shall be used for cable trays	Comply
6.8.6 Only metallic tubing shall be used for conduit. <i>Exception: Nonmetallic conduit shall be permitted to be used with concrete encasement or for direct burial runs.</i>	Comply
6.8.6.1 Thin-wall metallic tubing shall not be used.	Comply
6.8.6.2 Flexible metallic tubing shall only be used in lengths less than 5 ft (1.5 m) to connect components to equipment.	Comply
6.8.6.3 Other raceways shall be made of noncombustible materials.	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
<p>6.9* Exposure Protection. Buildings shall be protected from exposure fires by any one of the following:</p> <p>(1) A listed 3-hour fire barrier with automatic or self-closing fire doors having a fire protection rating of 3 hours and listed penetration protection of a 3-hour rating</p> <p>(2) A spatial separation of at least 50 ft (15.2 m)</p> <p>(3) Exterior exposure protection</p>	Comply
<p>6.10 Electrical Systems for the Plant. The electrical design and installation of electrical generating, control, transmission, distribution, and metering of electrical energy shall be provided in accordance with NFPA 70, <i>National Electrical Code</i>, or ANSI C2, <i>National Electrical Safety Code</i>, as applicable.</p>	Comply
<p>6.11 Communications.</p>	N/A - Heading
<p>6.11.1 The plant-approved voice/alarm communication system in accordance with NFPA 72, <i>National Fire Alarm Code</i>®, shall be available on a priority basis for fire announcements, directing plant fire brigade, and fire evacuation announcements.</p>	Comply
<p>6.11.2* A portable radio communication system shall be provided for use by the fire brigade and other operation personnel required to achieve safe shutdown.</p>	Comply
<p>6.11.3 The radio communication system shall not interfere with the communication capabilities of the plant security force.</p>	Comply
<p>6.11.4 The impact of fire damage on the communication systems shall be considered when installing fixed repeaters to permit the use of portable radios. Repeaters shall be located such that a fire-induced failure of the repeater will not also cause failure of the other communication systems relied upon for safe shutdown.</p>	Comply
<p>6.11.5* Plant control equipment shall be designed so that the control equipment is not susceptible to radio frequency interferences from portable radios.</p>	Comply
<p>6.11.6 Preoperational tests and periodic testing shall demonstrate that the frequencies used for portable radio communications will not affect actuation of protective relays or other electrical components.</p>	Comply
<p>Chapter 7 General Fire Protection Systems and Equipment</p>	N/A - Heading
<p>7.1 General.</p>	N/A - Heading
<p>7.1.1* A fire hazards analysis shall be conducted to determine the fire protection requirements for the facility.</p>	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
<p>7.1.2* All fire protection systems, equipment, and installations shall be dedicated to fire protection purposes.</p> <p><i>Exception No. 1: Except when in accordance with 7.4.9.</i></p> <p><i>Exception No. 2: Fire protection systems shall be permitted to be used to provide redundant backup to nuclear-safety systems provided the fire protection systems meet the design basis requirements of the nuclear-safety systems. Fire protection systems used in this manner shall be designed to handle both functions.</i></p>	<p>The PCS tank has a dedicated volume for fire protection, however the balance of the tank serves other purposes</p> <p>The PCS recirculation pumps, which serve as a backup to the fire pumps after a seismic event, are not dedicated for fire protection</p> <p>PCS ancillary water tank has a dedicated volume for fire protection, however, the balance of the tank serves other purposes</p> <p>The fire pumps:</p> <p>serve the containment spray function through a normally closed valve</p> <ul style="list-style-type: none"> • can provide containment cooling • can provide component cooling to the RNS heat exchangers through temporary (not normally installed) connections <p>The second fire water storage tank has a dedicated volume for fire protection, however, the balance of the tank serves other purposes (raw water storage)</p>
<p>7.1.3 All fire protection equipment shall be listed or approved for its intended service.</p>	<p>The PCS tanks are not listed or approved equipment</p> <p>The PCS recirculation pumps are not listed or approved equipment</p>
<p>7.2 Water Supply.</p>	<p>N/A - Heading</p>

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
<p>7.2.1* The fire water supply shall be calculated on the basis of the largest expected flow rate for a period of 2 hours, but shall not be less than 300,000 gal (1,135,500 L). This flow rate shall be based on 500 gpm (1892.5 L/min) for manual hose streams plus the largest design demand of any sprinkler or fixed water spray system as determined in accordance with this standard, NFPA 13, <i>Standard for the Installation of Sprinkler Systems</i>, or NFPA 15, <i>Standard for Water Spray Fixed Systems for Fire Protection</i>. The fire water supply shall be capable of delivering this design demand with the hydraulically least demanding portion of fire main loop out of service.</p>	Comply
<p>7.2.2* Two 100 percent {minimum of 300,000 gal (1,135,500 L) each} system capacity tanks shall be installed. The tanks shall be interconnected such that fire pumps can take suction from either or both. A failure in one tank or its piping shall not cause both tanks to drain. The tanks shall be designed in accordance with NFPA 22, <i>Standard for Water Tanks for Private Fire Protection</i>. <i>Exception: Refill times for filling the water tanks do not apply.</i></p>	Comply
<p>7.2.3* The tanks shall not be supplied by an untreated, raw water source.</p>	Comply
<p>7.2.4 Fire Pumps.</p>	N/A - Heading
<p>7.2.4.1 Fire pumps shall meet the requirements of NFPA 20, <i>Standard for the Installation of Stationary Pumps for Fire Protection</i>, and shall be automatic starting.</p>	Comply
<p>7.2.4.2* Fire pumps shall be provided to ensure that 100 percent of the flow rate capacity will be available assuming failure of the largest pump.</p>	Comply
<p>7.2.4.3 Individual fire pump connections to the yard fire main loop shall be separated with sectionalizing valves between connections. Each pump and its driver and controls shall be located in a room separated from the remaining fire pumps by a fire wall with a minimum rating of 3 hours. The fuel for the diesel fire pump(s) shall be separated so that it does not provide a fire source exposing safety-related equipment.</p>	Comply
<p>7.2.4.4 A method of automatic pressure maintenance of the fire protection system shall be provided independent of the fire pumps.</p>	Comply
<p>7.2.4.5 Supervisory signals and visible indicators required by NFPA 20 shall be received in the control room.</p>	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
<p>7.3 Valve Supervision. All fire protection water supply and system control valves shall be under a periodic inspection program (<i>see Chapter 3</i>) and shall be supervised by one of the following methods:</p> <p>(1) Electrical supervision with audible and visual signals in the main control room or another constantly attended location and monthly valve inspections.</p> <p>(2) Locking valves in their normal position and monthly valve inspections. Keys shall be made available only to authorized personnel.</p> <p>(3) Sealing valves in their normal positions and weekly valve inspections. This option shall be utilized only where valves are located within fenced areas or under the direct control of the property owner.</p>	COL
<p>7.4 Yard Mains, Hydrants, and Building Standpipes.</p>	N/A - Heading
<p>7.4.1* The underground yard fire main loop shall be installed to furnish anticipated water requirements. The type of pipe and water treatment shall be design considerations, with tuberculation as one of the parameters. Means for inspecting and flushing the systems shall be provided.</p>	Comply
<p>7.4.2 Approved visually indicating sectional control valves such as post-indicator valves shall be provided to isolate portions of the main for maintenance or repair without simultaneously shutting off the supply to both primary and backup fire suppression systems.</p>	Comply
<p>7.4.3 Valves shall be installed to permit isolation of outside hydrants from the fire main for maintenance or repair without interrupting the water supply to automatic or manual fire suppression systems.</p>	Comply
<p>7.4.4* Sectional control valves shall permit maintaining independence of the individual loop around each unit. For such installations, common water supplies shall also be permitted to be utilized. For multiple-reactor sites with widely separated plants {approaching 1 mi. (1.6 km) or more}, separate yard fire main loops shall be used.</p>	Comply
<p>7.4.5 Outside manual hose installation shall be sufficient to provide an effective hose stream to any on-site location. Hydrants with individual hose gate valves shall be installed approximately every 250 ft (76 m) apart on the yard main system. A hose house equipped with hose and combination nozzle and other auxiliary equipment specified in NFPA 24, <i>Standard for the Installation of Private Fire Service Mains and Their Appurtenances</i>, shall be provided at intervals of not more than 1000 ft (305 m) along the yard main system.</p> <p><i>Exception: Mobile means of providing hose and associated equipment, such as hose carts or trucks, shall be permitted in lieu of hose houses. Where provided, such mobile equipment shall be equivalent to the equipment supplied by three hose houses.</i></p>	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
<p>7.4.6 Threads compatible with those used by local fire departments shall be provided on all hydrants, hose couplings, and standpipe risers, or the fire departments shall be provided with adapters that allow interconnection between plant equipment and the fire department equipment.</p>	Comply
<p>7.4.7 Sprinkler systems and manual hose station standpipes shall have connections to the plant underground water main so that a single active failure or a crack in a moderate-energy line can be isolated so as not to impair both the primary and backup fire suppression systems. Alternatively, headers fed from each end shall be permitted inside buildings to supply both sprinkler and standpipe systems, provided steel piping and fittings meeting the requirements of ANSI B31.1, <i>Code for Power Piping</i>, are used for the headers (up to and including the first valve) supplying the sprinkler systems where such headers are part of the seismically analyzed hose standpipe system. Where provided, such headers shall be considered an extension of the yard main system. Each sprinkler and standpipe system shall be equipped with an outside screw and yoke (OS&Y) gate valve or other approved shutoff valve.</p>	Comply
<p>7.4.8 For all power block buildings, Class III standpipe and hose systems shall be installed in accordance with NFPA 14, <i>Standard for the Installation of Standpipe, Private Hydrant, and Hose Systems</i>. For all other buildings on site, the requirements for standpipe and hose systems shall be appropriate for the hazard being protected.</p>	Comply
<p>7.4.9* The proper type of hose nozzle to be supplied to each area shall be based on the fire hazards analysis. The usual combination spray/straight-stream nozzle shall not be used in areas where the straight stream can cause unacceptable damage. Approved, electrically safe fixed fog nozzles shall be provided at locations where high-voltage shock hazards exist. All hose nozzles shall have shutoff capability.</p>	Comply
<p>7.4.10 Seismic Fire Suppression Capabilities.</p>	N/A - Heading
<p>7.4.10.1* Provisions shall be made to supply water at least to standpipes and hose stations for manual fire suppression in all areas containing nuclear-safety-related systems and components for safe shutdown in the event of a safe shutdown earthquake (SSE).</p>	Comply
<p>7.4.10.2 The piping system serving these hose stations shall be analyzed for safe shutdown and earthquake loading, and shall be provided with supports that ensure pressure boundary integrity. The piping and valves for the portion of hose standpipe system affected by this functional requirement shall, as a minimum, satisfy the requirements of ANSI B31.1, <i>Code for Power Piping</i>.</p>	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
<p>7.4.10.3 The system shall be designed to flow a minimum of one Class III standpipe station in accordance with NFPA 14, <i>Standard for the Installation of Standpipe, Private Hydrant, and Hose Systems</i>.</p>	<p>AC - The seismic standpipe system is operated in the same manner during normal plant operation or following a safe shutdown earthquake. It is supplied with water from the safety related passive containment cooling system storage tank and normally operates independently of the rest of the fire protection system. The supply line draws water from a portion of the storage tank, using water allocated for fire protection. This volume of water is sufficient to supply two hose streams, each with a flow of 75 gallons per minute, for 2 hours as required by BTP CMEB 9.5-1, Revision 2 (July 1981).</p>
<p>7.4.10.4 Where the seismic required hose stations are cross-connected to essential seismic Category I water systems, the fire flow shall not degrade the essential water system requirements.</p>	<p>Comply</p>
<p>7.5 Portable Fire Extinguishers.</p>	<p>N/A - Heading</p>
<p>7.5.1 Portable and wheeled fire extinguishers shall be installed, inspected, maintained, and tested in accordance with NFPA 10, <i>Standard for Portable Fire Extinguishers</i>.</p> <p><i>Exception: Where placement of extinguishers would result in required activities that are contrary to personnel radiological exposure concerns or nuclear-safety-related concerns, fire extinguishers shall be permitted to be inspected at intervals greater than those specified in NFPA 10, Standard on Portable Fire Extinguishers, or consideration shall be given to locating the extinguishers outside high radiation areas.</i></p>	<p>Comply</p>
<p>7.6 Fire Suppression Systems.</p>	<p>N/A - Heading</p>
<p>7.6.1 Automatic suppression systems shall be provided in all areas of the plant as required by the fire hazards analysis. Except as modified in this chapter, the following NFPA standards shall be used:</p> <p>(1) NFPA 11, Standard for Low-Expansion Foam</p> <p>(2) NFPA 11A, Standard for Medium-and High-Expansion Foam Systems</p> <p>(3) NFPA 12, Standard on Carbon Dioxide Extinguishing Systems</p>	<p>N/A - See below</p> <p>N/A</p> <p>N/A</p> <p>N/A</p>

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
(4) NFPA 13, Standard for the Installation of Sprinkler Systems	Comply
(5) NFPA 15, Standard for Water Spray Fixed Systems for Fire Protection	Comply
(6) NFPA 16, Standard for the Installation of Foam-Water Sprinkler and Foam-Water Spray Systems	N/A
(7) NFPA 17, Standard for Dry Chemical Extinguishing Systems	N/A
(8) NFPA 214, Standard on Water-Cooling Towers	Comply
(9) NFPA 2001, Standard on Clean Agent Fire Extinguishing Systems	N/A
7.6.2 The extinguishing systems chosen shall be based upon the design parameters required as a result of the fire hazards analysis.	Comply
7.6.3 Selection of extinguishing agent shall be based on all of the following: (1) Type or class of hazard (2) Effect of agent discharge on critical equipment such as thermal shock, continued operability, water damage, overpressurization, cleanup, and so forth (3) Health hazards	Comply Comply Comply Comply
7.6.4 Each fire suppression system shall be equipped with approved alarming devices and annunciate in a constantly attended area.	Comply
7.7 Fire Alarm Systems.	N/A - Heading
7.7.1 Fire signaling systems shall be provided in all areas of the plant as required by the fire hazards analysis. The requirements of this chapter shall constitute the minimum acceptable protective signaling system functions when used in conjunction with NFPA 72, <i>National Fire Alarm Code</i> .	Comply
7.7.2* The signaling system's initiating device and signaling line circuits shall provide emergency operation for fire detection, fire alarm, and water flow alarm during a single break or a single ground fault.	Comply
7.7.3 The fire signaling equipment used for fixed fire suppression systems shall give audible and visual alarm and system trouble annunciation in the plant control room for the power block buildings. Local alarms shall be provided. Other fire alarm signals from other buildings shall be permitted to annunciate at the control room or other locations that are constantly attended.	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
7.7.4* Audible signaling appliances shall produce a distinctive sound, used for no other purpose. Audible signaling devices shall be located and installed so that the alarm can be heard above ambient noise levels.	Comply
7.7.5 Plant control room or plant security personnel shall be trained in the operation of all fire signaling systems used in the plant. This training shall include the ability to identify any alarm zone or fire protection system that is operating.	Comply
7.7.6 Fire signaling equipment and actuation equipment for the release of fixed fire suppression systems shall be connected to power supply sources in accordance with the requirements of NFPA 72, <i>National Fire Alarm Code</i> , and shall be routed outside the area to be protected.	Comply
7.7.7* Manual fire alarm boxes shall be installed as required by the fire hazards analysis. Where manual release devices are installed for the purpose of releasing an extinguishing agent in a fixed fire suppression system, the manual releases shall be clearly marked for that purpose. The manual release device circuits shall be routed outside the area protected by the fixed extinguishing system.	Comply
7.7.8 All signals shall be permanently recorded in accordance with NFPA 72, <i>National Fire Alarm Code</i> .	Comply
<p>7.8 Fire Detectors. Automatic fire detectors shall be selected and installed in accordance with all of the following:</p> <p>(1) NFPA 72, <i>National Fire Alarm Code</i></p> <p>(2) The design parameters required as a result of the fire hazards analysis of the plant area</p> <p>(3) The additional requirements of this standard</p>	<p>Comply</p> <p>Comply</p> <p>Comply</p> <p>Comply</p>
Chapter 8 Identification of and Protection Against Hazards	N/A - Heading
8.1* General. The identification and selection of fire protection systems shall be based on the fire hazards analysis. This chapter identifies fire and explosion hazards in advanced light water reactor plants and specifies the protection criteria that shall be used unless the fire hazards analysis indicates otherwise.	Comply
8.2 Primary and Secondary Containments.	N/A - Heading
8.2.1 Normal Operation. Fire protection for the primary and secondary containment areas shall be provided for hazards identified by the fire hazards analysis.	Comply
8.2.1.1 Operation of the fire protection systems shall not compromise the integrity of the containment or other safety-related systems. Fire protection systems in the containment areas shall function in conjunction with total containment requirements such as ventilation and control of containment liquid and gaseous release.	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
<p>8.2.1.2 Inside primary containment, fire detection systems shall be provided for each fire hazard identified in the fire hazards analysis. The type of detection used and the location of the detectors shall be the most suitable for the particular type of fire hazard identified by the fire hazards analysis.</p>	Comply
<p>8.2.1.3 A general area fire detection capability shall be provided in the primary containment as a backup for the hazard detection described above. To accomplish this, suitable smoke or heat detectors compatible with the radiation environment shall be installed in accordance with NFPA 72, <i>National Fire Alarm Code</i>.</p>	Comply
<p>8.2.1.4 Standpipe and hose stations shall be installed inside containment. Standpipe and hose stations inside containment shall be permitted to be connected to a high quality water supply of sufficient quantity and pressure other than the fire main loop if plant-specific features prevent extending the fire main supply inside containment.</p> <p><i>Exception: For inerted primary containment, standpipe and hose stations shall be permitted to be placed outside the primary containment, with hose no longer than 100 ft (30.5 m), to reach any location inside the primary containment with a 30-ft (9.1-m) effective hose stream.</i></p>	Comply
<p>8.2.1.5 Reactor coolant pumps with an external lubrication system shall be provided with an oil collection system. The oil collection system shall be so designed, engineered, and installed that failure of the oil collection system will not lead to a fire during normal operations, or off-normal conditions such as accident conditions or earthquakes.</p>	N/A. AP1000 RCPs use water lubrication.
<p>8.2.1.6* The oil collection systems shall be capable of collecting oil from all potential pressurized and unpressurized leakage sites in the reactor coolant pump oil systems. Leakage shall be collected and drained to a vented closed container that can hold the entire oil system inventory. Leakage points to be protected shall include the lift pump and piping, overflow lines, oil cooler, oil fill and drain lines and plugs, flanged connections on oil lines, and oil reservoirs where such features exist on the reactor coolant pumps. The drain line shall be large enough to accommodate the largest potential oil leak.</p>	N/A. AP1000 RCPs use water lubrication.
<p>8.2.2 Refueling and Maintenance.</p>	N/A - Heading
<p>8.2.2.1* Management procedures and controls necessary to ensure adequate fire protection for fire hazards introduced during maintenance and refueling shall be provided. Adequate backup fire suppression shall be provided so that total reliance is not placed on a single fire suppression system.</p>	O/O
<p>8.2.2.2 Adequate self-contained breathing apparatus shall be provided near the containment entrance for fire-fighting and damage control personnel. These units shall be independent of any breathing apparatus or air supply systems provided for general plant activities and shall be clearly marked as emergency equipment.</p>	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
8.3 Control Room Complex.	N/A - Heading
8.3.1 The control room complex (including kitchen, office spaces, etc.) shall be protected against disabling fire damage and shall be separated from other areas of the plant by floors, walls, ceilings, and roofs having a minimum fire resistance rating of 3 hours. Peripheral rooms in the control room complex shall have an automatic water-based suppression system, where required by the fire hazards analysis, and shall be separated from the control room by noncombustible construction with a minimum fire resistance rating of 1 hour. Ventilation system openings between the control room and the peripheral rooms shall have automatic smoke dampers installed that close on operation of the fire detection and fire suppression systems.	Comply - The MCR/Operator Work Area wall is not fire-rated based on other design criteria. Manual fire suppression is provided for peripheral rooms. See Appendix 9A of the Design Control Document.
8.3.2 Manual fire-fighting capability shall be provided for both of the following: (1) Fires originating within a cabinet, console, or connecting cables (2) Exposure fires involving combustibles in the general room area	Comply Comply Comply
8.3.3 Portable Class A and Class C fire extinguishers shall be located in the control room. A fire hose station shall be installed immediately outside of the control room.	Comply
8.3.4 Nozzles that are compatible with the hazards and the equipment in the control room shall be provided for the fire hose stations. The choice of nozzles shall satisfy fire-fighting requirements and electrical safety requirements, and shall minimize physical damage to electrical equipment from hose stream impingement.	Comply
8.3.5 Smoke detectors shall be provided in the control room complex, the electrical cabinets, and consoles. If redundant safe shutdown equipment is located in the same control room cabinet or console, the cabinet or console shall be provided with internal separation (noncombustible barriers) to limit the damage to one safety division.	NC - Smoke detectors are not provided in cabinets and consoles. The control room is continuously occupied so that a fire is promptly detected and extinguished.
8.3.6 Breathing apparatus for the control room operators shall be readily available.	Comply
8.3.7 The outside air intakes for the control room ventilation system shall be provided with smoke detection capability to alarm in the control room and enable manual isolation of the control room ventilation system, thus preventing smoke from entering the control room.	Comply
8.3.8 Venting of smoke produced by a fire in the control room by means of the normal ventilation system shall be permitted to be acceptable; however, provision shall be made to permit isolation of the recirculation portion of the normal ventilation system. Manually operated venting of the control room shall be available to the operators.	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
8.3.9 All cables that enter the control room shall terminate in the control room. No cabling shall be routed through the control room from one area to another. Cables in spaces under-floor and in above-ceiling spaces shall meet the separation criteria necessary for fire protection.	Comply
8.3.10 Air-handling functions shall be ducted separately from cable runs in such spaces (i.e., if cables are routed in under-floor or ceiling spaces, these spaces shall not be used as air plenums for ventilation of the control room). Fully enclosed electrical raceways located in such underfloor and ceiling spaces, if over 1 ft ² (0.09 m ²) in cross-sectional area, shall have automatic fire suppression inside. Area automatic fire suppression shall be provided for underfloor and ceiling spaces if used for cable runs unless all cable is run in 4-in. (101.6-mm) or smaller steel conduit or cables are in fully enclosed raceways internally protected by automatic fire suppression.	NC <ul style="list-style-type: none"> The under-floor space of the control room complex is used as a distribution plenum for ventilation of the main control room. Smoke detectors in the under-floor space cause prompt closure of combination fire/smoke dampers to shut off air flow. Automatic fire suppression is not provided for cable runs.
8.4 Cable Concentrations.	N/A - Heading
8.4.1 Cable Spreading Room.	N/A - Heading
8.4.1.1 The cable spreading room shall have an automatic water-based suppression system. The location of sprinklers or spray nozzles shall consider cable tray arrangements to ensure adequate water coverage for areas that could present exposure fire hazards to the cable raceways. Automatic sprinkler systems shall be designed for a density of 0.30 gpm/ft ² (12.2 L/min·m ²) over the most remote 2500 ft ² (232.2 m ²).	N/A - AP1000 has no cable spreading room.
8.4.1.2 Suppression systems shall be zoned to limit the area of protection to that which the drainage system can handle with any two adjacent systems actuated. Deluge and water spray systems shall be hydraulically designed with each zone calculated with the largest adjacent zone flowing.	N/A - AP1000 has no cable spreading room.
8.4.1.3 Cable spreading rooms shall have all of the following: <ol style="list-style-type: none"> At least two remote and separate entrances for access by the fire brigade personnel An aisle separation between tray stacks at least 3 ft (0.9 m) wide and 8 ft (24m) high Hose stations and portable fire extinguishers installed immediately outside the room * Area smoke detection 	N/A - AP1000 has no cable spreading room. N/A - AP1000 has no cable spreading room.

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
8.4.2 Cable Tunnels.	N/A - Heading
8.4.2.1* Detection Systems. Cable tunnels shall be provided with smoke detection.	Comply
8.4.2.2 Suppression Systems.	N/A - Heading
8.4.2.2.1 Cable tunnels shall be provided with automatic fixed suppression systems. Automatic sprinkler systems shall be designed for a density of 0.30 gpm/ft ² (12.2 L/min·m ²) for the most remote 100 linear ft (30.5 m) of cable tunnel up to the most remote 2500 ft ² (232.2 m ²).	NC. AP1000 does not provide cable tunnels with automatic fixed suppression systems.
8.4.2.2.2 The location of sprinklers or spray nozzles shall consider cable tray arrangements and possible transient combustibles to ensure adequate water coverage for areas that could present exposure fire hazards to the cable raceways.	Comply
8.4.2.2.3 Deluge sprinkler systems or deluge spray systems shall be zoned to limit the area of protection to that which the drainage system can handle with any two adjacent systems actuated. The systems shall be hydraulically designed with each zone calculated with the largest adjacent zone flowing.	Comply
8.4.2.3 Cables shall be designed to allow wetting undamaged cables with water supplied by the fire suppression system without electrical faulting.	Comply
<p>8.4.2.4 Cable tunnels over 50 ft (15.2 m) long shall have all of the following:</p> <ul style="list-style-type: none"> (1) At least two remote and separate entrances for access by the fire brigade personnel (2) An aisle separation between tray stacks at least 3 ft (0.9 m) wide and 8 ft (2.4 m) high (3) Hose stations and portable fire extinguishers installed immediately outside the tunnel 	<p>AP1000 is not explicitly designed to meet this requirement.</p> <p>AP1000 is not explicitly designed to meet this requirement.</p> <p>AP1000 is not explicitly designed to meet this requirement.</p>
8.4.3 Cable Shafts and Risers. Cable tray fire breaks shall be installed every 20 ft (6.1 m) for vertical cable trays that rise over 30 ft (9.1 m). Access to cable shafts shall be provided every 40 ft (12.2 m) with the topmost access within 20 ft (6.1 m) of the cable shaft ceiling. Automatic sprinkler protection and smoke detection shall be provided at the ceiling of the vertical shaft.	AP1000 is not explicitly designed to meet this requirement.
8.5 Plant Computer and Communication Rooms. Computer and communication rooms shall meet the applicable requirements of NFPA 75, <i>Standard for the Protection of Electronic Computer/ Data Processing Equipment</i> .	AP1000 is not explicitly designed to meet the requirements of NFPA 75.

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
8.6 Switchgear Rooms and Relay Rooms.	N/A - Heading
8.6.1* Smoke detection shall be provided and shall alarm in both the control room and locally. Cables entering the safety-related switchgear rooms shall terminate in the switchgear room. The safety-related switchgear rooms shall not be used for other purposes. Fire hose stations and portable fire extinguishers shall be readily available outside the area.	Comply
8.6.2 Equipment shall be located to facilitate fire fighting. Drains shall be provided to prevent water accumulation from damaging safety-related equipment. Remote manually actuated ventilation shall be provided for smoke removal when manual fire suppression is needed. <i>(See Section 6.4.)</i>	Comply
8.7 Battery Rooms.	N/A - Heading
8.7.1* Battery rooms shall be provided with ventilation to limit the concentration of hydrogen to 2 percent by volume. Loss of ventilation shall alarm in the control room.	Comply
8.7.2 Safety-related battery rooms shall be protected against fires and explosions. Battery rooms shall be separated from other areas of the plant by fire barriers having a 1-hour minimum rating. Direct current switchgear and inverters shall not be located in these battery rooms. Fire detection shall be provided. Fire hose stations and portable fire extinguishers shall be readily available outside the room.	Comply
8.8 Turbine Building.	N/A - Heading
8.8.1* The turbine building shall be separated from adjacent structures containing safety-related equipment by fire-resistive barriers having a minimum 3-hour rating. The fire barriers shall be designed so that the barrier will remain in place even in the event of a complete collapse of the turbine structure. Openings and penetrations shall be minimized in the fire barrier and shall not be located where turbine oil systems or generator hydrogen cooling systems create a direct fire exposure hazard to the fire barrier. Smoke and heat removal systems shall be provided in accordance with 6.4.3. <i>Exception: For those plants provided with complete automatic sprinkler protection at the roof level, smoke and heat removal systems are not required.</i>	Comply
8.8.2 Beneath Turbine Generator Operating Floor.	N/A - Heading
8.8.2.1* All areas beneath the turbine generator operating floor shall be protected by an automatic sprinkler or foam-water sprinkler system. The sprinkler system beneath the turbine generator shall take into consideration obstructions from structural members and piping and shall be designed to a minimum density of 0.30 gpm/ft ² (12.2 L/min·m ²) over a minimum application of 5000 ft ² (464.5 m ²).	AC - AP1000 does not sprinkler all areas beneath the turbine generator operating floor. Sprinklers are provided as identified in the AP1000 DCD Section 9A.

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
8.8.2.2 Foam-water sprinkler systems installed in place of automatic sprinklers described above shall be designed in accordance with NFPA 16, <i>Standard for the Installation of Foam-Water Sprinkler and Foam-Water Spray Systems</i> , and the design densities specified above.	N/A. AP1000 does not use foam-water sprinkler systems.
8.8.2.3 Electrical equipment in the area covered by a water or foam system shall be of the enclosed type or otherwise protected to minimize water damage in the event of system operation.	Comply
8.8.3* Turbine Generator Bearings.	Comply
8.8.3.1 Automatic fixed suppression systems shall be provided for all turbine generator and exciter bearings. If closed-head water spray systems utilizing directional nozzles in accordance with NFPA 15, <i>Standard for Water Spray Fixed Systems for Fire Protection</i> , are provided, bearing protection shall be provided for a minimum density of 0.30 gpm/ft ² (12.2 L/min·m ²) over the protected area.	Comply - Automatic fixed suppression systems are provided for oil spill areas around the turbine-generator and the generator seal oil unit.
8.8.3.2 Accidental water discharge on bearing points and hot turbine parts shall be considered. If necessary, these areas shall be permitted to be protected by shields and encasing insulation with metal covers.	Comply
8.8.4 Lubricating oil lines above the turbine operating floor shall be protected with an automatic sprinkler system covering those areas subject to oil accumulation, including the area within the turbine lagging (skirt). The automatic sprinkler system shall be designed to a minimum density of 0.30 gpm/ft ² (12.2 L/min·m ²).	Comply - Automatic fixed suppression systems are provided for oil spill areas around the turbine-generator.
8.8.5 Lubricating oil reservoirs and handling equipment shall be protected in accordance with 8.8.2.1. If the lubricating oil reservoir is elevated, sprinkler protection shall be extended to protect the area beneath the reservoir.	Comply
8.8.6 If shaft-driven ventilation systems are not used, the area inside a directly connected exciter housing shall be protected with an automatic fire suppression system. If shaft-driven ventilation systems are used, an automatic preaction sprinkler system providing a density of 0.30 gpm/ft ² (12.2 L/min·m ²) over the entire area shall be provided.	NC - AP1000 is not explicitly designed to meet this paragraph.
8.8.7* Clean or dirty oil storage areas shall be protected based on the fire risk evaluation. The designer shall consider, as a minimum, the installation of fixed automatic fire protection systems and the ventilation and drainage requirements in Chapter 6.	Comply
8.8.8 Hydrogen Systems.	N/A - Heading
8.8.8.1* General.	N/A - Heading

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
8.8.8.1.1* Bulk hydrogen systems supplying one or more generators shall have automatic valves located at the supply and operable by “dead man”-type controls at the generator fill point(s) or operable from the control room. Alternatively, vented guard piping shall be permitted to be used inside the building to protect runs of hydrogen piping.	Comply
8.8.8.1.2 A flanged spool piece or equivalent arrangement shall be provided to facilitate the separation of hydrogen supply when the generator is open for maintenance.	Comply
8.8.8.1.3 Control room alarms shall be provided to indicate abnormal gas pressure, temperature, and percentage of hydrogen in the generator.	Comply
8.8.8.1.4 The generator hydrogen dump valve and hydrogen detrainning equipment shall be arranged to vent directly to a safe outside location. The dump valve shall be remotely operable from the control room or from an area accessible during a machine fire.	Comply
8.8.8.1.5* An excess-flow check valve shall be provided for the bulk supply hydrogen piping.	Comply
8.8.8.2 Hydrogen Seal Oil Pumps.	N/A - Heading
8.8.8.2.1 Redundant hydrogen seal oil pumps with separate power supplies shall be provided for adequate reliability of seal oil supply.	Comply
8.8.8.2.2 Where feasible, electrical circuits to redundant pumps shall be run in buried conduit or provided with fire-retardant coating if exposed in the area of the turbine generator to minimize the possibility of loss of both pumps as a result of a turbine generator fire.	Comply
8.8.8.2.3 Hydrogen seal oil units shall be protected in accordance with 8.8.2. Hydrogen seal oil units shall be protected by an automatic, open-head water spray system providing a density of 0.30 gpm (1.13 L/min) over the hydrogen seal area.	See response to 8.8.2.
8.8.8.2.4 Curbing or drainage or both shall be provided for the hydrogen seal oil unit in accordance with Section 6.5.	Comply
8.8.8.3 Hydrogen in Safety-Related Areas.	N/A - Heading
8.8.8.3.1 Hydrogen lines in safety-related areas shall be either designed to seismic Class I requirements or sleeved such that the outer pipe is directly vented to the outside, or shall be equipped with excess-flow valves so that, in case of a line break, the hydrogen concentration in the affected areas will not exceed 2 percent.	Comply
8.8.8.3.2 Hydrogen lines or sensing lines containing hydrogen shall not be piped into or through the control room.	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
8.8.9 Hydraulic Control Systems. The hydraulic control system shall use a listed fire-resistant fluid.	AC - The AP1000 design follows equipment manufactures recommendation and does not explicitly include this requirement.
8.8.10* Lubricating Oil Systems.	N/A - Heading
8.8.10.1 Turbine lubricating oil reservoirs shall be provided with vapor extractors, which shall be vented to a safe outside location.	Comply
8.8.10.2 Curbing or drainage or both shall be provided for the turbine lubricating oil reservoir in accordance with Section 6.5.	Comply
8.8.10.3 All oil pipe serving the turbine generator shall be designed and installed to minimize the possibility of an oil fire in the event of severe turbine vibration.	Comply
8.8.10.4* Piping design and installation shall consider all of the following measures: (1) Welded construction (2) Guard pipe construction with the pressure feed line located inside the return line or in a separate shield pipe drained to the oil reservoir (3) Route oil piping clear of or below steam piping or metal parts (4) Insulate with impervious lagging for steam piping or hot metal parts under or near oil piping or turbine bearing points	Comply
8.8.10.5 Cable for operation of the lube oil pumps shall be protected from fire exposure. Where feasible, electrical circuits to redundant pumps shall be run in buried conduit. Protection shall be permitted to consist of separation of cables for ac and dc oil pumps or 1-hour fire-resistive coating (derating of cable shall be considered).	Comply
8.9 Standby Emergency Diesel Generators and Combustion Turbines.	N/A - Heading
8.9.1 The installation and operation of standby emergency diesel generators and combustion turbines shall be in accordance with NFPA 37, <i>Standard for the Installation and Use of Stationary Combustion Engines and Gas Turbines</i> . <i>Exception: Automatic shutdown and remote shutdown features, which shall be governed by nuclear-safety requirements.</i>	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
8.9.2 Standby emergency diesel generators and combustion turbines located within main plant structures shall be protected by automatic sprinkler, water spray, or foam-water sprinkler systems. Sprinkler and water spray protection systems shall be designed for a 0.25-gpm/ft ² (10.19-L/min·m ²) density over the entire area.	Comply
8.9.3 Fire detection shall be provided to alarm and annunciate in the control room and to alarm locally. Fire hose stations and portable fire extinguishers shall be readily available outside the area. Drainage for fire-fighting water and means for local manual venting of smoke shall be provided.	Comply
8.9.4 A day tank shall be permitted in standby emergency diesel generator and combustion turbine rooms if the day tank is located in a diked enclosure that has sufficient capacity to hold 110 percent of the contents of the day tank or is drained to a safe location.	Comply
8.10 Diesel Fuel Storage and Transfer Areas.	N/A - Heading
8.10.1* Diesel fuel oil storage tanks shall not be located inside buildings containing other nuclear-safety-related equipment. If aboveground tanks are used, they shall be located at least 50 ft (15.2 m) from any building, or if within 50 ft (15.2 m), they shall be separated from the building by a fire barrier having a minimum 3-hour rating. Potential oil spills shall be confined or directed away from buildings containing safety-related equipment.	Comply
8.10.2 Aboveground tanks shall be provided with automatic fire suppression systems.	NC
8.11 Nuclear Safety-Related Pump Rooms. These rooms shall be protected by fire detection systems. Automatic fire suppression systems shall be provided unless the fire hazards analysis determines that fire suppression is not required. Fire hose stations and fire extinguishers shall be readily accessible.	N/A. AP1000 has no safety-related pumps.
8.12 New Fuel Area.	N/A - Heading
8.12.1 Fire extinguishers shall be located within the new fuel area. Fire hose stations shall be located as determined by the fire hazards analysis to facilitate access and use for fire-fighting operations. Fire detection systems shall be provided. Combustible material shall be limited to the minimum necessary for operation in the new fuel area.	Comply
8.12.2 The storage configuration of new fuel shall always be maintained as to preclude criticality for any water density that could occur during fire water application.	Comply
8.13 Spent Fuel Pool Area. Protection for the spent fuel pool area shall be provided by fire hose stations and fire extinguishers. Fire detection shall be provided in the area.	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
8.14 Rad Waste and Decontamination Areas. Fire barriers, fire detection, and automatic fire suppression shall be provided as determined by the fire hazards analysis. Manual ventilation control to assist in smoke removal shall be provided if necessary for manual fire fighting.	Comply
8.15 Safety-Related Water Tanks. Storage tanks that supply water for fire-safe shutdown shall be protected from the effects of an exposure fire. Combustible materials shall not be stored next to these tanks.	Comply
8.16 Record Storage Areas. Record storage areas shall be located and protected in accordance with NFPA 232, <i>Standard for the Protection of Records</i> . Record storage areas shall not be located in safety-related areas and shall be separated from safety-related areas by fire barriers having a minimum 3-hour rating.	N/A – Not in AP1000 certified design.
8.17 Cooling Towers. Cooling towers shall be of noncombustible or limited-combustible construction and located such that a fire in the cooling tower will not adversely affect safety-related systems or equipment. Cooling towers shall be of non-combustible construction when the basin is used as the ultimate heat sink. <i>Exception: If combustible construction is used, the cooling towers shall be protected by automatic sprinklers or water spray systems in accordance with NFPA 214, Standard on Water Cooling Towers, and shall be located so that they do not affect safety-related systems or equipment in the event of a fire.</i>	Comply
8.18 Acetylene-Oxygen Fuel Gases. Gas cylinder storage locations or the fire protection systems that serve those safety-related areas shall not be in areas that contain or expose safety-related equipment.	Comply, O/O
8.19 Storage Areas for Ion Exchange Resins. Unused ion exchange resins shall not be stored in areas that contain or expose safety-related systems or equipment.	Comply, O/O
8.20 Storage Areas for Hazardous Chemicals. Hazardous chemicals shall not be stored in areas that contain or expose safety-related systems or equipment.	Comply, O/O
8.21 Warehouses. Automatic sprinkler protection shall be provided for warehouses that contain high-value equipment or combustible materials.	N/A - Not in AP1000 certified design
8.22 Fire Pump Room/House. Rooms housing diesel-driven fire pumps shall be protected by automatic sprinkler, water spray, or foam-water sprinkler systems. If sprinkler and water spray systems are provided for fire pump houses, they shall be designed for a minimum density of 0.25 gpm/ft ² (10.19 L/min·m ²) over the entire fire area	Comply

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT						
8.23 Transformers.	N/A - Heading						
8.23.1 Buildings shall be protected from exposure fires involving oil-filled transformers by locating the transformer casing, conservator tank, and cooling radiators at least 50 ft (15.2 m) from buildings, by providing a minimum 2-hour fire barrier between transformers as required in Figures 8.23.1(a) and (b) and exposed buildings or by complying with Table 8.23.1. <i>{See Figures 8.23.1(a) and (b).}</i> A minimum 1-hour fire barrier or a distance of 30 ft (9.1 m) shall be provided between adjacent transformers. Means shall be provided to contain oil spills.	Comply						
<p style="text-align: center;">Table 8.23.1 Transformer Spacing Separation Distances</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Transformer Oil Capacity</th> <th style="text-align: left;">Minimum (Line-of-Sight) Separation without Firewall</th> </tr> </thead> <tbody> <tr> <td>Less than 5000 gal (18,925 L)</td> <td>25 ft (7.6 m)</td> </tr> <tr> <td>Over 5000 gal (18,925 L) 50 ft</td> <td>50 ft (15.2 m) Bushing</td> </tr> </tbody> </table>	Transformer Oil Capacity	Minimum (Line-of-Sight) Separation without Firewall	Less than 5000 gal (18,925 L)	25 ft (7.6 m)	Over 5000 gal (18,925 L) 50 ft	50 ft (15.2 m) Bushing	Comply
Transformer Oil Capacity	Minimum (Line-of-Sight) Separation without Firewall						
Less than 5000 gal (18,925 L)	25 ft (7.6 m)						
Over 5000 gal (18,925 L) 50 ft	50 ft (15.2 m) Bushing						
FIGURE 8.23.1(a) Transformer spacing.	Comply						
FIGURE 8.23.1(b) Transformer spacing.	Comply						
8.23.2 Oil-filled main, station service, and start-up transformers shall be protected with automatic water spray systems in accordance with NFPA 15, <i>Standard for Water Spray Fixed Systems for Fire Protection</i> , or foam-water spray systems in accordance with NFPA 16, <i>Standard for the Installation of Foam-Water Sprinkler and Foam-Water Spray Systems</i> .	Comply						
8.23.3 Transformers installed inside fire areas containing safety-related systems or equipment shall be of the dry type or insulated and cooled with noncombustible liquid. <i>Exception: Transformers filled with combustible fluid that are located indoors shall be enclosed in a transformer vault {see Article 450(c) of NFPA 70}.</i>	Comply						
8.24 Auxiliary Boilers.	N/A - Heading						
8.24.1 Auxiliary boilers, their fuel burning systems, combustion product removal systems, and related control equipment shall be installed and operated in accordance with NFPA 85, <i>Boiler and Combustion Systems Hazards Code</i> .	The AP1000 is not explicitly designed to the requirements of NFPA 85. It is designed to NFPA 8501.						
8.24.2 Oil-fired boilers or boilers using oil ignition within the main plant shall be protected with automatic sprinkler, water spray, or foam-water sprinkler systems covering the boiler area. Sprinkler and water spray systems shall be designed for a minimum density of 0.25 gpm/ft ² (10.19 L/min·m ²) over the entire area.	Comply						

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
8.25 Offices, Shops, and Storage Areas. Automatic sprinklers shall be provided for storage rooms, offices, and shops containing combustible materials that present an exposure to surrounding areas that are critical to plant operation, and shall be so located and protected that a fire or the effects of a fire, including smoke, will not adversely affect any safety-related systems or equipment.	N/A - Not in AP1000 certified design.
8.26 Simulators. Simulators shall be provided with a fixed automatic suppression system. Simulators and supporting equipment shall be separated from other areas by a fire barrier with a minimum 1-hour rating.	N/A - Not in AP1000 certified design.
8.27 Technical Support and Emergency Response Centers. Technical support centers shall be separated from all other areas by fire barriers, or separated from all other buildings by at least 50 ft (15.2 m), and protected by an automatic fixed suppression system as required by the fire hazards analysis.	Comply - The AP1000 fire hazards analysis does not require fixed suppression in these areas.
8.28 Intake Structures. Intake structures shall be of noncombustible construction and shall be provided with automatic sprinkler protection.	COL
Chapter 9 Fire Protection for the Construction Site	N/A - Heading
9.1* General. Consideration of fire protection shall include safety to life and potential for delays in construction schedules and plant startup, as well as protection of property.	O/O
9.2 Administration.	N/A - Heading
9.2.1 The responsibility for fire protection for the entire site during the construction period shall be clearly defined. The administrative responsibilities shall be to develop, implement, and periodically update as necessary the measures outlined in this standard.	COL
9.2.2 The responsibility for fire protection programs among various organizations on-site shall be clearly delineated. The fire protection program to be followed and the owner's right to administration and enforcement shall be established.	O/O
9.2.3 The fire protection program shall include a fire risk evaluation of the construction site and construction activities.	COL
9.2.4 Written procedures shall be established for the new construction site, including major construction projects in existing plants. Such procedures shall be in accordance with Chapter 3.	COL
9.2.5* Security guard service, including recorded rounds, shall be provided through all areas of construction during times when construction activity is not in progress.	O/O
9.2.6 Construction schedules shall be coordinated so that the planned permanent fire protection systems are installed and placed in service as soon as possible.	COL

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
9.2.7 Construction and installation of fire barriers and fire doors shall be given priority in the construction schedule.	COL
9.3 Site Clearing and Construction Equipment.	N/A - Heading
9.3.1 Site Clearing.	N/A - Heading
9.3.1.1 Prior to clearing forest and brush-covered areas, the owner shall ensure that a written fire control plan is prepared and that fire-fighting tools and equipment are made available as required by NFPA 295, <i>Standard for Wildfire Control</i> . Contact shall be made with local fire and forest agencies for current data on restrictions and fire potential, and to arrange for necessary permits.	COL
9.3.1.2 All construction vehicles and engine-driven portable equipment shall be equipped with effective spark arresters. Vehicles equipped with catalytic converters shall be prohibited from wooded and heavily vegetated areas.	O/O
9.3.1.3 Fire tools and equipment shall be distinctly marked and used for fire emergencies only.	O/O
9.3.1.4 Each site utility vehicle shall be equipped with at least one fire-fighting tool, portable fire extinguisher, or backpack pump filled with 4 gal to 5 gal (15 L to 19 L) of water.	O/O
9.3.1.5 Cut trees, brush, and other combustible spoil shall be disposed of promptly.	O/O
9.3.1.6* Where it is necessary to dispose of combustible waste by on-site burning, designated burning areas shall be established with approval of the owner and shall be in compliance with federal, state, and local regulations and guidelines. The contractor shall coordinate burning with the agencies responsible for monitoring fire danger in the area and shall obtain all appropriate permits prior to the start of work.	O/O
9.4 Construction Warehouses, Shops, and Offices.	N/A - Heading
9.4.1 All structures that are to be retained as part of the completed plant shall be constructed of materials as indicated in Chapter 6 and in accordance with other applicable sections in this standard.	COL
9.4.2* Construction warehouses, offices, trailers, sheds, and other facilities for the storage of tools and materials shall be located with consideration of their exposure to major plant buildings or other important structures.	COL
9.4.3* A fire risk evaluation shall be performed.	COL

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
9.4.4 Warehouses that contain high-value equipment (as defined by the individual responsible for fire prevention and fire protection), or where the loss of or damage to contents would cause a delay in start-up dates of the completed plant, shall be arranged and protected as indicated below. Although some of these structures are considered to be temporary and will be removed upon completion of the plant, the fire and loss potential shall be thoroughly evaluated and protection provided where warranted.	O/O
9.4.4.1 Building construction materials shall be noncombustible or limited combustible.	O/O
9.4.4.2 Automatic sprinkler systems shall be designed and installed in accordance with NFPA 13, <i>Standard for the Installation of Sprinkler Systems</i> . Waterflow alarms shall be provided and located so as to be monitored at a constantly attended location as determined by the individual responsible for fire protection.	O/O
9.4.4.3* Air-supported structures shall only be used for the storage of noncombustibles.	O/O
9.4.5 Temporary enclosures, including trailers, inside permanent plant buildings shall be prohibited except where permitted by the individual responsible for fire prevention and fire protection. Where the floor area of a combustible enclosure exceeds 100 ft ² (9.29 m ²) or where the occupancy presents a fire exposure, the enclosure shall be protected with an approved automatic fire suppression system.	O/O
9.4.6 Storage of construction materials, equipment, or supplies that are either combustible or in combustible packaging shall be prohibited in main plant buildings unless either of the following conditions exist: (1) An approved automatic fire suppression system is in service in the storage area (2) Where loss of the materials or loss to the surrounding plant area would be minimal, as determined by the individual responsible for fire prevention and fire protection	O/O
9.4.7 Construction areas comprised of mobile buildings arranged with the buildings adjoining each other to form one large fire area shall be avoided. If buildings cannot be adequately separated, fire walls shall be installed between units or automatic sprinklers shall be provided throughout the buildings.	O/O
9.4.8 Fire alarms shall be connected to a constantly attended central location.	O/O
9.4.9 The handling, storage, and dispensing of flammable liquids and gases shall meet the requirements of NFPA 30, <i>Flammable and Combustible Liquids Code</i> ; NFPA 58, <i>Liquefied Petroleum Gas Code</i> ; and NFPA 395, <i>Standard for the Storage of Flammable and Combustible Liquids at Farms and Isolated Sites..</i>	O/O
9.4.10 Vehicle repair facilities shall meet the requirements of NFPA 88B, <i>Standard for Repair Garages</i> .	O/O

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
9.5 Construction Site Lay-Down Areas.	N/A - Heading
9.5.1 Fire hydrant systems with an adequate water supply shall be provided in lay-down areas where the need is determined by the individual responsible for fire prevention and fire protection.	O/O
9.5.2 Combustible materials shall be separated by a clear space to allow access for manual fire-fighting equipment. Access shall be provided and maintained to all fire-fighting equipment including fire hoses, extinguishers, and hydrants.	O/O
9.6 Temporary Construction Materials.	N/A - Heading
9.6.1* Noncombustible or fire-retardant scaffolds, formwork, decking, and partitions shall be used both inside and outside of permanent buildings where a fire could cause substantial damage or delay construction schedules.	O/O
9.6.2* The use of listed pressure-impregnated fire-retardant lumber or listed fire-retardant coatings shall be provided.	O/O
9.6.3 Tarpaulins (fabrics) and plastic films shall be certified to conform to the weather-resistant and fire-retardant materials described in NFPA 701, <i>Standard Methods of Fire Tests for Flame Propagation of Textiles and Films</i> .	O/O
9.6.4 Where it is necessary to store new nuclear fuel in areas other than the permanent storage facilities, a written procedure shall be developed to address separation from combustible materials, security, nuclear criticality, packing material, noncombustible or limited-combustible building materials, standpipe, portable fire extinguishers, and hydrant protection.	N/A
9.7 Water Supplies, Supply Mains, and Hydrants.	N/A - Heading
9.7.1* General. The permanent underground yard system, fire hydrants, and water supply (at least one water source), as indicated in Chapter 6, shall be installed during the early stages of construction. Where provision of all or part of the permanent underground system and water supply is not practical, temporary systems shall be provided. Temporary water supplies shall be hydrostatically tested, flushed, and arranged to maintain a high degree of reliability, including protection from freezing and loss of power.	O/O
9.7.2 Hydrants shall be installed, as indicated in Chapter 6, in the vicinity of main plant buildings, important warehouses, office or storage trailer complexes, and important outside structures with combustible construction or combustible concrete formwork (e.g., cooling towers). The underground main shall be arranged to minimize the possibility that any one break will remove from service any fixed water extinguishing system or leave any area without accessible hydrant protection.	O/O

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
<p>9.7.3 A fire protection water supply shall be provided on the construction site and shall be capable of furnishing the larger of the following for a minimum 2-hour duration:</p> <p>(1) 500 gpm (1892.5 L/min)</p> <p>(2) The inservice fixed water extinguishing system with the highest water demand and 500 gpm (1892.5 L/min) for hose streams</p>	O/O
<p>9.7.3.1 The highest water demand shall be determined by the hazards present at the stage of construction, which might not correspond with the highest water demand of the completed plant.</p>	O/O
<p>9.7.3.2* As fixed water extinguishing systems are completed, they shall be placed in service, even when the available construction phase fire protection water supply is not adequate to meet the designed system demand. However, when the permanent hazard is introduced, the water supply shall be capable of providing the designed system demand. Where using construction water in permanent systems, adequate strainers shall be provided to prevent clogging of the system by foreign objects and dirt.</p>	O/O
<p>9.7.3.3 The water supply shall be sufficient to provide adequate pressure for hose connections at the highest elevation.</p>	O/O
<p>9.8 Manual Fire-Fighting Equipment.</p>	N/A - Heading
<p>9.8.1* Fire-fighting equipment shall be provided in accordance with NFPA 600, <i>Standard on Industrial Fire Brigades</i>, and NFPA 241, <i>Standard for Safeguarding Construction, Alteration, and Demolition Operations</i>.</p>	O/O
<p>9.8.2 Portable fire extinguishers of suitable capacity shall be provided in accordance with NFPA 10, <i>Standard for Portable Fire Extinguishers</i>, where one or more of the following occurs:</p> <p>(1) Flammable liquids are stored or handled.</p> <p>(2) Combustible materials are stored.</p> <p>(3) Temporary oil- or gas-fired equipment is used.</p> <p>(4) A tar or asphalt kettle is used.</p> <p>(5) Welding or open flames are in use.</p>	O/O
<p>9.8.3* A standpipe system shall be provided in any permanent building that has two-floor equivalent wall heights erected. Additional standpipe hose connections shall be added to each floor level as soon as sufficient landings are available to fight fires from that level. Protection from freezing shall be provided.</p>	O/O

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
9.8.4 Hoses and nozzles shall be available at strategic locations, such as inside hose cabinets or hose houses or on dedicated fire response vehicles.	O/O
9.8.5 If fire hose connections are not compatible with local fire-fighting equipment, adapters shall be made available.	O/O
Chapter 10 Referenced Publications	N/A - Heading
10.1 The following documents or portions thereof are referenced within this standard as mandatory requirements and shall be considered part of the requirements of this standard. The edition indicated for each referenced mandatory document is the current edition as of the date of the NFPA issuance of this standard. Some of these mandatory documents might also be referenced in this standard for specific informational purposes and, therefore, are also listed in Appendix B.	AP1000 compliance to this paragraph is addressed in the given paragraphs above.
<p>10.1.1 NFPA Publications. National Fire Protection Association, 1 Batterymarch Park, P.O. Box 9101, Quincy, MA 02269- 9101.</p> <p>NFPA 10, <i>Standard for Portable Fire Extinguishers</i>, 1998 edition.</p> <p>NFPA 11, <i>Standard for Low-Expansion Foam</i>, 1998 edition.</p> <p>NFPA 11A, <i>Standard for Medium- and High-Expansion Foam Systems</i>, 1999 edition.</p> <p>NFPA 12, <i>Standard on Carbon Dioxide Extinguishing Systems</i>, 2000 edition.</p> <p>NFPA 13, <i>Standard for the Installation of Sprinkler Systems</i>, 1999 edition.</p> <p>NFPA 14, <i>Standard for the Installation of Standpipe, Private Hydrant, and Hose Systems</i>, 2000 edition..</p> <p>NFPA 15, <i>Standard for Water Spray Fixed Systems for Fire Protection</i>, 1996 edition.</p> <p>NFPA 16, <i>Standard for the Installation of Foam-Water Sprinkler and Foam-Water Spray Systems</i>, 1999 edition.</p> <p>NFPA 17, <i>Standard for Dry Chemical Extinguishing Systems</i>, 1998 edition.</p> <p>NFPA 20, <i>Standard for the Installation of Stationary Pumps for Fire Protection</i>, 1999 edition.</p> <p>NFPA 22, <i>Standard for Water Tanks for Private Fire Protection</i>, 1998 edition.</p>	N/A - General

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
<p>NFPA 24, <i>Standard for the Installation of Private Fire Service Mains and Their Appurtenances</i>, 1995 edition.</p> <p>NFPA 30, <i>Flammable and Combustible Liquids Code</i>, 2000 edition.</p> <p>NFPA 31, <i>Standard for the Installation of Oil-Burning Equipment</i>, 2001 edition.</p> <p>NFPA 37, <i>Standard for the Installation and Use of Stationary Combustion Engines and Gas Turbines</i>, 1998 edition.</p> <p>NFPA 50A, <i>Standard for Gaseous Hydrogen Systems at Consumer Sites</i>, 1999 edition.</p> <p>NFPA 50B, <i>Standard for Liquefied Hydrogen Systems at Consumer Sites</i>, 1999 edition.</p> <p>NFPA 51B, <i>Standard for Fire Prevention During Welding, Cutting, and Other Hot Work</i>, 1999 edition.</p> <p>NFPA 54, <i>National Fuel Gas Code</i>, 1999 edition.</p> <p>NFPA 58, <i>Liquefied Petroleum Gas Code</i>, 2001 edition.</p> <p>NFPA 70, <i>National Electrical Code</i> ® , 1999 edition.</p> <p>NFPA 72, <i>National Fire Alarm Code</i> ® , 1999 edition.</p> <p>NFPA 75, <i>Standard for the Protection of Electronic Computer/ Data Processing Equipment</i>, 1999 edition.</p> <p>NFPA 80, <i>Standard for Fire Doors and Fire Windows</i>, 1999 edition.</p> <p>NFPA 85, <i>Boiler and Combustion Systems Hazards Code</i>, 2001 edition.</p> <p>NFPA 88B, <i>Standard for Repair Garages</i>, 1997 edition.</p> <p>NFPA 90A, <i>Standard for the Installation of Air-Conditioning and Ventilating Systems</i>, 1999 edition.</p> <p>NFPA 101 ® , <i>Life Safety Code</i> ® , 2000 edition.</p> <p>NFPA 211, <i>Standard for Chimneys, Fireplaces, Vents, and Solid Fuel-Burning Appliances</i>, 2000 edition.</p> <p>NFPA 214, <i>Standard on Water-Cooling Towers</i>, 2000 edition.</p> <p>NFPA 220, <i>Standard on Types of Building Construction</i>, 1999 edition.</p> <p>NFPA 232, <i>Standard for the Protection of Records</i>, 2000 edition.</p> <p>NFPA 241, <i>Standard for Safeguarding Construction, Alteration, and Demolition Operations</i>, 2000 edition.</p>	

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
<p>NFPA 251, <i>Standard Methods of Tests of Fire Endurance of Building Construction and Materials</i>, 1999 edition.</p> <p>NFPA 252, <i>Standard Methods of Fire Tests of Door Assemblies</i>, 1999 edition.</p> <p>NFPA 253, <i>Standard Method of Test for Critical Radiant Flux of Floor Covering Systems Using a Radiant Heat Energy Source</i>, 2000 edition.</p> <p>NFPA 255, <i>Standard Method of Test of Surface Burning Characteristics of Building Materials</i>, 2000 edition.</p> <p>NFPA 256, <i>Standard Methods of Fire Tests of Roof Coverings</i>, 1998 edition.</p> <p>NFPA 259, <i>Standard Test Method for Potential Heat of Building Materials</i>, 1998 edition.</p> <p>NFPA 295, <i>Standard for Wildfire Control</i>, 1998 edition.</p> <p>NFPA 395, <i>Standard for the Storage of Flammable and Combustible Liquids at Farms and Isolated Sites</i>, 1993 edition.</p> <p>NFPA 600, <i>Standard on Industrial Fire Brigades</i>, 2000 edition.</p> <p>NFPA 601, <i>Standard for Security Services in Fire Loss Prevention</i>, 2000 edition.</p> <p>NFPA 701, <i>Standard Methods of Fire Tests for Flame Propagation of Textiles and Films</i>, 1999 edition.</p> <p>NFPA 780, <i>Standard for the Installation of Lightning Protection Systems</i>, 1997 edition.</p> <p>NFPA 1500, <i>Standard on Fire Department Occupational Safety and Health Program</i>, 1997 edition.</p> <p>NFPA 2001, <i>Standard on Clean Agent Fire Extinguishing Systems</i>, 2000 edition.</p>	
10.1.2 Other Publications.	N/A - Heading
10.1.2.1 ANSI Publications. American National Standards Institute, Inc., 11 West 42nd Street 13th floor, New York, NY 10036. ANSI B31.1, <i>Code for Power Piping</i> , 1992 edition. ANSI C2, <i>National Electrical Safety Code</i> , 1993 edition.	N/A - General
10.1.2.2 ASME Publications. American Society of Mechanical Engineers, Three Park Avenue, New York, NY 10016-5990. ASME <i>Boiler and Pressure Vessel Code</i> , Section III, 1992 edition. ASME NQA-1, <i>Quality Assurance Program Requirements for Nuclear Facilities</i> , 1994 edition.	N/A - General

NFPA 804 PARAGRAPH	AP1000 COMPLIANCE STATEMENT
<p>10.1.2.3 ASTM Publications. American Society for Testing and Materials, 100 Barr Harbor Drive, West Conshohocken, PA 19428-2959. ASTM D 92, <i>Standard Test Method for Flash and Fire Points by Cleveland Open Cup</i>, 1990 edition. ASTM E 84, <i>Standard Test Method for Surface Burning Characteristics of Building Materials</i>, 1994 edition. ASTM E 119, <i>Standard Test Methods for Fire Tests of Building Construction and Materials</i>, 1988 edition. ASTM E 136, <i>Standard Test Method for Behavior of Materials in a Vertical Tube Furnace at 750</i>, 1994 edition. ASTM E 814, <i>Fire Tests of Through-Penetration Fire Stops</i>, 1994 edition.</p>	N/A - General
<p>10.1.2.4 IEEE Publication. Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331. IEEE 383-1974 (R-1992) <i>Standard for Type Test of Class IE Electric Cables, Field Splices and Connections for Nuclear Power Generating Stations</i>.</p>	N/A - General
<p>10.1.2.5 UL Publications. Underwriters Laboratories Inc., 333 Pfingsten Road, Northbrook, IL 60062. UL 586, <i>Standard for Test Performance of High-Efficiency Particulate Air Filter Units</i>, 1990 edition. UL 1479, <i>Standard for Safety Fire Tests of Through-Penetration Firestops</i>, 1994 edition.</p>	N/A - General
<p>10.1.2.6 U.S. Government Publications. U.S. Government Printing Office, Ishington, DC 20402. NRC Generic Letter 86-10, Supplement 1. Title 10, <i>Code of Federal Regulations</i>, Part 100, "Reactor Site Criteria."</p>	N/A - General

This page was added to the quality record by the PRIME system upon its validation and shall not be considered in the page numbering of this document.

Approval Information

Author Approval Corletti Michael Sep-02-2020 14:18:53

Files approved on Sep-02-2020

*** This record was final approved on 9/2/2020 2:18:53 PM. (This statement was added by the PRIME system upon its validation)

Southern Nuclear Operating Company

ND-21-0486

Enclosure 11

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

WCAP-15927-NP, "Design Process for AP1000 Common Q Safety Systems," Revision 8

[Non-proprietary version of WCAP-15927-P, Revision 8]

(Enclosure 11 consists of 33 pages, plus this cover page)

WESTINGHOUSE NON-PROPRIETARY CLASS 3

WCAP-15927-NP

**Design Process for AP1000
Common Q Safety Systems**

Matthew A. Shakun*
Licensing Engineering

August 2020

Verifier: Christopher S. Phillips*, Principal Engineer
Standard Hardware and Common Q Platform

Reviewer: Kasey Corbin*, Principal Engineer
APR1400 Software Engineering

Reviewer: Richard M. Paese*, Fellow Licensing Engineer
Licensing Engineering

Reviewer: Scott A. Faber*, Project Manager
AP1000 PMS

Approved: Zachary S. Harper*, Manager
Licensing Engineering

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

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

© 2020 Westinghouse Electric Company LLC
All Rights Reserved

TABLE OF CONTENTS

LIST OF TABLES iii

LIST OF FIGURES iii

REVISION HISTORY iv

REVISION HISTORY (cont.)..... v

1 INTRODUCTION AND SCOPE 1-1

2 DEFINITIONS..... 2-1

 2.1 ACRONYMS..... 2-1

 2.2 TERMS 2-2

3 AP1000-SPECIFIC APPLICATION DEVELOPMENT 3-1

 3.1 CONCEPTUAL PHASE..... 3-2

 3.2 SYSTEM DEFINITION PHASE 3-2

 3.2.1 Platform Requirement Analysis..... 3-2

 3.2.2 System Requirements Analysis/Functional Design 3-3

 3.2.3 System Architectural Design 3-5

 3.2.4 Software Requirements Analysis..... 3-6

 3.2.5 System Hardware Requirements 3-8

 3.3 SOFTWARE DESIGN PHASE 3-8

 3.4 HARDWARE DESIGN PHASE..... 3-9

 3.5 SOFTWARE IMPLEMENTATION PHASE..... 3-10

 3.5.1 Final RSED..... 3-10

 3.5.2 Final Software Definition Document 3-10

 3.6 HARDWARE IMPLEMENTATION (ASSEMBLY) PHASE..... 3-11

 3.7 SYSTEM INTEGRATION PHASE 3-11

 3.8 INSTALLATION PHASE 3-11

 3.9 ALTERNATIVE METHODS TO PROCESSES DEFINED IN WCAP-16096-P-A 3-11

 3.10 ALTERNATIVES TO PROCESSES AND DESCRIPTIONS IN WCAP-16097-P-A .. 3-11

4 REFERENCES 4-1

 4.1 INDUSTRY STANDARDS AND CODES 4-1

 4.2 WESTINGHOUSE DOCUMENTS 4-1

LIST OF TABLES

Table 3-1 Alternative Methods to the Common Q SPM.....3-12

Table 3-2 Alternative Methods to the Common Q Topical Report3-17

LIST OF FIGURES

Figure 3-1 Development Process.....3-23

Figure 3-2 Correlation to Standard Life Cycle Phase.....3-24

REVISION HISTORY**RECORD OF CHANGES**

Revision	Author	Description	Completed
0	Thomas M. Hayes	Original issue.	9/18/02
1	Steven W. Gore	<p>Class 3 DCP changes as detailed below:</p> <p>Added further definition of the Concept Phase (Section 1).</p> <p>Added additional description of life cycle (Section 1).</p> <p>Removed descriptions also in Common Q NRC docketed reports (Section 1).</p> <p>Added missing acronyms and terms (Section 2).</p> <p>Merged the application and platform design life cycle descriptions into one section to eliminate redundant descriptions common to both (Section 3 and throughout document).</p> <p>Added clarification that critical anomalies had to be completed for each phase (Section 3).</p> <p>Added Functional Design to System Requirements (Section 3.2).</p> <p>Project Master Documents now referred to as Document Index (Section 3.1).</p> <p>Updated Figure 3-1, "Development Process," with additional V&V methods.</p> <p>Updated reference document numbers (throughout document and Section 4).</p> <p>Removed explanation of Platform System Design Phase because it is not applicable to AP1000 PMS since it describes generic architecture (Section 4 of Rev. 0).</p>	11/21/08
2	Warren R. Odess-Gillett	Changes are Class 3 as per NSNP 3.4.1. Updated Figure 3-1 per RAI response RAI-SRP 7.1-ICE-10, reference the SPM for the operation, maintenance and retirement software life cycle phases, and technical editing changes	6/3/09
3	Warren R. Odess-Gillett	<p>Updated to reference the newly NRC-approved Common Q™ Topical Report (WCAP-16097-P-A, Rev. 3).</p> <p>Updated to reference the newly NRC-approved Software Program Manual for Common Q Systems (WCAP-16096-P-A, Rev. 4).</p> <p>Updated Section 3.1 to remove the term Document Index.</p>	4/10/13
4	Matthew A. Shakun	<p>The following change was made to address APP-GW-GEE-4380 and CAPAL 100320452:</p> <ul style="list-style-type: none"> Updated to include alternate processes to WCAP-16096-P-A, Rev. 4, "Software Program Manual for Common Q™ Systems" and WCAP-16097-P-A, Rev. 3, "Common Qualified Platform Topical Report" 	9/22/15

REVISION HISTORY (cont.)**RECORD OF CHANGES (cont.)**

Revision	Author	Description	Completed
4 (cont.)	Matthew A. Shakun	The following editorial changes were made: <ul style="list-style-type: none"> Section 2.1 was updated to fix the acronym for AMPL Sections 3 and 4 were updated to fix the title for IEEE Std. 1074-1995. Reference 4.2.3 was deleted since it is not being cited in the document. 	9/22/15
5	Matthew A. Shakun	The following changes were made to address APP-GW-GEE-4380 and CAPAL 100405203: <ul style="list-style-type: none"> Updated SPM alternative methods in Table 3-1 per APP-GW-GF-115, Rev. 0. 	9/8/16
6	Matthew A. Shakun	The following changes were made to address APP-GW-GEE-4380 and CAPAL 100444282: <ul style="list-style-type: none"> Updated SPM alternative methods in Table 3-1 to remove alternative related to site test planning. 	2/17/17
7	Matthew A. Shakun	The following changes were made to address APP-FSAR-GEF-045: <ul style="list-style-type: none"> Updated Table 3-2 to add alternative design descriptions to the Common Q Topical Report 	10/30/18
8	Matthew A. Shakun	The following changes were made to address APP-FSAR-GEF-169: <ul style="list-style-type: none"> Updated Table 3-2 to add alternative design descriptions to the Common Q Topical Report 	See PRIME

1 INTRODUCTION AND SCOPE

This document defines the process for system-level design, software design and implementation, and hardware design and implementation for the AP1000[®] protection and safety monitoring system development. This document supplements WCAP-16096-P-A, “Software Program Manual for Common Q[™] Systems” (Reference 4.2.1). Project definition activities are described in this document as a Conceptual Phase (see Section 3.1). The Conceptual Phase is a preparatory phase before the system design begins; it is described here because it forms the management and technical baseline for the development activities.

The objective of the development process is the production of a high quality instrumentation and control (I&C) system that is to be used for the AP1000 protection and safety monitoring system. The design of the system is derived from functional and other requirements applicable to AP1000 (in addition to general requirements that may apply to all similar applications).

The functional requirements of the software are, for the most part, a direct derivation of the system functional requirements. The end product of application development is an operating I&C system, so the life cycle extends through the retirement phase (the operation, maintenance and retirement phases are sufficiently covered in Reference 4.2.1).

The Common Q[™] platform consists primarily of the Asea Brown Boveri, Inc. (ABB) Advant[®] Controller 160 (AC160) hardware and software product line, including the Advant development tools. The development of the AC160 hardware and software and Advant tools is outside the scope of this document. The AC160 product line is developed commercially, and is qualified for use in Common Q applications by a process of commercial dedication. The commercial dedication process is defined in WCAP-16097-P-A, “Common Qualified Platform Topical Report” (Reference 4.2.2). The Common Q platform also has certain generic hardware and software modules that are developed by Westinghouse specifically for safety system applications and that are reusable for multiple systems of various types. The development of these reusable, generic modules is integrated into the life cycle process as described in this document.

2 DEFINITIONS

2.1 ACRONYMS

ABB	Asea Brown Boveri, Inc.
AC160	Part of the ABB Advant open control system family product line
AF100	Advant Fieldbus 100
AMPL	ABB Master Programming Language
CHT	Cabinet Hardware Test
CIT	Channel Integration Test
DCD	Design Control Document
DI	Document Index
EMC	Electromagnetic Compatibility
EST	Element Software Test
HSI	Human System Interface
HSL	High Speed Datalink
I&C	Instrumentation and Control
I/O	Input/Output
PMST	Processor Module Software Test
RSED	Reusable Software Element Document
RTA	Requirements Traceability Analysis
RTM	Requirements Traceability Matrix
SAT	Site Acceptance Testing
SDD	Software Design Description
SDS	System Design Specification
SIT	System Integration Test
SRS	Software Requirements Specification
SSD	System Specification Document
V&V	Verification and Validation

Advant is a trademark or registered trademark of its respective owner. Other names may be trademarks of their respective owners.

AP1000 and Common Q are trademarks or registered trademarks of Westinghouse Electric Company LLC, its affiliates and/or its subsidiaries in the United States of America and may be registered in other countries throughout the world. All rights reserved. Unauthorized use is strictly prohibited. Other names may be trademarks of their respective owners.

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

2.2 TERMS

Advant	An ABB open control system family product line.
Common Q	Common Qualified Platform – a safety system I&C platform as defined in WCAP-16097-P-A, “Common Qualified Platform Topical Report” (Reference 4.2.2).
Data Highway	A serial digital communications circuit that provides communications among several devices.
Datalink	A hardware link used for unidirectional or bi-directional communications between two process modules.
V&V	Verification and validation performed by an organization that is technically, managerially, and financially independent of the development organization.

3 AP1000-SPECIFIC APPLICATION DEVELOPMENT

This section defines the process that is followed in the design of the AP1000 protection and safety monitoring system and in the design and implementation of application hardware and software that are applied to AP1000. The general relationship of hardware, software, and system verification and validation (V&V) (including testing) to this development process is shown, but the details are defined by the V&V Plan.

The following phases occur in the development of the AP1000 protection and safety monitoring hardware and software:

1. Conceptual (Project Definition)
2. System Definition
3. Software Design
4. Hardware Design
5. Software Implementation
6. Hardware Implementation
7. System Integration
8. Installation

Note that testing activities are defined as part of the V&V process.

Figure 3-1 illustrates the relationship of the application development phases to each other and to the V&V process. It also shows the outputs of each phase. The activities and products of these phases are described in the remainder of Section 3. The flow of activities shown in Figure 3-1 is intended to expand on the classic “waterfall” lifecycle model. These activities may be both iterative and overlapping. In particular, because of the constraints of I&C projects, and considering the distributed character of the AP1000 I&C systems, work may commence on a given development phase before preceding phases are complete. For example, it is not necessary for the documentation of system functional requirements to be finished before software design and implementation can start on parts of the system for which the requirements have been defined. However, for a given development phase, all critical anomalies related to that phase must be resolved before the completion of that phase.

Figure 3-2 illustrates the relationship of the development phases defined in this document to the phases (or processes) defined in other documents, specifically IEEE Standard 1074-1995, “IEEE Standard for Developing Software Life Cycle Processes” (Reference 4.1.1); IEEE/EIA 12207.0-1996, “Industry Implementation of International Standard ISO/IEC 12207: 1995 (ISO/IEC 12207) Standard for Information Technology-Software Life Cycle Processes” (Reference 4.1.2); and WCAP-16096-P-A, “Software Program Manual for Common Q™ Systems” (Reference 4.2.1).

3.1 CONCEPTUAL PHASE

The major tasks of the Conceptual, or Project Definition, Phase are project management planning and project baselining.

The project execution strategy is established and documented. Resources, personnel, and organizational interfaces and dependencies are identified. Planning for schedule, costs, risk management, communication, and project closure is performed. Requisite processes are identified, and may include acquisition, supply, development, operation, and maintenance, and the supporting processes of configuration management, quality assurance, safety, verification, validation, and problem resolution.

The technical baseline is established and documented. Project baseline information typically includes:

- Definition of the scope of the development
- AP1000 Design Control Document (DCD)
- System Specification Documents (SSDs)
- Safety classification of all parts of the system included in the scope of development
- Plant documentation and databases
- Plant-wide I&C requirements
- Applicability of codes and standards, including decomposition of key codes and standards to specific requirements

3.2 SYSTEM DEFINITION PHASE

There are three main tasks in the system definition phase—system requirements analysis, system architectural design, and software requirements analysis. These three tasks overlap in their execution, and there may be considerable iteration among them. The output of this phase is a System Requirements/Functional Design document, a System Design Specification (SDS), and a Software Requirements Specification (SRS).

3.2.1 Platform Requirement Analysis

The Common Q platform is analyzed against the requirements for the AP1000 protection and safety monitoring system. Any modifications or additions to the Common Q platform are identified. These modifications or additions become first-time engineering projects that follow the same design process as described herein.

3.2.2 System Requirements Analysis/Functional Design

In this task, the project technical baseline (Section 3.1) is analyzed to specify the system requirements. This task produces the System Requirements document. Information in the System Requirements document includes system design requirements, system functional requirements (including function-related setpoints, and constants), system interface requirements, and human system interface (HSI) requirements. Detailed requirements for the interface of individual external signals and communications data are documented in an external signal database and an external communications database.

3.2.2.1 System Design Requirements

The system design requirements comprise the overall requirements and constraints for the system design, aside from the specific system functions and specific interface signals. The application System Requirements document incorporates, by reference, the platform system design requirements and identifies additions and/or exceptions that apply specifically to AP1000. The system design requirements include the following categories of requirements:

- Applicability of codes and standards, either in whole, or in part, or as guidance (which may be defined by reference to the applicability documented in the technical baseline)
- General design requirements: design basis, single failure criteria, integrity, independence, maintenance, manual capabilities, information display, access control, identification, calibration capabilities, reliability, and availability
- Hardware qualification: environmental, electromagnetic compatibility (EMC), and seismic
- Power and grounding
- External interface capabilities
- Performance requirements: time response, accuracy, and signal noise
- Test and diagnostic capabilities
- Design constraints and objectives

3.2.2.2 System Functional Requirements

The system functional requirements provide a complete definition of the sense and command features within the scope of the system (including non-safety functions, such as provision of data to the plant information system, control interlocks, information displays, etc.). They include the following categories of requirements. The requirements are provided by a combination of textual description, logic diagrams, mathematical formulas, and tables.

- Safety functions and corresponding protective actions (exact definition of the required response of the system for all design basis events)

- Non-safety-related functions (e.g., control interlocks, data to non-safety displays and systems)
- Performance requirements associated with functions (time response, accuracy)
- Setpoints and constants associated with functions (fixed value or range of adjustment, hysteresis)
- Response to failures and out-of-range conditions (internal and external)
- Functional diversity
- Signal diversity
- Separation and isolation requirements for individual functions or interfaces (e.g., assignment of signals and functions to separation divisions)
- Required auxiliary features, such as:
 - Maintenance bypass and trip logic
 - Automatic, manual, and/or continuous test capabilities
 - Maintenance functions

3.2.2.3 System Interface Requirements

The system interface requirements define the interface between the protection system being specified and the rest of the physical plant. The requirements include the following categories:

- System scope (defines what is included in the scope of supply)
- System boundaries:
 - Mechanical system (the plant process; generally, however, the actual boundary between the process and the protection system is the I&C boundary)
 - Electrical system (power and grounding)
 - I&C systems (a general description of the signal interfaces—detailed definition of all external signals is recorded in the external interface database)
 - Functional interfaces (description of the external systems with which the protection system interfaces, and identification of the parameters, controls, indications, and functions that are monitored or actuated)
- Requirements for associated equipment (e.g., time response of actuated equipment)
- Isolation requirements for external interfaces (e.g., individual requirements for Class 1E)

3.2.2.4 HSI Requirements

The HSI requirements identify all of the required operator and maintenance personnel interfaces; for example, displays, alarms, operator controls, and maintenance and test interfaces, including the associated functionality.

3.2.2.5 External Interface Database

The external interface database supplements the System Requirements document and contains two categories of information: external signal information and external communications information.

The database identifies each external physical signal received by or produced by the system. When the database is initially populated, it provides a unique identifier by which each signal can be referenced, and it defines the signal type, signal range, functional description, source or destination (by external system), and external identifier (e.g., tag number) of the signal. As the system design progresses, information is added to each signal to identify where the signal originates and terminates within the protection system, by cabinet, then, ultimately, by specific termination, including terminal identities and identity of the input/output (I/O) or communication module and point that provide the controller interface to each signal.

The database identifies each data item that the protection system receives or transmits via a data channel (datalink or data highway). The database identifies the data channel and defines, where applicable, the data type, range, functional description, update timing, and grouping with other data items. This database provides a unique identifier by which the data item can be referenced.

3.2.3 System Architectural Design

The system architectural design task identifies the major hardware and software elements of the system and their interconnections. This task produces the SDS requirements that are allocated among these items. In particular, the functional, HSI, and interface requirements are mapped to individual subsystems. System hardware requirements are identified. External signals are allocated to individual subsystems, and this information is added to the external interface database, as noted in subsection 3.2.2.5. Intrasystem signals and communications data are identified; details may be documented in an intrasystem interface database.

3.2.3.1 System Architecture

A description is given of the architecture of the protection system as a whole. Information provided includes the following, and typically will include architecture diagrams, hardware configuration diagrams, and textual descriptions of the architectural elements:

- Identification of all parts of the system, to the cabinet and subsystem level
- Interconnections among subsystems
- Assignment of power and grounding interfaces to specific cabinets or subsystems

- Definition of subsystem hardware configuration to a level of detail necessary to support software design and to identify any hardware or software that must be designed or procured (i.e., that is not part of the standard platform hardware and software)
- Evaluation of the selected architecture against the product qualification of the standard platform hardware and software

3.2.3.2 Functional Mapping

The system functions and performance requirements defined in the System Requirements document are assigned to individual subsystems. For most sense and command features (both safety and non-safety) this can be documented as a list or table of the functions that are defined in the system functional requirements (see subsection 3.2.2.2) with the subsystem assignment. If functions must be allocated to a particular processor within a subsystem because of separation requirements defined in the system functional requirements, that assignment is documented here as well. Auxiliary features, such as testing capabilities, are mapped to the architecture at a high level here.

3.2.3.3 Intrasystem Interface Database

The intrasystem interface database contains two categories of information: intrasystem signal information and intrasystem communications information.

This database identifies each physical signal that is connected between different subsystems within the protection system. The intrasystem interface database defines the signal type, signal range, functional description, and the source and destination(s) (by subsystem) and provides a unique identifier by which the signal can be referenced. Ultimately, this database also includes specific termination information, including terminal identities and identity of the I/O or communication module and point that provide the controller interface to each signal. The termination information, however, does not necessarily need to be included before hardware and software design can proceed.

The Intrasystem Interface Database also identifies each data item that the protection system receives or transmits via an intrasystem data channel (datalink or data highway). It identifies the data channel and defines, where applicable, the data type, range, functional description, update timing, and grouping with other data items. It provides a unique identifier by which the data item can be referenced.

3.2.4 Software Requirements Analysis

The software requirements analysis task completes the identification of the requirements for the software in the system. The outputs of this task are several reusable software element documents (RSEDs) and an SRS for the system-specific software. The requirements for the sense and command features typically will have been documented by the functional mapping documented in the SDS (see subsection 3.2.2.2). Any additional requirements will be identified in the SRS as defined in subsection 3.2.3.2.

3.2.4.1 Reusable Software Element Document (Summary and Requirements)

Reusable common software elements can be created for the AC160 product line in the form of type circuits and custom PC elements. A type circuit is a prearranged group of the smaller pre-existing commercially available software units (PC elements) into a larger, more complex software entity. Type circuits are not compiled code, but more like the ABB Master Programming Language (AMPL) macro definitions that can be saved individually and reused throughout one or more projects. Custom PC elements are compiled from source code and added to the library of standard PC elements available for AMPL programming. Common software elements that are type circuits or general purpose custom PC elements (new PC elements intended for common use in many different safety applications) are documented with a composite document referred to as an RSED. An RSED combines requirements, design description, and user information into a single document.

The portion of an RSED that contains the product of the software requirements analysis contains the following categories of information:

- An element (type circuit, functional unit, custom PC element) summary consisting of a general functional description of the element
- Requirements Specification:
 - Functional requirements (functions implemented, timing, accuracy)
 - I/O terminal descriptions (default values, data types, data ranges)
 - Overflow/error handling (range checking, failure modes, alarming)
 - Truth Table (outputs as a function of input combinations)

3.2.4.2 Software Requirements Specification

The high-level requirements for auxiliary features are refined into detailed requirements in the SRS. The SRS ensures that all requirements are documented for the software in each subsystem. This information may be in the System Requirements as they are mapped to subsystems and processors by the SDS (including information in the signal and communications databases). Additional information is documented as detailed requirements in the SRS. Information in the software requirements analysis includes:

- Software structure
- Software technical description
- Specific inputs and outputs, both those that are physical signals and information that is received from and supplied to human users and external data systems
- Valid input ranges
- Output ranges, if they must be specifically limited

- Required HSI formats (e.g., input screen formats, printed report formats)
- Required sequences of operations (e.g., test sequences, operator dialog sequences)
- Functional processing of the data
- Timing requirements or constraints
- Response to abnormal conditions and error recovery
- Retention, use, and initialization of previous state information, where required
- Safety and security requirements
- Design constraints (e.g., the required use of a particular programming tool or language, or the required use of particular platform software)

3.2.5 System Hardware Requirements

The system hardware requirements describe the hardware requirements needed to support the architecture of the protection system. Information provided includes the following:

- Identification of all the hardware elements used in the system, such as cabinets, panels, subassemblies, wiring, terminations and modules
- Definition of the hardware configuration needed to support the architecture of the protection system
- Cabinet power and grounding requirements
- Cabinet cooling requirements
- Cabinet labeling requirements
- Cabinet environmental requirements
- Cabinet shipping and storage requirements

3.3 SOFTWARE DESIGN PHASE

In the software design phase, the software requirements are decomposed and allocated to individual software components. The use of existing software components to implement the requirements is described within an existing RSED. New software components that must be created are identified and likewise documented within an RSED. The portion of an RSED that contains the product of the Software Design Phase contains any design information that is not obvious from the implementation (AMPL diagram or code comments).

The software design is described in Software Design Description (SDD) documents. A preliminary SDD is produced in the software design phase, while a final SDD is produced in the software implementation phase. There is an SDD generated for each processor module that executes unique code. Redundant processors that execute identical, or nearly identical, code may have a single SDD; this includes processors in separate divisions, if they have essentially identical code (implement the same functions).

The preliminary SDD contains the following categories of information:

- Decomposition of the required functions into software entities (modules, procedures, type circuits, etc.), including entity names and the reason for the existence of the entity
- Module timing and priority
- A description, where applicable, of how safety (sense and command) functions and auxiliary functions are combined (e.g., the functionality required in bistable and logic processors to implement periodic testing; local functionality required to support maintenance functions, such as calibration data changes). In typical cases, this description may be made generic and included in the “Design Constraints” section of the application SRS, or even in platform (non-project-specific) documentation; a reference to such generic information should be made where applicable.
- Identification of any generic type circuits or custom PC elements that need to be developed. These may be project-universal elements, applicable in multiple processors in a specific project, or they may be new platform software. In either case, their design and implementation follows the platform software development process.
- Where applicable, handling of software initialization, redundancy, and tracking

3.4 HARDWARE DESIGN PHASE

In the hardware design phase, the final construction configuration of the production hardware is specified. The production unit specific cabinet assembly drawings and cabinet configuration drawings are issued at this stage. These drawings contain all of the information necessary to produce the production unit hardware. The drawings include the following information:

- Cabinet layout details
- Cabinet assembly details
- Cabinet bill of materials
- Cabinet configuration details
- Cabinet termination frame details
- Cabinet internal wiring details

3.5 SOFTWARE IMPLEMENTATION PHASE

In the software implementation phase, the executable code modules are created, typically by use of the AMPL tools. (Non-AC160 subsystems require different tools.) The application modules are integrated with platform software to produce code modules that are downloaded into subsystem processors for V&V testing (described in a V&V plan). The final version of the RSED for all of the defined software components is an output of this phase. Descriptive information about the implementation is added to the preliminary SDD to produce the final SDD.

3.5.1 Final RSED

The implementation description (a printout of the AMPL diagram) is added to the RSED and a User's Guide section is added (providing the developer with adequate instruction to incorporate the common element into an application program). The complete RSED then contains the following information:

- The element summary
- The requirements specification
- Design information (as described in Section 3.3)
- Implementation (printout of AMPL diagram for the type circuits)
- Users Guide:
 - Detailed instantiation procedure (prerequisites, applicability, restrictions, signal connections)
 - Configuration/applications (database elements connections, I/O interfaces, high speed datalink [HSL] interfaces, Advant Fieldbus 100 (AF100) interfaces, default values used)

3.5.2 Final Software Definition Document

The following categories of information are added to produce the final SDD:

- Mapping of signal names used in the code to names used in the requirements documents and databases, where these differ
- Printouts of the AMPL function chart diagrams
- Any other non-obvious information that is needed to understand the software implementation and its interfaces. The intention is that this is an aid to the individuals who will verify or maintain the code. This should not repeat information that is clear to a knowledgeable individual reading the diagrams (or non-AMPL source code listings).

3.6 HARDWARE IMPLEMENTATION (ASSEMBLY) PHASE

In this phase, the construction of the production unit hardware system is completed using the drawings specified in Section 3.4.

3.7 SYSTEM INTEGRATION PHASE

In this phase, completed cabinets containing the applications software are connected together as an integrated system. Validation testing (described in the V&V plan) is performed to test system functionality that was not covered by the cabinet-level validation testing. System integration and testing may be done on appropriate portions (e.g., individual divisions) of the system or on the complete system.

3.8 INSTALLATION PHASE

The completed system is installed at the site. Site Acceptance Testing (SAT), described in the V&V plan, is performed to assure that the system has not been damaged by shipping and installation. The SAT also confirms proper operation of any interfaces that were not completely tested by the factory validation testing; e.g., interfaces to other plant systems.

3.9 ALTERNATIVE METHODS TO PROCESSES DEFINED IN WCAP-16096-P-A

Table 3-1 identifies alternatives to the processes defined in WCAP-16096-P-A, “Software Program Manual for Common Q Systems” (Reference 4.2.1).

3.10 ALTERNATIVES TO PROCESSES AND DESCRIPTIONS IN WCAP-16097-P-A

Table 3-2 identifies alternatives to the processes and design descriptions in WCAP-16097-P-A, “Common Qualified Platform Topical Report” (Reference 4.2.2).

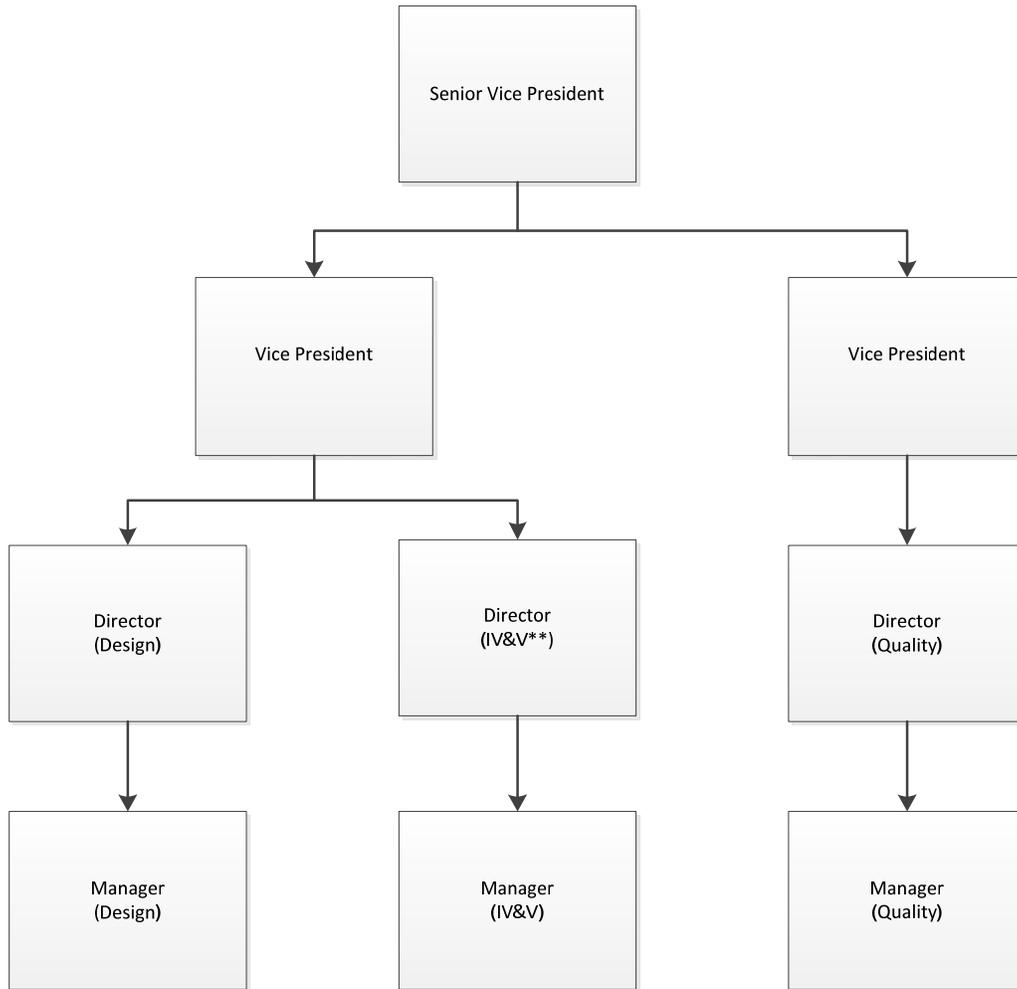
Table 3-1 Alternative Methods to the Common Q SPM		
WCAP-16096-P-A Section	WCAP-16096-P-A Text	Alternative
Glossary of Terms: Project Quality Plan (PQP)	A document that specifies alternatives or supplements to the Westinghouse QMS, Level 2, or Level 3 procedures as required to meet contractual requirements or quality standards other than those specified in the Westinghouse QMS. When the SPM refers to a PQP, it includes the Project Quality Plan and Project Plan defined in the Westinghouse Quality Procedures.	<u>Alternative</u> A document that specifies alternatives or supplements to the Westinghouse QMS, Level 2, or Level 3 procedures as required to meet contractual requirements or quality standards other than those specified in the Westinghouse QMS. When the SPM refers to a PQP, it includes the Project Quality Plan and Project Plan (including the Software Development Plan) defined in the Westinghouse Quality Procedures.
4.3.2.1 Initiation (Concept) Phase	Any alternatives to the SPM processes or additional project specific information for the SQAP, SVVP, SCMP or SOMP shall be documented and justified in the PQP.	Any alternatives to the SPM processes or additional project specific information for the SQAP, SVVP, SCMP or SOMP shall be documented and justified in the PQP.
4.3.1 Organization	The NA organization includes a Quality organization and an Engineering organization. The design team and the IV&V team are organized within the Engineering organization.	<u>Alternative</u> The NA organization includes a Quality organization and an Engineering organization. The design team and the IV&V team are in separate organizations at least to the Director level.
Exhibit 2-1 Design/IV&V Team Organization		See updated SPM Exhibit 2-1 Design/IV&V Team Organization following this table.

Table 3-1 Alternative Methods to the Common Q SPM (cont.)		
WCAP-16096-P-A Section	WCAP-16096-P-A Text	Alternative
4.6.2.10 Post Mortem Review	Suggestions for improvement and/or best practices that are identified during the Post Mortem Review should be documented via EXHIBIT 11-2 CORRECTIVE ACTIONS PROCESS.	<u>Alternative</u> Suggestions for improvement and/or best practices that are identified during the Post Mortem Review should be documented via the Corrective Action, Prevention and Learning (CAPAL) system. EXHIBIT 11-2 contains a screenshot of the Corrective Action Process (CAP) system. The CAP system has since been migrated to the Corrective Action, Prevention and Learning (CAPAL) system per Westinghouse Level 2 procedures.
5.5.1 Management of IV&V	The resources for performing the IV&V shall be identified in the Project Quality Plan (Reference 4) that is prepared by the Project Manager during the conception phase of the software life cycle.	<u>Alternative</u> The resources for performing the IV&V shall be identified in the AP1000 PMS SVVP that is prepared by the IV&V team during the conception phase of the software life cycle.
6.3.2 Configuration Change Control	Software Change Request Procedure, Step 5: Revised System Baseline: The SCR forms will be used as the basis to track all system changes and to verify that changes have been properly implemented and that documentation has been updated.	<u>Alternative</u> Software Change Request Procedure, Step 5: Revised System Baseline: The SCR forms will be used as the basis to track all software changes and to verify that changes have been properly implemented and that documentation has been updated.
6.3.4 Configuration Audits and Reviews	Configuration Audits and Reviews 3. External audits by customers or regulators shall be coordinated by the EPM [Engineering Project Manager] who will schedule personnel to be available if additional support is required.	<u>Alternative</u> External audits by customers or regulators shall be coordinated by QA or Licensing who will schedule personnel to be available, if additional support is required.

Table 3-1 Alternative Methods to the Common Q SPM (cont.)		
WCAP-16096-P-A Section	WCAP-16096-P-A Text	Alternative
6.4 SCM Schedule	<p>SCM milestones that shall be indicated on the project schedule include:</p> <ul style="list-style-type: none"> • CCB establishment • Establishment of a configuration baseline, and • Implementation of change control procedures. 	<p><u>Alternative</u></p> <p>SCM milestones that shall be indicated in the project schedule include:</p> <ul style="list-style-type: none"> • Establishment of a configuration baseline, and • Implementation of change control procedures. <p>Establishment of the Configuration Control Board (CCB) is captured in the AP1000 I&C program plan.</p>
9.2.3 Control	<p>An SCR log shall be maintained for the specific Common Q™ system implementation.</p> <p>The Platform Lead shall confirm that the approved SCR is entered into this log.</p>	<p><u>Alternative</u></p> <p>An SCR log shall be maintained for the specific Common Q™ system implementation. The Platform Lead shall confirm that the approved SCR is entered into the SCR log for any internal generic software changes. The Lead Software Engineer shall confirm that the approved SCR is entered into the SCR log for any PMS-specific software changes.</p>
10.5.1 Software Verification and Validation Plan	<p>The PQP shall also define the tracking and recording process for the hardware configuration pertinent to the software verification and validation process during all phases of the software life cycle.</p>	<p><u>Alternative</u></p> <p>The AP1000 PMS SVVP shall define the tracking and recording process for the hardware configuration (i.e., test configuration records) pertinent to the software verification and validation process during all phases of the software life cycle.</p>
10.10 Computer Code Certificate	<p>The completion of the implementation and checkout phase Software Verification and Validation report is the basis for the issuance of a Computer Code Certificate (see EXHIBIT 10-1 COMPUTER CODE CERTIFICATE for content requirements).</p>	<p><u>Alternative</u></p> <p>The completion of the installation and checkout phase Software Verification and Validation report is the basis for the issuance of a Computer Code Certificate (see EXHIBIT 10-1 COMPUTER CODE CERTIFICATE for content requirements).</p>

Table 3-1 Alternative Methods to the Common Q SPM (cont.)		
WCAP-16096-P-A Section	WCAP-16096-P-A Text	Alternative
11.4 Corrective Action	Corrective actions shall be documented on Exception Reports and Common Q™ Comment Records by the design team and shall be completed by the due date specified on the form...Once the independent reviewer is satisfied with the corrective action taken, the report form shall be signed.	<u>Alternative</u> Corrective actions shall be documented in RITS by the design team and shall be completed by the due date specified on the form...Once the RITS independent reviewer is satisfied with the corrective action taken, the report form shall be closed.
12 Secure Development and Operational Environment Plan	Secure Development and Operational Environment	<u>Alternative</u> The SPM, Section 12, details a Secure Development and Operational Environment Plan for Common Q systems. While this plan provides an acceptable method to comply with computer security requirements, AP1000 PMS will instead continue to use the Incorporated by Reference document APP-GW-J0R-012, "AP1000 Protection and Safety Monitoring System Computer Security Plan."

Exhibit 2-1
Westinghouse Organization Chart*



*This example organization chart shows the minimum level of separation required for the Design, IV&V, and Quality Teams

**System level validation testing is performed by another group. This group meets the same minimum level of independence required for the IV&V group depicted in this organization chart

Table 3-2 Alternative Methods and Design Descriptions to the Common Q Topical Report		
WCAP-16097-P-A Section	WCAP-16097-P-A Text	Alternative
References	27. WCAP-17266, Rev. 0, "Common Q Platform Generic Change Process," Westinghouse Electric Company LLC.	<u>Alternative</u> 27. WCAP-17266, "Common Q Platform Generic Change Process," Westinghouse Electric Company LLC.
5.2.1.1.1	A Motorola MC68360 processor (application processor), 1 Mbyte nonvolatile memory (Flash PROM) for the user built application and 2 Mbytes of nonvolatile memory (Flash PROM) for the system software and 2 Mbytes of Static RAM (SRAM). At startup, the application and system software are copied from the nonvolatile memory into the SRAM memory where it is executed.	<u>Alternative</u> A Motorola MC68360 processor (application processor), 1 Mbyte nonvolatile memory (Flash PROM) for the user built application and 2 Mbytes of nonvolatile memory (Flash PROM) for the system software and 2 Mbytes of Static RAM (SRAM). At startup, the application software is copied from the nonvolatile memory into the SRAM memory where it is executed, whereas the system software is executed out of the nonvolatile memory.
5.2.1.1.1	A second Motorola MC68360 processor for HSL communications, with an extra 512 Kbytes nonvolatile memory (Flash PROM) for the system software and an extra 2 Mbytes SRAM is provided for communications.	<u>Alternative</u> A second Motorola MC68360 processor for HSL communications, with an extra 512 Kbytes nonvolatile memory (Flash PROM) for the system software and an extra 512 Kbytes SRAM is provided for communications.
5.2.1.2.1	[]a,c	[]a,c
5.2.1.2.1	[]a,c	[]a,c

Table 3-2 Alternative Methods and Design Descriptions to the Common Q Topical Report		
WCAP-16097-P-A Section	WCAP-16097-P-A Text	Alternative
5.2.1.2.1	[] ^{a,c}	[] ^{a,c}
5.2.1.2.3	These tools can be used for on-line programming of the controller. However, for safety-related Common Q™ applications, this capability will be controlled administratively with additional password protection.	<u>Alternative</u> These tools can be used for on-line programming of the controller. However, for safety-related Common Q™ applications, this capability will be controlled administratively with additional password protection placed on the Windows OS login.
5.2.1.3	<i>[See “Section 5.2.1.3 Watchdog Timer Text” following this table.]</i>	<u>Alternative</u> <i>[See “Updated Section 5.2.1.3 Watchdog Timer Text” following this table.]</i>
Figure 5-13	<i>[See Figure 5-13 Watchdog Timer Configuration following this table.]</i>	<u>Alternative</u> <i>[See Updated Figure 5-13 Watchdog Timer Configuration following this table.]</i>
Table 5-1	<i>[See Table 5-1 Processor Module WDT Arrangement Watchdog Timer Summary following this table.]</i>	<u>Alternative</u> <i>[See Updated Table 5-1 Processor Module WDT Arrangement Watchdog Timer Summary following this table.]</i>
5.3.1.1	[] ^{a,c}	[] ^{a,c}
5.4.1.1	[] ^{a,c}	[] ^{a,c}

Table 3-2 Alternative Methods and Design Descriptions to the Common Q Topical Report		
WCAP-16097-P-A Section	WCAP-16097-P-A Text	Alternative
	[]a,c	[]a,c
5.4.1.4.1	This error report can be used for alarm or screen indication to direct technicians to the specific AC160 node that has the CI failure. Normally the failed module will be indicated by a red light on the front panel. However, if this was a transient error and the PM is able to reboot the CI, the CI will return to service and there will be no red light.	<u>Alternative</u> This error report can be used for alarm or screen indication to direct technicians to the specific AC160 node that has the CI failure. Normally the failed module will be indicated by a red light on the front panel.
5.6.10	[]a,c	[]a,c

Section 5.2.1.3 Watchdog Timer Text:

[

]a,c

Updated Section 5.2.1.3 Watchdog Timer Text:

[

]a,c

a,c

a,c

Table 5-1 Processor Module WDT Arrangement Watchdog Timer Summary

a,c

Updated Table 5-1 Processor Module WDT Arrangement Watchdog Timer Summary

a,c

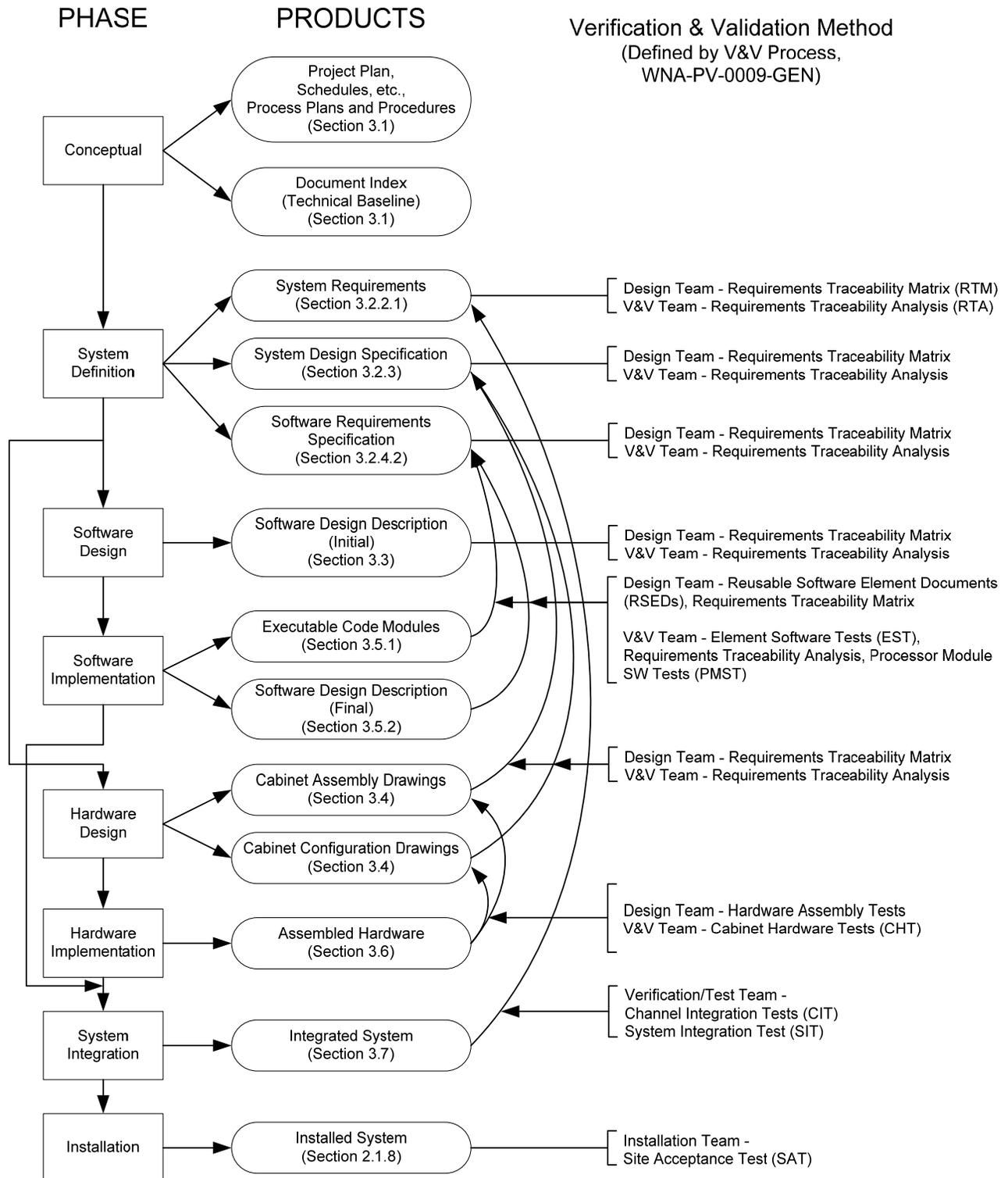


Figure 3-1 Development Process

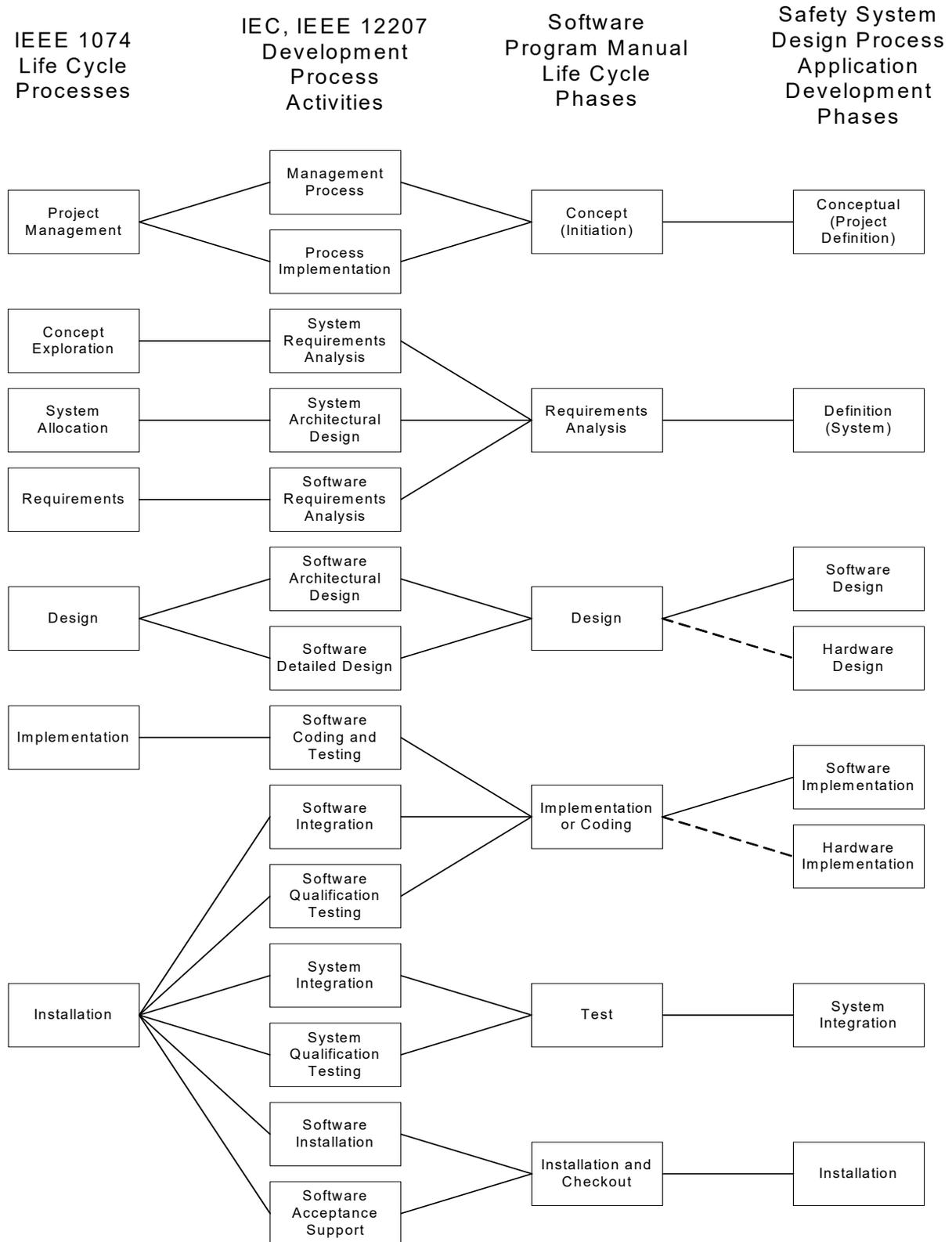


Figure 3-2 Correlation to Standard Life Cycle Phase

4 REFERENCES

4.1 INDUSTRY STANDARDS AND CODES

4.1.1 IEEE Standard 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," Institute of Electrical and Electronics Engineers, 1995.

4.1.2 IEEE/EIA 12207.0-1996, "Industry Implementation of International Standard ISO/IEC 12207: 1995 (ISO/IEC 12207) Standard for Information Technology-Software Life Cycle Processes," Institute of Electrical and Electronics Engineers/Electronic Industries Alliance, 1996.

4.2 WESTINGHOUSE DOCUMENTS

4.2.1 WCAP-16096-P-A (Proprietary), Rev. 4, "Software Program Manual for Common Q™ Systems," Westinghouse Electric Company LLC.

4.2.2 WCAP-16097-P-A (Proprietary), Rev. 3, "Common Qualified Platform Topical Report," Westinghouse Electric Company LLC.

Southern Nuclear Operating Company

ND-21-0486

Enclosure 12

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

**Westinghouse Electric Company Application for Withholding Proprietary Information
from Public Disclosure and Accompanying Affidavit CAW-20-5088**

(Enclosure 12 consists of 3 pages, plus this cover page)

Westinghouse Non-Proprietary Class 3

CAW-20-5088
Page 1 of 3AFFIDAVIT

COMMONWEALTH OF PENNSYLVANIA:

COUNTY OF BUTLER:

- (1) I, Zachary S. Harper, have been specifically delegated and authorized to apply for withholding and execute this Affidavit on behalf of Westinghouse Electric Company LLC (Westinghouse).
- (2) I am requesting the proprietary portions of WCAP-15927-P, Revision 8 and WCAP-16675-P, Revision 10 be withheld from public disclosure under 10 CFR 2.390.
- (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 10 CFR 2.390, 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 and is not customarily disclosed to the public.
 - (ii) 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 technical evaluation justifications 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.

Westinghouse Non-Proprietary Class 3

CAW-20-5088
Page 2 of 3AFFIDAVIT

- (5) Westinghouse has policies in place to identify proprietary information. 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.
- (6) The attached documents are bracketed and marked to indicate the bases for withholding. The justification for withholding 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

Westinghouse Non-Proprietary Class 3

CAW-20-5088
Page 3 of 3AFFIDAVIT

lower case letters refer to the types of information Westinghouse customarily holds in confidence identified in Sections (5)(a) through (f) of this Affidavit.

I declare that the averments of fact set forth in this Affidavit are true and correct to the best of my knowledge, information, and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: 9/3/2020


Zachary S. Harper, Manager
Licensing Engineering

Southern Nuclear Operating Company

ND-21-0486

Enclosure 14

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

**WCAP-16674-NP, "AP1000 I&C Data Communication and Manual Control of Safety
Systems and Components," Revision 9**

[Non-proprietary version of WCAP-16674-P, Revision 9]

(Enclosure 14 consists of 47 pages, plus this cover page)

WCAP-16674-NP
Revision 9
APP-GW-GLR-087
Revision 7

June 2019

AP1000[®] I&C Data Communication and Manual Control of Safety Systems and Components

Nuclear Safety Related



REVISION HISTORY

RECORD OF CHANGES

Revision	Author	Description
6	Albert W. Crew Edward P. Schindhelm	For the detailed record of changes for Revision 6, please see the record copy of that revision in EDMS.
7	Kastytis Vaicenas Edward P. Schindhelm	For the detailed record of changes for Revision 7, please see the record copy of that revision in EDMS.
8	Joseph D. Veturis	For the detailed record of changes for Revision 8, please see the record copy of that revision in EDMS.
9	Melissa R. Englert	<p>This revision affects the following documents:</p> <ul style="list-style-type: none"> • <u>Proprietary</u> WCAP-16674-P, Revision 9 APP-GW-GLR-065, Revision 9 • <u>Non-Proprietary</u> WCAP-16674-NP, Revision 9 APP-GW-GLR-087, Revision 7 <p>The following E&DCRs were incorporated:</p> <ol style="list-style-type: none"> 1. APP-FSAR-GEF-008 <ol style="list-style-type: none"> a. Removed Reference 14. b. Revised text in Sections 4.1.3.1, 4.2.1, 6.4, and 7.2. 2. APP-FSAR-GEF-045 <ol style="list-style-type: none"> a. Updated Reference 1. b. Updated revision of Reference 7. c. Added new Reference 15. <p>The licensing review for this document is completed by reference.</p>

TABLE OF CONTENTS

LIST OF TABLES	v
LIST OF FIGURES	vi
ACRONYMS AND TRADEMARKS	vii
REFERENCES	ix
1 INTRODUCTION	1-1
2 AP1000 I&C ARCHITECTURE	2-1
3 NON-SAFETY COMMUNICATION	3-1
3.1 NON-SAFETY COMMUNICATION NETWORK	3-1
3.1.1 Real-Time Data Distribution	3-2
3.1.2 General Communications	3-2
3.1.3 Access Control.....	3-2
3.1.4 System Capacity	3-3
3.1.5 Data Storm Control.....	3-4
3.1.6 Analysis	3-5
3.2 NON-SAFETY DATALINK INTERFACES.....	3-5
3.2.1 Standalone Systems	3-6
3.2.2 Remote I/O	3-6
3.2.3 Non-Safety Smart I/O Fieldbuses.....	3-6
4 SAFETY COMMUNICATION	4-1
4.1 SAFETY COMMUNICATION NETWORKS	4-1
4.1.1 Real-Time Data Distribution	4-1
4.1.2 General Communications	4-1
4.1.3 Access Control.....	4-2
4.2 SAFETY DATALINK INTERFACES.....	4-2
4.2.1 Standalone Systems	4-2
4.2.2 Remote I/O	4-2
4.2.3 Safety Smart I/O Fieldbuses	4-2
4.2.4 Common Q High-Speed Links	4-2

TABLE OF CONTENTS (cont.)

5 COMMUNICATION BETWEEN SAFETY AND NON-SAFETY EQUIPMENT 5-1

5.1 SAFETY TO NON-SAFETY DATA FLOW 5-2

5.1.1 Case A and Case B – Hardwired Signal Interfaces 5-2

5.1.2 Case C – Unidirectional Network Datalink 5-3

5.2 NON-SAFETY TO SAFETY DATA FLOW 5-7

5.2.1 Case D – Non-Safety Manual Control of System-Level Safety Functions and
Non-Safety Interlock of PMS Test Functions 5-7

5.2.2 Case E – Non-Safety Control of Safety Components 5-8

6 COMPONENT INTERFACE MODULE 6-1

6.1 HARDWARE IMPLEMENTATION 6-3

6.1.1 []^{a,c} 6-3

6.1.2 Component Interface Module 6-3

6.2 LOGIC IMPLEMENTATION 6-6

6.3 VALIDATION 6-7

6.4 EQUIPMENT QUALIFICATION 6-7

7 MANUAL CONTROL OF SAFETY SYSTEMS AND COMPONENTS 7-1

7.1 MANUAL SYSTEM-LEVEL CONTROL 7-1

7.2 MANUAL COMPONENT-LEVEL CONTROL 7-2

8 CONCLUSIONS 8-1

LIST OF TABLES

None.

LIST OF FIGURES

Figure 2-1	High-Level Overview of the AP1000 I&C Architecture	2-4
Figure 3-1	Ovation Network Topology	3-1
Figure 5-1	Data Flow Between Safety and Non-Safety Equipment.....	5-2
Figure 5-2	Example Implementation of Case C Data Flow.....	5-6
Figure 5-3	Implementation of Case E Data Flow	5-11
Figure 6-1	CIM Functional Overview	6-1
Figure 6-2	Photograph of CIM Assembly	6-4
Figure 6-3	CIM Block Diagram	6-5

ACRONYMS AND TRADEMARKS

Acronyms	Definition
AC160	Advant [®] Controller 160
ADS	Automatic Depressurization System
AF100	Advant FieldBus 100
AOI	Advant Ovation Interface
BPL	Bistable Processor Logic
CDP	Cyclic Data Packet
CET	Core Exit Thermocouples
CIM	Component Interface Module
CMF	Common Mode Failure
CMT	Core Makeup Tank
COL	Combined Operating License
Common Q [™]	Common Qualified
DAS	Diverse Actuation System
DC	Direct Current
DDS	Data Display and Processing System
ELC	Ethernet Link Controller
EOF	Emergency Operations Facility
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Feature Actuation System
FOR	Fiber Optic Receiver
FOT	Fiber Optic Transmitter
FPGA	Field Programmable Gate Array
HART [®]	Highway Addressable Remote Transducer
HSI	Human-System Interface
I&C	Instrumentation and Control
I/O	Input/Output
IIS	In-core Instrumentation System
ILP	Integrated Logic Processor
IRWST	In-Containment Refueling Water Storage Tank
ITAAC	Inspections, Tests, Analyses and Acceptance Criteria
LCL	Local Coincidence Logic
LCS	Local Control Station
MCR	Main Control Room
NAP	Nuclear Application Program
NIS	Nuclear Instrumentation System
NRC	U.S. Nuclear Regulatory Commission
OCS	Operation and Control Centers
OLEDB	Object Linking and Embedding Database
OSC	Operations Support Center
OSI	OSIsoft, Inc.
PCB	Printed Circuit Board

ACRONYMS AND TRADEMARKS (cont.)

Acronyms	Definition
PI	A product of OSIsoft, Inc.
PLC	Programmable Logic Controllers
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
QDPS	Qualified Data Processing System
RCS	Reactor Coolant System
RLC	R-line Link Controller
RNC	Remote Node Controller
RNS	Residual Normal Heat Removal System
RMS	Radiation Monitoring System
RSR	Remote Shutdown Room
RTP	RTP Corporation
RTS	Reactor Trip System
SER	Safety Evaluation Report
SMS	Special Monitoring System
SOE	Sequence of Events
SPM	Software Program Manual
SRNC	Safety Remote Node Controller
T/C	Thermocouple
TCP/IP	Transmission Control Protocol/Internet Protocol
TSC	Technical Support Center
UDP/IP	User Datagram Protocol/Internet Protocol
UTP	Unshielded Twisted Pair

Advant, AMS, DeviceNet, Excel, Foundation, HART, Microsoft, Modbus, Ovation, Profibus-DP, QNX, and SNAP-ON are trademarks or registered trademarks of their respective owners. Other names may be trademarks of their respective owners

AP1000 and Common Q are trademarks or registered trademarks of Westinghouse Electric Company LLC, its affiliates and/or its subsidiaries in the United States of America and may be registered in other countries throughout the world. All rights reserved. Unauthorized use is strictly prohibited. Other names may be trademarks of their respective owners.

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

REFERENCES

1. WCAP-16097-P-A (Proprietary), Rev. 3, "Common Qualified Platform Topical Report," (as modified by the Topical Report alternatives in WCAP-15927, Rev. 7), Westinghouse Electric Company LLC.
2. Deleted.
3. Deleted.
4. Deleted.
5. APP-GW-GL-700, Rev. 19, "AP1000 Design Control Document," Westinghouse Electric Company LLC.
6. Deleted.
7. WCAP-16675-P (Proprietary), Rev. 9, "AP1000 Protection and Safety Monitoring System Architecture Technical Report," Westinghouse Electric Company LLC.
8. IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Inc., 1991.
9. IEEE Standard 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electric and Electronics Engineers, Inc., 2003.
10. WCAP-16096-P-A (Proprietary), Rev. 4, "Software Program Manual for Common Q Systems," Westinghouse Electric Company LLC.
11. IEEE Standard 384-1981, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," Institute of Electrical and Electronics Engineers, Inc., 1981.
12. Deleted.
13. WCAP-17226-P (Proprietary), Rev. 1, "Assessment of Potential Interactions between the Core Exit Thermocouple Signals and the Self-Powered Detector Signals in the AP1000 In-core Instrumentation System," Westinghouse Electric Company LLC.
14. Deleted.
15. WCAP-15927, Rev. 7, "Design Process for AP1000 Common Q Safety Systems," Westinghouse Electric Company LLC.

1 INTRODUCTION

This document provides technical information regarding:

1. Data communication between the functional systems that comprise the AP1000[®] Instrumentation and Control (I&C) system and between the AP1000 I&C system and external systems. (Situations in which downstream components {valves, breakers, etc.} receive independent demands from both safety and non-safety I&C systems are beyond the scope of this document.)
2. The Component Interface Module (CIM) that is used to interface the I&C system to safety system components.
3. The manual control of the safety system at the system-level and the component-level.

Submittal of this information allows for early U.S. Nuclear Regulatory Commission (NRC) review of the communication design and compliance with applicable regulatory guidance and criteria prior to completion of the detailed design. This document will be used to address Protection and Safety Monitoring System (PMS) Design Inspections, Tests, Analyses and Acceptance Criteria (ITAAC) and Combined Operating License (COL) item closure.

2 AP1000 I&C ARCHITECTURE

A high-level overview of the AP1000 I&C architecture is shown in Figure 2-1. The architecture is divided into the following functional systems:

- Safety System
 - Protection and Safety Monitoring System (PMS) – The safety grade PMS detects off-nominal conditions and actuates appropriate safety functions necessary to achieve and maintain safe shutdown. The PMS is implemented using the Westinghouse Common Qualified (Common Q™) Platform described in WCAP-16097-P-A, “Common Qualified Platform Topical Report” (Reference 1), and accepted by the U.S. Nuclear Regulatory Commission (NRC) via the Safety Evaluation Reports included in Reference 1.
- Non-Safety Systems¹
 - Plant Control System (PLS) – The PLS provides the functions required for normal operation from cold shutdown through full power. This also includes the Digital Rod Position Indication System, the Digital Rod Control System, and a portion of the Turbine Control and Protection System.
 - Data Display and Processing System (DDS) – The DDS provides data that result in alarms and displays for both normal and emergency plant operations to the equipment used for processing. It includes the displays, the real-time data network, the alarm system, the Nuclear Application Programs (NAPs), the logging function, and the archiving function. DDS also provides the manual actuation switches in the remote shutdown room (RSR).
 - Special Monitoring System (SMS) – The SMS consists of standalone diagnostic systems that preprocess data from specialized sensors. An example includes the Digital Metal Impact Monitoring System.
- Other Systems
 - Diverse Actuation System (DAS) – The DAS is a non-safety system that provides an alternate means of initiating reactor trip, actuating selected engineered safety features (ESFs), and monitoring plant information. This system addresses the unlikely coincidence of a postulated plant transient and a postulated common mode failure (CMF) in the PMS. The DAS is a non-safety system, but has special design process requirements due to its mission.

1. The PLS functions and the DDS functions are both implemented on a common integrated platform. In practice, the differentiation between the two functional systems is somewhat artificial.

- In-core Instrumentation System (IIS) – The primary function of the IIS is to provide data for a three-dimensional flux map of the reactor core. This is a non-safety function. The secondary function is to provide the PMS with thermocouple (T/C) signals for the post-accident inadequate core-cooling monitor. This is a safety function. The tertiary function is to provide the DAS with a separate set of T/C signals. This is a non-safety function. The safety and non-safety functions share only the mechanical instrumentation assemblies (that are placed within the reactor) and cabling. There is no electrical interface between the core exit thermocouples (CETs) and the incore instrumentation electronics of the IIS. Separate signal processing electronics are used. See WCAP-17226-P, “Assessment of Potential Interactions between the Core Exit Thermocouple Signals and the Self-Powered Detector Signals in the AP1000 In-core Instrumentation System” (Reference 13).
- Operation and Control Centers (OCS) System – The OCS system includes the main control room (MCR), the technical support center (TSC), the operations support center (OSC), the RSR, the emergency operations facility (EOF), and the Local Control Stations (LCSs). From an I&C point of view, the OCS represents the integration of AP1000 human-system interface (HSI) resources from the PMS, PLS, DDS, and DAS. It, therefore, has portions that are safety grade and portions that are non-safety grade.

The Radiation Monitoring System (RMS) design descriptions and licensing requirements are captured in APP-GW-GL-700 “AP1000 Design Control Document” (Reference 5) Section 11.5. The RMS is referenced in this document because of its interfaces to the PMS and PLS as a standalone system.

The major non-safety systems (DDS, PLS, and SMS) and the non-safety portions of the IIS, RMS, and OCS are integrated using a plant-wide real-time data distribution network. That network is implemented using the Emerson Ovation[®] Network.

Within each PMS division, the intra-division ABB Advant[®] FieldBus 100 (AF100) bus provides the means to exchange data between the Class 1E cabinets within the division, including data that have been received from external systems. This bus is part of the Westinghouse Common Q platform, is described in the Common Q topical report (Reference 1), and is referred to as the Common Q network. Specifically, the AF100 bus is used to allow the various Advant Controller 160 (AC160) controllers and Flat Panel Display Systems within a division to exchange information for maintenance, test, diagnostic, communication (to the non-safety system), display, and manual control. The majority of the dataflow is from the AC160 controllers to the Flat Panel Display Systems (for display and for communication to the non-safety system). Therefore, the AF100 bus is used to integrate information exchange among the AC160 controllers performing the Engineered Safety Feature Actuation System (ESFAS) and reactor trip functions and the Flat Panel Display Systems. The AF100 bus is not in the sensor-to-reactor trip path or sensor-to-ESFAS-actuation path. The ESFAS and reactor trip functions do not require information from each other to perform their safety functions, except for ESFAS functions that also initiate reactor trip (i.e., Safeguards Actuation, Automatic Depressurization System {ADS} Actuation, and Core Makeup Tank {CMT} Injection).

In order to support the DDS and OCS functions, there is a need to transfer a large amount of data from the safety portions of the I&C system to the non-safety portions of the I&C system. To achieve this data transfer, there are four unidirectional gateways, one for each of the PMS divisions. The Advant Ovation Interface (AOI) communication gateways allow the PMS divisions to provide data to the non-safety systems. The AOI gateway comprises a non-safety portion connected to the Ovation network and a safety system portion connected to the Common Q network in each division. The design of this gateway meets Class 1E to non-Class 1E separation requirements.

The DAS is diverse and independent from the PMS from the sensors up to the actuation devices. It is also separate from the PLS. Its only connections to the PLS are contact outputs used to facilitate reporting of DAS actuations and faults to the operator via the DDS.

In conclusion, the AP1000 I&C system consists of: one safety system (PMS) which has four independent divisions, three non-safety systems (PLS, DDS, and SMS), and two systems that perform both safety and non-safety functions (IIS and OCS), and interfaces with the RMS which performs both safety and non-safety functions. Within each safety division, the PMS internal functions (Nuclear Instrumentation System {NIS}, Qualified Data Processing System {QDPS}, Reactor Trip System {RTS}, ESFAS, and the Component Logic System) and the safety portions of IIS, RMS, and OCS are integrated using the Common Q network. The non-safety systems (PLS, DDS, and SMS), the non-safety portions of IIS, RMS, and OCS, and the safety system data (via the AOI gateways) are integrated using the Emerson Ovation Network. The DAS is diverse and independent from the PMS from the sensors up to the actuation devices and separate from the PLS.

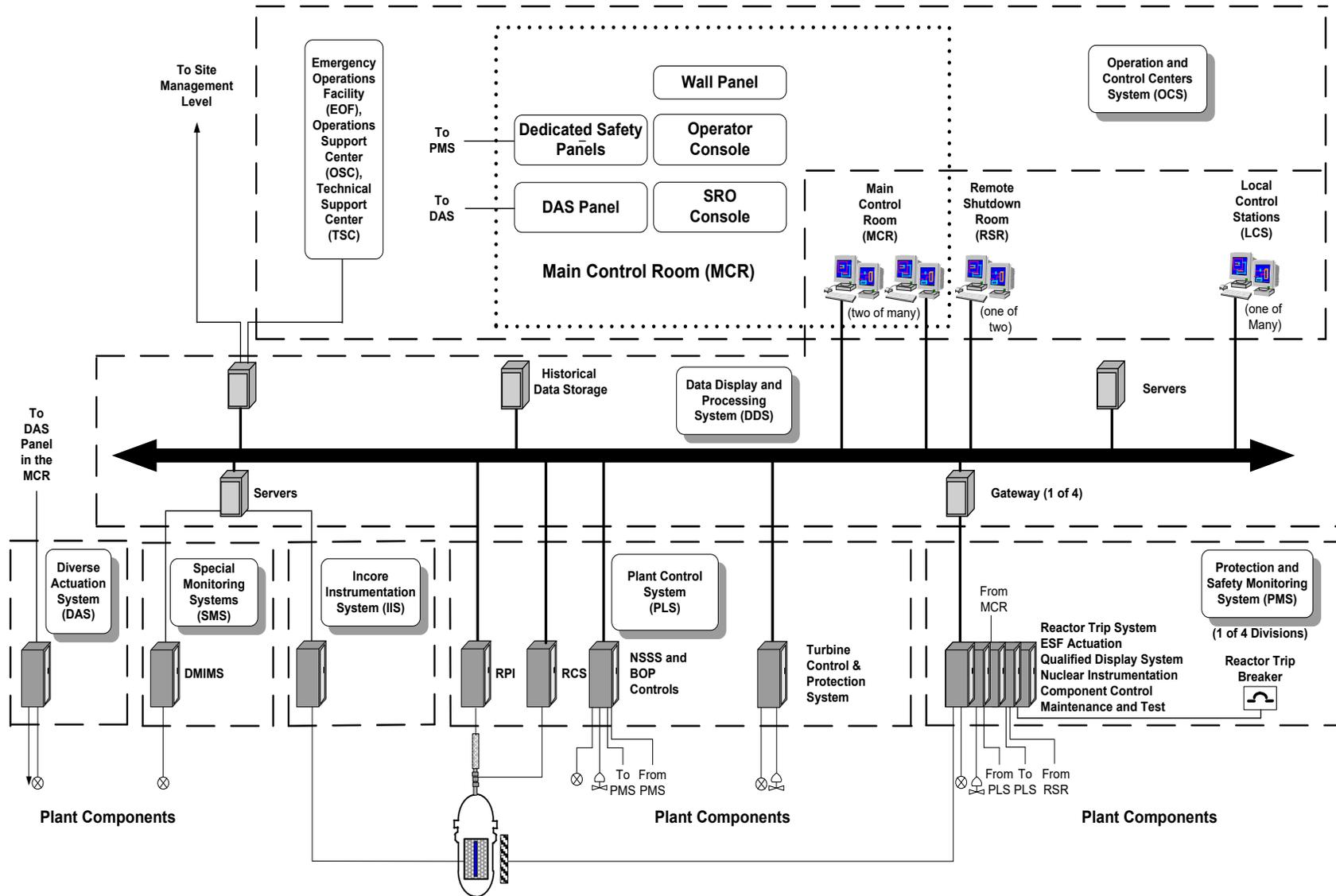


Figure 2-1. High-Level Overview of the AP1000 I&C Architecture

3 NON-SAFETY COMMUNICATION

Non-safety communication consists primarily of the non-safety communication network and the non-safety datalink interfaces. These interfaces do not directly communicate with the safety systems, except as described in Section 4.

3.1 NON-SAFETY COMMUNICATION NETWORK

The non-safety communication network is implemented using the Ovation network. It is a robust, fault-tolerant, high-speed, commercially available communications network designed for mission critical process control applications.

The network is comprised of a number of high-speed Ethernet switches¹ configured in a redundant, two-tiered, hierarchical, tree topology as shown in Figure 3-1.

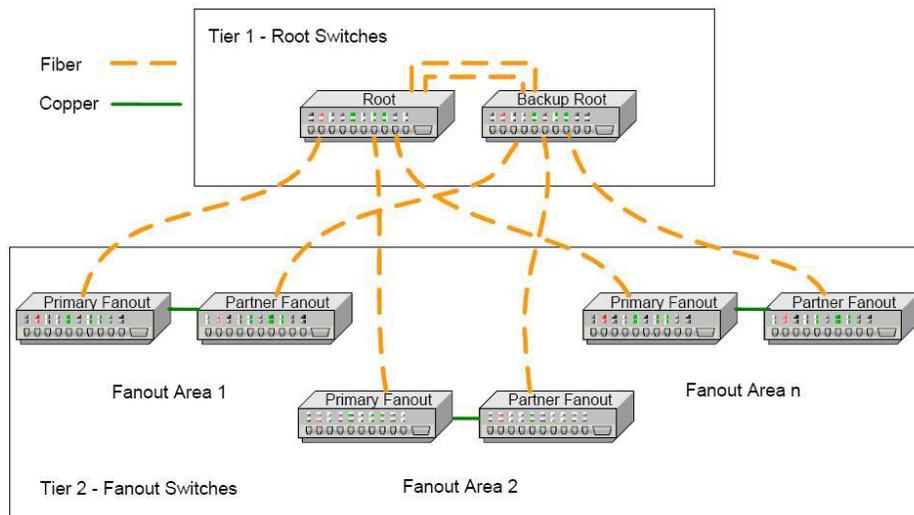


Figure 3-1. Ovation Network Topology

The network uses unaltered Ethernet protocols, high-speed Ethernet switches, and full-duplex cabling (fiber or copper unshielded twisted pair {UTP}). [

] ^{a,c}

1. The material presented here uses the term “switch” to refer to the communications devices that comprise the backbone of the network. Switches provide the minimum capability required to implement the network. Devices with more capabilities, such as routers, may also be used for this function.

The network provides real-time data distribution and general purpose communication. Real-time data distribution is defined as the scheduled periodic multicast of real-time data pertaining to the plant processes. General purpose communication is defined as the aperiodic exchange of data for other purposes, such as system operation, diagnostics, maintenance, etc.

3.1.1 Real-Time Data Distribution

Real-time data distribution within the non-safety system supports the integration within functional systems and among functional systems, including the integration between the safety system and non-safety systems.

The network supports the automatic periodic transmission of data at two rates: one sample per second and ten samples per second. The total periodic data capacity is 200,000 point values per second.

3.1.2 General Communications

The Ovation network supports network standard communications protocols such as Transmission Control Protocol/Internet Protocol (TCP/IP) and User Datagram Protocol/Internet Protocol (UDP/IP) for general purpose communications. Within the Ovation system, general purpose communications based upon standard protocols are used for aperiodic data, including file-type data transferred from the historian and plant database to be presented at the HSI, plant informational data messages, alarm messages, and sequence of events (SOE) messages to the plant historian for long-term historical storage. This communication occurs on the same physical media as the real-time periodic data, but is implemented in such a way as to preserve the design philosophy of guaranteeing the real-time periodic data transmission without loss, degradation, or delay, even during plant upsets.

The Ovation network can also simultaneously support non-Ovation general purpose communications on the same physical network. [

] ^{a,c}

3.1.3 Access Control

While the Ovation open interfaces provide enhanced connectivity, the control network is protected from the outside world via the use of security devices and software. The network can be configured to provide secure communications with the remainder of the plant business and engineering systems. If required, additional security devices may be implemented between the Ovation network and higher levels in the network hierarchy that permit bidirectional communication.

3.1.3.1 On-Site

On-site access to Ovation information is through a local login at a workstation physically attached to the Ovation network. The Ovation system provides a tool set to permit the configuration of an integral security scheme, where the combination of the user's login privileges, the physical workstation, and the local/remote access method determines the functionality that can be performed in that session. In this context, "remote" is still within the Ovation network, e.g., remote access to a particular workstation in the Ovation network from another workstation in the Ovation network. [

] ^{a,c}

3.1.3.2 Off-Site

Off-site access to Ovation information is provided via secure servers that provide methods for delivering Ovation information to external, non-Ovation resources, ensuring that this communication cannot interfere with Ovation operation. Off-site access to view-only Ovation data can be employed using security appliances to enforce unidirectional communication to less secure networks.

The data access servers provide standard methods for accessing information from the Ovation network for use by engineering and business applications. These server interfaces are designed to support both human interaction (e.g., Intranet-view-only of control system data) and programmatic interfaces (e.g., Object Linking and Embedding Database {OLEDB} provider access to historical information for use in programs). Additionally, Ovation provides standard reporting tools that can be used to generate periodic reports that can be generated and stored in standard applications format (such as Microsoft[®] Excel[®] spreadsheet software).

Off-site access from the EOF and the Utility/Business Operations network will be implemented using the various methods outlined above, the details of which will be determined during system design.

3.1.4 System Capacity

With respect to periodic data, the network is designed to support up to 200,000 point values per second using a nominal percentage of the overall network bandwidth. The values per second number is obtained by combining the number of points originated at the one second frequency at a 1:1 ratio, with those points originated at a tenth of a second frequency at a 10:1 ratio. For example, if a system contains 50,000 one second points and 500 tenth of a second points, the total point values per second is $55,000 = ((50,000 * 1) + (500 * 10))$. The network load associated with periodic data origination is constant; it does not change during plant upset conditions. The Ovation vendor has thoroughly tested the network at the 200,000 point values per second limit. The total point count continues to be defined as the AP1000 design progresses. A design goal is to limit the number of point values per second to the extent possible. The exact number of point values per second, and therefore the base load on the network, will be evaluated as the design is finalized.

With respect to aperiodic data, the network load is variable, but managed. As described previously, aperiodic network data includes: alarm message data, historical archival and retrieval data, and print requests. Alarm message data will be minimized to the extent possible by limiting the number of points subject to alarm checking and by carefully selecting alarm limits to minimize nuisance alarms. A similar engineering analysis will be performed to determine the number of points subject to historical data collection. A comprehensive evaluation of data collection deadbands will be performed to ensure optimal collection sampling rates, which will limit the number of data samples transferred over the network to the historian. An additional component of aperiodic network traffic is that generated by station staff. Operations and engineering personnel located within the main control area can request historical data for display on historical reviews. This data is retrieved from the historian and transferred over the network for display at the Operator Station. Personnel can also request data from the system to be directed to printers in order to produce hardcopies. This aperiodic network load does NOT include requests for plant data from users external to the main control area, e.g., TSC, enterprise network users, etc. Request for data by these “external users” is managed outside the plant I&C network and therefore has no impact on non-safety network load.

3.1.5 Data Storm Control

Storm control is configured on the Ovation network to ensure that highway availability requirements are satisfied given the unlikely possibility that a software or hardware malfunction, or a malicious network attack, would introduce a packet storm on the control system highway.

Storm control is implemented with configuration settings provided by the switch operating system. In general, each port subject to storm control is configured with traffic ingress block and restoration settings. These values are typically a percentage of the total available bandwidth that can be used by the broadcast or multicast traffic. When traffic entering a port exceeds the pre-defined block value, packet forwarding on the port is blocked. Packet forwarding resumes when the traffic falls below the predefined “restore forwarding” setting. [

] ^{a,c}

Storm control is put in place to protect the network from data storms produced as a result of atypical conditions including: hardware malfunctions and errors introduced by humans. The thresholds are set on a per port basis such that native Ovation traffic – periodic process point data; aperiodic alarm message traffic, etc. – will not activate the storm control function. [

] ^{a,c} As the system design is finalized, the overall point count, and the point distribution across the drops, will be defined to a level to permit a more detailed analysis of overall network load, as well as the network load attributed to a specific drop.

This information, in conjunction with vendor data, will be used to confirm that the data storm threshold settings are appropriate.

In addition to the system storm control configuration installed on the network switches, the Ovation controller has been hardened against excessive network traffic through the implementation of a software modification that prioritizes critical control functionality over network communications. This capability, used in conjunction with control logic design that requires no inputs from the network, permits the controller to continue to control critical plant operations during a network storm or a complete loss of network event.

3.1.6 Analysis

As described above, the load on the AP1000 non-safety network consists of periodic and aperiodic data. Periodic data consists of a maximum of 200,000 point values per second resulting in a constant base load on the network. An AP1000 design goal is to utilize much less than the maximum available point values per second. This will provide additional spare capacity and will result in a lower base load on the network. As the design is finalized, a firm number of point values per second will be determined. This will be used to calculate the base network load, and therefore, the network bandwidth available for aperiodic data communications. Analytical justification of network capacities will be reviewed for correctness. In general, the network load due to aperiodic data traffic is expected to be very small in relation to the overall bandwidth of the system. The aperiodic data levels can be managed through careful system configuration. Network impacts associated with station staff in the main control area is somewhat limited by the number of operators and Operator Stations and the number of engineers and Engineering Stations.

Based on the current evaluation of expected network traffic, the single network design will meet or exceed all system capacity and network loading requirements. Westinghouse will continue to evaluate the expected network loading impacts associated with both periodic and aperiodic data communication and refine the network design as required to ensure reliable network operation.

3.2 NON-SAFETY DATALINK INTERFACES

Non-safety datalinks are employed to transmit data between various systems. The interfaces to these systems must be carefully designed to preserve the integrity of the AP1000 control system network. To that end, mitigative strategies will be employed to ensure that defense in depth is maintained throughout the network. Assessments of each datalink pathway and associated assets/systems will be used as a basis for determining the specific mitigative measures that may need to be deployed.

3.2.1 Standalone Systems

The Ovation system supports standard and custom datalinks, both at the controller and workstation level. Controller-level interfaces include standard interfaces to Allen-Bradley programmable logic controllers (PLCs), and GE Mark V/VI, Toshiba, and Mitsubishi Heavy Industries turbine control systems, as well as a standard Modbus™ interface and OSIsoft, Inc. (OSI) PI historian interface. At the controller level, the datalink interface can be accomplished via a standard input/output (I/O) module (e.g., the R-line Link Controller {RLC} for RS-232/RS-422/RS-485 serial links or the Ethernet Link Controller {ELC} for Fast Ethernet Links), or via Fast Ethernet communications interfaces at the controller processor level. RLC interfaces are used for low-speed or low-capacity interfaces such as component monitoring. Ethernet interfaces are used for higher-speed information or larger amounts of data, such as interfacing to a PLC-based local control system. For the RLC, ELC, and Ethernet controller links, the interface can be supplied redundantly, and is designed in such a way that the controller can utilize the information in standard Ovation control schemes just as native I/O points.

Workstation datalinks include both standard and custom link implementations. Custom links are generally provided to interface to non-standard protocols, as is typically encountered in the retrofit market. Standard links are available for interfacing, for example, to foreign I/O such as RTP I/O, Modbus over Ethernet, and for standard serial communications such as RS-232. The AOI is an example of a Westinghouse standard workstation datalink. Any workstation that functions as a datalink application server can provide the interfaced information to the Ovation network with up to 10,000 process points per drop, supporting all scan and alarming features.

3.2.2 Remote I/O

The Ovation system supports the use of remote I/O so that I/O modules can be clustered close to field devices, minimizing field cabling costs and also accommodating harsher environments. Remote I/O is in contrast to local I/O, which is housed in the same cabinet as the controller or next to it in an extended cabinet. For local I/O, all I/O modules reside in up to four cabinets, which are placed side by side. All field wiring leads to local or remote cabinets. [

] ^{a,c}

3.2.3 Non-Safety Smart I/O Fieldbuses

The Ovation system supports Highway Addressable Remote Transducer (HART®) I/O, Foundation™ Fieldbus, Profibus-DP®, and DeviceNet™ smart I/O interfaces. The Ovation fieldbus solution is modular, and a single controller can simultaneously interface to fieldbus devices, HART I/O modules, conventional I/O modules, and third-party I/O.

3.2.3.1 HART I/O

The Ovation controller supports native HART I/O modules. HART is technology that provides a digital information signal superimposed on a 4-20 mA traditional sensor loop. The digitized signal provides up to four HART multivariables which provide additional information from HART-enabled devices, eliminating additional cabling required to provide the same information using traditional sensors and control output devices.

The Ovation HART input module has eight inputs, with each input having an individual HART modem (supporting up to four HART multivariables), and individual channel-to-channel isolation. The Ovation HART output module has four channels, also with individual HART modems per channel, and individual channel-to-channel isolation.

The HART I/O modules can support both traditional 4-20 mA devices and HART devices on the same card.

3.2.3.2 Foundation Fieldbus

Foundation Fieldbus H1 is typically used for analog-type devices such as sensors and modulating control valves. There is a large assortment of “smart” devices available with the interface.

The Ovation Foundation Fieldbus solution is modular and scalable. The interface between the Foundation Fieldbus instrumentation and the Ovation controller is via native Ovation Foundation Fieldbus interfaces modules. There are up to eight Foundation Fieldbus interface modules per controller, with each interface modules supporting two Fieldbus segments, and up to 16 devices per segment. Typically, up to 12 devices are utilized per segment, with fewer devices if the segment is used for closed loop control. Evaluation of the applicability of Ovation Foundation Fieldbus is part of the ongoing I&C system design process.

3.2.3.3 Profibus-DP

Profibus-DP is typically used for digital ON/OFF type devices. In addition to being supported by the appropriate devices, it is suitable for long distances while remaining less sensitive to power, grounding, polarity, and resistance concerns.

The interface between the Profibus devices and the Ovation controller is via native Ovation Profibus interface modules operating as a DP-V2 Profibus master. Each Ovation Profibus I/O module supports communication with two segments and up to 126 field devices. [

] ^{a,c}

3.2.3.4 DeviceNet

DeviceNet is a field-proven interface for discrete actuators and sensors. The interface between the DeviceNet devices and the Ovation controller is via native Ovation DeviceNet interface modules.

The DeviceNet communication, while supported by the Ovation platform, is not used on AP1000 I&C architecture.

3.2.3.5 Asset Management

Another important component of the intelligent field interface solution is the Asset Management Solutions (AMS™) suite of software. AMS software and the associated SNAP-ON™ applications are a suite of software solutions for streamlining all maintenance activities relative to instrumentation and valves in a process plant. This package can be integrated into the Ovation workstation and Ovation controller to give the user direct access to all intelligent devices connected to the Ovation I/O. With AMS integrated into Ovation, digitized HART or Foundation Fieldbus parameters such as valve position can be mapped to Ovation process points which can be used anywhere required in the Ovation Distributed Control System. AMS provides direct visibility from the Ovation workstation to each “smart” device in the plant that is connected to Ovation.

4 SAFETY COMMUNICATION

Communication within the safety system consists primarily of the four intra-divisional safety communication networks and safety datalink interfaces.

4.1 SAFETY COMMUNICATION NETWORKS

Within each PMS division, the intra-divisional ABB Advant[®] FieldBus 100 bus provides the means to exchange data between the Class 1E cabinets within the division, including data that have been received from external systems. This network is part of the Westinghouse Common Q Platform (see Reference 1) and is referred to as the Common Q network.

The AF100 bus is a high-performance, deterministic communication network, intended for communication between AC160 controllers and Flat Panel Display Systems within the same division. The transmission rate is 1.5 Mbit/second or faster.

Like the non-safety network, the AF100 bus provides real-time data distribution and general purpose communication. On the AF100 bus, real-time data distribution is referred to as process data transfer and general purpose communication is referred to as message transfer. [

] ^{a,c}

4.1.1 Real-Time Data Distribution

Real-time data distribution is accomplished using process data transfer communication on the AF100 bus. [

] ^{a,c}

4.1.2 General Communications

General communication is accomplished using message transfer services. Message transfer is not performed cyclically like process data transfer, but only when one (or more) of the attached communication interfaces have something to send. Message transfer does not influence process data transfer in any way. Process data transfer remains deterministic. [

] ^{a,c}

Within the PMS, general communication is primarily used for diagnostic purposes. Security is maintained since the Flat Panel Display Systems cannot be remotely programmed over the AF100 bus and the ability to remotely program the AC160 controllers over the AF100 bus has been disabled in the PMS.

4.1.3 Access Control

4.1.3.1 On-Site

The four PMS intra-divisional Common Q networks are only accessible in the divisional equipment rooms and in the MCR. Network fiber optic cabling between each of the equipment rooms and the MCR is in an enclosed raceway. Access is not available in any of the other operation and control centers.

4.1.3.2 Off-Site Access

The four PMS intra-divisional Common Q networks are not accessible from off-site locations.

4.2 SAFETY DATALINK INTERFACES

4.2.1 Standalone Systems

The PMS interfaces to the standalone Radiation Monitoring System (RMS). RMS has two parts, one for safety functions and the other for non-safety functions. There is no interface between the two parts. The safety portion of the RMS interfaces to the PMS using simple analog and/or discrete digital signals; this interface does not use network or datalink connections. Electrical isolation between the RMS and the PMS is not required since the safety portion of the RMS is Class 1E. There is no interface between the non-safety portion of the RMS and the PMS.

The CETs used by the QDPS function of the PMS are physically housed within IIS. There is no electrical interface between the CETs and the incore instrumentation electronics of the IIS. The CETs interface to the PMS using simple analog signals; these interfaces do not use network or datalink connections. Electrical isolation between the CETs and the PMS is not required since the CETs are Class 1E.

4.2.2 Remote I/O

The PMS does not use a remote I/O system. However, some of the PMS cabinets do contain components that are accessed via the PLS remote I/O system (e.g., hardwired connections from SOE to PLS cabinets).

4.2.3 Safety Smart I/O Fieldbuses

The PMS does not use smart I/O devices and their associated fieldbus communication buses (e.g., Foundation Fieldbus and Profibus). It does use the ABB AF100 bus. However, the AF100 bus is not used as a smart I/O bus; rather, it is used to implement the Common Q network discussed previously.

4.2.4 Common Q High-Speed Links

The PMS uses high-speed links to serially communicate certain data within and across PMS divisions. These links are part of the Westinghouse Common Q Platform (see Reference 1). The functionality of these links within the PMS is described in WCAP-16675-P, "AP1000 Protection and Monitoring System Architecture Topical Report" (Reference 7).

5 COMMUNICATION BETWEEN SAFETY AND NON-SAFETY EQUIPMENT

The AP1000 certified design (APP-GW-GL-700, Rev. 19, “AP1000 Design Control Document” {Reference 5}) includes the following types of data flow between the safety and non-safety systems:

1. Data Flow from PMS to PLS for Control Purposes – this type of data flow is necessary since the PLS uses PMS sensor signal values and PMS calculated values as inputs to control functions.
2. Data Flow from PMS to DDS for Information System Purposes – this type of data flow is necessary since the DDS is responsible for the traditional plant computer functions that include the display, processing, alarming, logging, and archiving of PMS process and system data.
3. Data Flow from DDS to PMS for Safety System Actuation Purposes – this type of data flow is necessary to implement system-level actuation of the safety system from the RSR which is entirely non-safety. (See, for example, the Inspections, Tests, Analyses, and Acceptance Criteria {ITAAC}).
4. Data Flow from PLS to PMS for Component Control Purposes – this type of data flow is necessary to implement soft control of safety system components from the PLS.

The certified design establishes the following ITAACs (in Table 2.5.2-8 of Reference 5) regarding the implementation of these data flows:

- 7.a) The PMS provides process signals to the PLS through isolation devices.
- 7.b) The PMS provides process signals to the DDS through isolation devices.
- 7.c) Data communication between safety and non-safety systems does not inhibit the performance of the safety function.
- 7.d) The PMS ensures that the automatic safety function and the Class 1E manual controls both have priority over the non-Class 1E soft controls.
- 7.e) The PMS receives signals from non-safety equipment that provide interlocks for PMS test functions through isolation devices.

In the certified design, the required data flows are implemented using divisionalized unidirectional gateways and individual analog and discrete digital signals as shown in Figure 5-1. Five cases are identified in the figure and labeled A through E. The cases are discussed in more detail in the following sections.

a,c



Figure 5-1. Data Flow Between Safety and Non-Safety Equipment

5.1 SAFETY TO NON-SAFETY DATA FLOW

5.1.1 Case A and Case B – Hardwired Signal Interfaces

Analog inputs required for both control and protection functions (e.g., pressurizer pressure) are processed independently with separate input circuitry. The input signals are classified as safety-related and are, therefore, isolated in the PMS cabinets before being sent to the PLS as individual hardwired analog signals. This is identical to the type of interface in existing Westinghouse plants. An example of this type of interface is shown as Case A on Figure 5-1.

The PMS also provides data to non-safety equipment pertaining to analog and discrete digital signals calculated within the PMS (e.g., Over Temperature Delta Temperature Margin to Trip). These signals are classified as safety-related and are, therefore, isolated in the PMS cabinets before being sent to the non-safety equipment as individual hardwired analog or discrete digital signals. Typically, the resulting signals are sent to the PLS. Additionally, the outputs of certain PMS CIMs also directly actuate selected non-safety components (e.g., pressurizer heater block and feedwater pump trip). These isolated hardwired analog or discrete digital signal interfaces (whether to PLS or to non-safety components) are identical to those in existing Westinghouse plants. An example of this type of interface (between PMS and PLS) is shown as Case B on Figure 5-1.

In both cases A and B, qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by IEEE Standard 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations” {Reference 8}) They also provide functional isolation by preventing the non-safety system from adversely affecting the safety function.

Comparing these implementations against the ITAACs:

- 7.a) The PMS provides process signals to the PLS through isolation devices. – This ITAAC is met.
- 7.b) The PMS provides process signals to the DDS through isolation devices. – This ITAAC is not applicable to these data flows since the data flows are PMS to PLS data flows. However, the PLS does make this information available to the DDS.
- 7.c) Data communication between safety and non-safety systems does not inhibit the performance of the safety function. – This ITAAC is met.
- 7.d) The PMS ensures that the automatic safety function and the Class 1E manual controls both have priority over the non-Class 1E soft controls. – This ITAAC is not applicable to these data flows since the data flows are not used to implement non-Class 1E manual soft controls.
- 7.e) The PMS receives signals from non-safety equipment that provide interlocks for PMS test functions through isolation devices. – This ITAAC is not applicable to these data flows since the data flows are not used to implement the test interlock function.

5.1.2 Case C – Unidirectional Network Datalink

Various process-related signals (analog input signals, analog signals calculated within the PMS, digital signals calculated within the PMS, and SOE signals) are sent to the DDS for information system (plant computer) purposes. Non-process signals are also provided to the DDS for information system purposes. The non-process outputs inform the DDS of cabinet entry status, cabinet temperature, direct current (DC) power supply voltages, and subsystem diagnostic status, etc. There are also process-related signals that are sent from PMS to PLS that do not require the low transmission latency or the control system segmentation provided by the dedicated signal interfaces described for Cases A and B.

The AOI gateway in each PMS division connects the division's internal network to the non-safety real-time data network, which supports the remainder of the I&C system. Each gateway has two subsystems. One is the safety subsystem, which is part of the PMS division and interfaces to the Common Q network. The other is the non-safety subsystem, which is part of DDS and interfaces to the Emerson Ovation Network. The two subsystems are connected by a fiber-optic link. This type of interface is shown as Case C on Figure 5-1.

The flow of information between the two gateway subsystems is strictly from the safety subsystem to the non-safety subsystem. The unidirectional nature of the gateway is assured by the use of a single unidirectional fiber to connect the two gateway subsystems. Within the safety system, the fiber is connected to an optical transmitter. Within the non-safety system, the fiber is connected to a fiber-optic receiver. This arrangement provides electrical isolation between the systems (as required by IEEE 603-1991 {Reference 8}) and prevents all data flow (data, protocols, and handshaking) from the non-safety system to the safety system (providing the communication isolation envisioned by IEEE Standard 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" {Reference 9}, Annex E). It also provides functional isolation by preventing the non-safety system from adversely affecting the safety function. This implementation is shown in Figure 5-2.

The safety software for the AOI gateway has two parts. The first part is the Ethernet driver that is part of the QNX[®] operating system. The QNX operating system was commercially dedicated and the dedication report was accepted by the NRC as part of the Common Q Safety Evaluation Report (SER) process.

The second part of the AOI gateway software was developed by Westinghouse. This software followed the process specified for "Important to Safety" software in WCAP-16096-P-A, "Software Program Manual for Common Q Systems" (Reference 10) (the SPM), for safety software. The SPM was accepted by the NRC as part of the SER process for the Common Q Platform.

The AOI uses a physically unidirectional transmission fiber-optic datalink from the PMS to the non-safety system. The AOI gateway has no protection function in the PMS. The reliability of the PMS to perform its safety function is not dependent on the AOI gateway being functional.

For SOE signals such as partial trip signals, reactor trip signals, and ESF actuation signals, each division provides the signals to the SOE system/interface via a unidirectional fiber-optic link. The flow of information is strictly from the safety subsystem to the non-safety SOE system/interface. The unidirectional nature of the link is assured by the use of a single unidirectional fiber. The safety end of the fiber is connected to an optical transmitter. The non-safety end of the fiber is connected to a fiber-optic receiver. This arrangement provides electrical isolation between the safety and non-safety portions of the system (as required by IEEE 603-1991 {Reference 8}) and prevents all data flow (data, protocols, and handshaking) from non-safety to safety (providing the communication isolation envisioned by IEEE 7-4.3.2-2003 {Reference 9}, Annex E). It also provides functional isolation by preventing the non-safety equipment from adversely affecting the safety function. This type of interface is a variation of Case C in Figure 5-1.

Comparing this implementation against the ITAACs:

- 7.a) The PMS provides process signals to the PLS through isolation devices. – This ITAAC is met.
- 7.b) The PMS provides process signals to the DDS through isolation devices. – This ITAAC is met.
- 7.c) Data communication between safety and non-safety systems does not inhibit the performance of the safety function. – This ITAAC is met.
- 7.d) The PMS ensures that the automatic safety function and the Class 1E manual controls both have priority over the non-Class 1E soft controls. – This ITAAC is not applicable to this data flow since the data flow is not used to implement non-Class 1E manual soft controls.
- 7.e) The PMS receives signals from non-safety equipment that provide interlocks for PMS test functions through isolation devices. – This ITAAC is not applicable to this data flow since the data flow is not used to implement the test interlock function.

a,c



Figure 5-2. Example Implementation of Case C Data Flow

5.2 NON-SAFETY TO SAFETY DATA FLOW

The non-safety to safety data flows are not implemented using communication links; rather, they are implemented using discrete digital signals. These signals are used to implement non-safety manual control from the RSR of system-level safety functions (actuators, manual blocks and resets, manual reactor trip), non-safety interlock of certain PMS test functions, and non-safety manual component-level control of safety components.

5.2.1 Case D – Non-Safety Manual Control of System-Level Safety Functions and Non-Safety Interlock of PMS Test Functions

In the RSR, the non-safety manual control of system-level safety functions (actuators, manual blocks and resets, manual reactor trip) originate from dedicated switches. The individual discrete digital signals are classified as non-safety-related and are, therefore, isolated in the PMS cabinets before being used. At the RSR, a fiber-optic transmitter sends the switch contact state over the fiber-optic cable. In the PMS, the fiber-optic receiver recreates the switch contact state on its discrete output signal to the AC160 rack in the Safety System. Electrical isolation is provided via the fiber-optic connection. There is no metallic path to conduct an electrical fault into the PMS. This type of interface is shown as Case D on Figure 5-1.

Qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by IEEE 603-1991 {Reference 8}).

Functional isolation provided by logic within the PMS prevents this data flow from inhibiting the safety function. First, the functionality associated with these controls is disabled until operation is transferred from the MCR to the RSR. Thus, these controls are disabled, except in the extremely unlikely situation of having to evacuate the MCR. This transfer is accomplished by the divisionalized Class 1E transfer switches, which are connected directly to the bistable processor logic subsystems in each division. Additionally, when the controls are enabled, their functionality is limited to that defined in the PMS functional design because the information transferred is only in the form of discrete digital signals (i.e., there is no computer software-based communication). Specifically, the manual system-level ESF actuators and the manual reactor trip inputs can only initiate safety functions, not inhibit them. The manual system-level blocks are subject to initiation permissives and to automatic removal. The manual system-level resets only remove the system-level actuation signals; they do not cause any components to change state. An additional signal is required to cause a component to change state.

To reduce the chance of the spurious actuation of a function that would require simultaneous operation of dual switches in the MCR, dual switches (each with its own fiber) are also provided for that function in the RSR. Two simultaneous failures would be required to cause a spurious actuation.

Certain PMS test functions are subject to interlocks from non-safety equipment. The purpose of these interlocks is to assure that the plant is properly aligned for the test. The individual hardwired discrete digital signals are classified as non-safety-related and are, therefore, isolated in the PMS cabinets before being used.

Qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by IEEE 603-1991 {Reference 8}) and prevent all but the required data flow from the non-safety equipment to the safety system (providing the communication isolation envisioned by IEEE 7-4.3.2-2003 {Reference 9}, Annex E).

Functional isolation provided by logic within the PMS prevents this data flow from inhibiting the safety function. The functionality associated with these signals only affects the ability to perform tests. The interlocks do not affect automatic or manual safety functions.

Comparing this implementation against the ITAACs:

- 7.a) The PMS provides process signals to the PLS through isolation devices. – This ITAAC is not applicable since the data flow is specified as a non-safety system/equipment to PMS data flow. (Note, however, that electrical, communication, and functional isolation is provided.)
- 7.b) The PMS provides process signals to the DDS through isolation devices. – This ITAAC is not applicable since the data flow is specified as a non-safety system/equipment to PMS data flow. (Note, however, that electrical, communication, and functional isolation is provided.)
- 7.c) Data communication between safety and non-safety systems does not inhibit the performance of the safety function. – This ITAAC is met.
- 7.d) The PMS ensures that the automatic safety function and the Class 1E manual controls both have priority over the non-Class 1E soft controls. – This ITAAC is not applicable to this data flow since the data flow is not used to implement non-Class 1E manual soft controls.
- 7.e) The PMS receives signals from non-safety equipment that provide interlocks for PMS test functions through isolation devices. – This ITAAC is met.

5.2.2 Case E – Non-Safety Control of Safety Components

PLS provides component-level soft controls in the MCR/RSR for most safety components. Additionally, PLS provides automatic control of some safety components for non-safety functions. The non-safety to safety data flows are not implemented using communication links; rather, they are implemented using discrete digital signals. However, to reduce the number of signals (cables) that must be run from the non-safety system to the safety system, the non-safety system's remote I/O capability is used to deliver the signals to the safety system and to accept component status signals from the safety system. Specifically, a remote I/O node from the non-safety system is physically located within each division of the safety system. The remote I/O node is electrically isolated from the non-safety system by the fiber-optic remote I/O bus. The node is powered by the safety system and the portions of the node not performing a safety function are qualified as Associated Class 1E equipment. This type of interface is shown as Case E on Figure 5-1.

The Associated Class 1E equipment, including the Remote Node Controller (RNC), shall meet the requirements of IEEE Std. 384-1981, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits" (Reference 11), Clause 5.5.2 and Clause 5.5.3. Specifically, it shall be part of the safety system qualification program that will demonstrate that when it is subject to environmental, electromagnetic, and seismic stressors, it does not degrade the Class 1E circuits below an acceptable level. The environmental, electromagnetic, and seismic stressors used for these tests are the same as those used to qualify the Class 1E equipment in the same cabinet.

The remote I/O node includes one or more Class 1E CIMs. Internally, these modules contain the equivalent of a discrete digital output module. The resulting discrete digital output signals, corresponding to the demands from the non-safety system, are made available to field programmable gate array (FPGA) based priority logic also contained in the CIM.

The priority logic within the CIM combines the non-safety demands with Class 1E automatic actuation signals and Class 1E manual actuation signals from the PMS subsystem. As applied to the AP1000 design, if either system demands a move to the actuated ("safe") state, the component is moved to the actuated ("safe") state; otherwise, if either system demands a move to the unactuated ("unsafe") state, the component is moved to the unactuated ("unsafe") state.

The CIMs also contain the equivalent of a discrete digital input module. It is used to read component status and internal CIM status. This information is made available to the non-safety system. Thus, at the point of interface to the priority logic, there are two unidirectional data flows: (1) demands going from non-safety to safety and (2) status going from safety to non-safety. Each of these data flows is implemented as simple discrete digital signals, not as a communication link.

As mentioned above, the remote I/O bus that is used to connect the non-safety system to the Associated Class 1E remote node is fiber-optic. This arrangement provides electrical isolation between the safety system and the non-safety system as required by IEEE 603-1991 (Reference 8). The RNC and the communication function within the CIM implement the communications, and only the resulting discrete digital signals interface with the Class 1E priority logic in the CIM. The simple discrete signal interface from the communication function within the CIM to the Class 1E priority logic within the CIM provides the communication isolation envisioned by IEEE 7-4.3.2-2003 (Reference 9), Annex E. Although the remote I/O bus uses bidirectional communications, the simple discrete signal interface between the communication function and the Class 1E priority logic assures that the only data reaching the logic are the intended commands. The priority logic within the CIM provides functional isolation by implementing the priority logic and by only implementing the functionality defined in the PMS functional design. This implementation is shown in Figure 5-3. More information on the CIM is presented in Section 6.

Comparing this implementation against the ITAACs:

- 7.a) The PMS provides process signals to the PLS through isolation devices. – This ITAAC is met for the status information provided to PLS.
- 7.b) The PMS provides process signals to the DDS through isolation devices. – This ITAAC is met for the status information provided to DDS.
- 7.c) Data communication between safety and non-safety systems does not inhibit the performance of the safety function. – This ITAAC is met.
- 7.d) The PMS ensures that the automatic safety function and the Class 1E manual controls both have priority over the non-Class 1E soft controls. – This ITAAC is met.
- 7.e) The PMS receives signals from non-safety equipment that provide interlocks for PMS test functions through isolation devices. – This ITAAC is not applicable to this data flow since the data flow is not used to implement the test interlock function.

a,c



Figure 5-3. Implementation of Case E Data Flow

6 COMPONENT INTERFACE MODULE

The Component Logic System provides actuation, sequencing, monitoring, protection and manual control of various plant components. It also resolves the internal redundancy of the Local Coincidence Logic (LCL) and prioritizes demands from the non-safety system and the safety system.

[

] ^{a,c} Specifically, the CIM is used to combine signals from the PLS soft controls and from the redundant ILPs in the PMS. [

] ^{a,c} Demand signals from the DAS (DAS automatic functions and the DAS manual switches) bypass the CIM and interface to redundant component actuators or redundant inputs to the motor control centers.



Figure 6-1. CIM Functional Overview

[

] ^{a,c}

The CIM module typically arbitrates the component command signals received on two different ports: Port X and Port Y. Port X connects to []^{a,c} the PMS and Port Y connects to the PLS via the Ovation remote I/O bus. As applied to the AP1000 design, if either system demands a move to the actuated (“safe”) state, the component is moved to the actuated state; otherwise, if either system demands a move to the unactuated (“unsafe”) state, the component is moved to the unactuated state.

For the AP1000 design, the automatic and manual system-level actuations are safety functions and are implemented in PMS. Manual component-level actuations are non-safety functions. Manual component-level commands typically originate in PLS, or for a limited number of plant components, in PMS. Once a PMS system-level actuation occurs, the associated plant components move to their actuated (“safe”) state. Upon reset of the PMS system-level actuation, the plant components remain in their actuated state until they are restored to their unactuated (“unsafe”) state by manual component-level commands that originate in PLS or PMS. To support this functionality, the CIM retains the current demanded state of the component.

[

[]^{a,c} The block is removed when there is a drop in Core Makeup Tank levels, low battery charger input voltage upon loss of AC power, MCR/RSR transfer, or operator action. The ADS and IRWST Injection Blocking Device consists only of hardware not subject to software failure modes. [

] ^{a,c}

The CIM supports continuous on-line diagnostics. [

] ^{a,c}

6.1 HARDWARE IMPLEMENTATION

[

] ^{a,c}

6.1.1 [] ^{a,c}

[

] ^{a,c}

6.1.2 Component Interface Module

[

] ^{a,c}

a,c



Figure 6-2. Photograph of CIM Assembly

a,c



Figure 6-3. CIM Block Diagram

6.1.2.1 []^{a,c}

[

] ^{a,c}

6.1.2.2 []^{a,c}

[

] ^{a,c}

6.1.2.3 []^{a,c}

[

] ^{a,c}

6.2 LOGIC IMPLEMENTATION

[

] ^{a,c}

The DAS provides a separate path to actuate the ESF components.

6.3 VALIDATION

[

]^{a,c}

6.4 EQUIPMENT QUALIFICATION

Equipment qualification requirements for AP1000 equipment are specified in APP-GW-GL-700, “AP1000 Design Control Document” (Reference 5) Appendix 3D.

7 MANUAL CONTROL OF SAFETY SYSTEMS AND COMPONENTS

The AP1000 I&C system provides for the manual control of the system-level safety functions and component-level safety functions.

7.1 MANUAL SYSTEM-LEVEL CONTROL

Several mechanisms are provided to initiate the system-level actuation of ESF functions. Once the functions are actuated, the associated plant components move to their actuated (“safe”) state.

Upon removal of the system-level actuation, the plant components remain in their actuated (“safe”) state until they are restored to their unactuated (“unsafe”) state by component-level controls. Controls are also provided for other ESF system-level commands such as blocks and resets.

- PMS Manual ESF System-Level Actuations from the MCR – The normal mechanism to manually actuate the ESF system is to use dedicated switches located in the MCR. Switches are located on the Primary Dedicated Safety Panel and the Secondary Dedicated Safety Panel. The MCR system-level actuation switches are cabled directly from the switches in the MCR to the LCL, located in the bistable coincidence cabinets in each instrument room. These switches are processed by the LCL in each PMS division. The resulting commands then fan out to the ILPs and the CIMs implementing the actuated function.
- PMS Manual ESF System-level Blocks and Resets from the MCR – The normal mechanism to control ESF blocks and resets is to use soft controls located on the divisionalized safety displays in the MCR. The safety displays are located on the Primary Dedicated Safety Panel. These commands are transmitted over the intra-division Common Q network and are processed by the LCL in the PMS division.
- DDS Manual ESF System-Level Actuations from the RSR – In the event of an evacuation of the MCR, the mechanism to actuate the ESF system is to use the non-Class 1E dedicated switches located in the RSR. The signals pass through qualified isolators in the PMS. The isolators provide electrical and communication isolation. These switches are processed by the LCL in each PMS division. Logic in the LCL provides functional isolation. First, the controls are disabled unless operation is transferred to the RSR. Second, the functionality is limited to that defined in the PMS functional design. From the LCL, the commands fan out to the ILPs and the CIMs implementing the actuated function.
- DAS Manual ESF System-Level Actuations from the MCR – In the event of a postulated CMF of the PMS, certain ESF functions can be actuated through diverse means. Dedicated switches for these functions are located on the DAS Panel in the MCR. These switches allow the ESF functions to be actuated through a path independent of the PMS and the DAS automatic actuation logic; for example, through a separate pilot solenoid on air-operated valves, through separate igniters on squib valves, and through separate inputs to the motor control center for motor-operated valves. All switches on the DAS panel are disabled until the DAS panel is enabled by a separate switch in the MCR.

7.2 MANUAL COMPONENT-LEVEL CONTROL

Normal manual component-level control of safety components is provided by the PMS or PLS. PMS component-level control is provided for components that meet any of the following criteria:

- Component actuation could cause a breach in the reactor coolant boundary
- Component actuation could cause an over pressurization of a low pressure system
- Component actuation cannot be reversed from the control room (e.g., squib valves)
- Operator action is required to manipulate controls to maintain safe conditions after the protective actions are completed
- Valves that require jogging

Components meeting these criteria include:

- All Squib Valves
 - PXS-V118A
 - PXS-V118B
 - PXS-V120A
 - PXS-V120B
 - PXS-V123A
 - PXS-V123B
 - PXS-V125A
 - PXS-V125B
 - RCS-V004A
 - RCS-V004B
 - RCS-V004C
 - RCS-V004D
- All ADS Valves (with the exception of those that are normally in their actuated state)
 - RCS-V001A
 - RCS-V001B
 - RCS-V002A
 - RCS-V002B
 - RCS-V003A
 - RCS-V003B
 - RCS-V004A this valve is also listed in the Squib Valve list
 - RCS-V004B this valve is also listed in the Squib Valve list
 - RCS-V004C this valve is also listed in the Squib Valve list
 - RCS-V004D this valve is also listed in the Squib Valve list
 - RCS-V011A

- RCS-V011B
- RCS-V012A
- RCS-V012B
- RCS-V013A
- RCS-V013B

- Head Vent Valves
 - RCS-V150A
 - RCS-V150B
 - RCS-V150C
 - RCS-V150D

- Residual Normal Heat Removal System (RNS) Valves
 - RNS-V001A
 - RNS-V001B
 - RNS-V002A
 - RNS-V002B
 - RNS-V023

For safety components that have normal manual component-level control from PLS:

- PLS Manual ESF Component-Level Control from the MCR – The normal mechanism to control these ESF components at the component-level is to use soft controls from the non-safety workstations located in the MCR. The soft control commands are transferred over the non-safety real-time data network to a non-safety controller. The controller then sends the command to the appropriate CIMs in the PMS via the remote I/O bus. The fiber-optic remote segment of the remote I/O bus provides electrical isolation. The communication function within the RNC and the CIM provide communication isolation. The CIM priority logic function provides functional isolation.
- PLS Manual ESF Component-Level Control from the RSR – In the event of an evacuation of the MCR, the mechanism to control these ESF components at the component-level is to use soft controls from the non-safety workstations located in the RSR. They are implemented in the same manner as described for those in the MCR.
- PLS Manual ESF Component-Level Control from the Equipment Rooms – Safety components that have normal manual component-level control from the PLS can also be controlled at the component-level using dedicated switches located on the CIMs that are part of PMS and are located in the equipment rooms. These switches have priority over other PLS and PMS demands.

The non-safety displays provide the mechanism to access the soft controls by selecting a target area (or poke field) on a display. The means to access and display the soft controls enables the operator to view the associated graphics displays while undertaking control actions. The soft controls provide control of both safety and non-safety systems and components, and provide component actuation and regulation

functions. They are accessible via the video display unit-based workstations on the operator's and supervisor's consoles in the MCR, although the control functionality is normally 'locked-out' at the supervisor's console.

The Ovation platform includes additional security features that provide multiple levels of security. Ovation user accounts will be setup to provide progressive levels of authorization based on user roles (e.g., operator, supervisor, engineer, maintenance, etc.) and the location of the workstation (i.e., main control area, radwaste control area, local plant workstations). The levels of access can be assigned as view only, initiate control actions, acknowledge alarms, changing setpoints, etc. Each role provides a unique level of access determined during the detailed system design and implemented by the security administrator using a graded approach. Group access policies that limit workstation functionality based on the location of the workstation will be assigned to computer accounts. In addition, the Ovation control system resides within the most secure network. Network security measures ensure that while information can be communicated from a secure network workstation to a less secure network workstation, network communication is not possible in the opposite direction. Thereby, a person who has access to a lower security workstation on the local area network cannot access or operate a soft control on any higher security system.

For safety components that have normal manual component-level control from the PMS:

- PMS Manual ESF Component-Level Control from the MCR – The normal mechanism to control these ESF components at the component-level is to use soft controls located on the divisionalized safety displays in the MCR. The soft controls use a multi-step sequence to reduce the chance of spurious actuation. The safety displays are located on the Primary Dedicated Safety Panel. These commands are transmitted over the intra-division Common Q network and are processed by the ILPs in that PMS division.
- PMS Manual ESF Component-Level Control from the Equipment Rooms – In the event of an evacuation of the MCR, the mechanism to control these ESF components at the component-level is to use dedicated maintenance and test switches located on CIMs in the equipment rooms.

8 CONCLUSIONS

This document provides technical information regarding:

1. Data communication between the functional systems that make up the AP1000 I&C system and between the AP1000 I&C system and external systems.
2. The CIM that is used to interface the I&C system to safety system components.
3. The manual control of the safety system at the system-level and the component-level.

Information is included on the data flows between the safety systems and the non-safety systems. The implementations are shown to meet the requirements of IEEE-603-1991 (Reference 8) and IEEE 7-4.3.2-2003 (Reference 9).

Information is included on the CIM that is used to implement non-safety control of safety components. The module is shown to meet the requirements of IEEE-603-1991 (Reference 8) and IEEE 7-4.3.2-2003 (Reference 9).

Information is included on the mechanisms the AP1000 I&C system provides for the manual control of the system-level safety functions and component-level functions. The mechanisms are shown to meet the requirements of IEEE-603-1991 (Reference 8) and IEEE 7-4.3.2-2003 (Reference 9).

Southern Nuclear Operating Company

ND-21-0486

Enclosure 15

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

**Westinghouse Electric Company Application for Withholding Proprietary Information
from Public Disclosure and Accompanying Affidavit CAW-19-4950**

(Enclosure 15 consists of 4 pages, plus this cover page)

AFFIDAVIT

COMMONWEALTH OF PENNSYLVANIA:

COUNTY OF BUTLER:

- (1) I, Zachary S. Harper, have been specifically delegated and authorized to apply for withholding and execute this Affidavit on behalf of Westinghouse Electric Company LLC (Westinghouse).
- (2) I am requesting the proprietary portions of WCAP-16674-P be withheld from public disclosure under 10 CFR 2.390.
- (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 10 CFR 2.390, 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 and is not customarily disclosed to the public.
 - (ii) 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 technical evaluation justifications 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.

AFFIDAVIT

- (5) Westinghouse has policies in place to identify proprietary information. 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.
- (6) The attached documents are bracketed and marked to indicate the bases for withholding. The justification for withholding 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

AFFIDAVIT

refer to the types of information Westinghouse customarily holds in confidence identified in Sections (5)(a) through (f) of this Affidavit.

I declare that the averments of fact set forth in this Affidavit are true and correct to the best of my knowledge, information, and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: 9/26/2019


Zachary S. Harper, Manager
Licensing Engineering

PROPRIETARY INFORMATION NOTICE

Transmitted herewith are proprietary and non-proprietary versions of a document, 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.

Southern Nuclear Operating Company

ND-21-0486

Enclosure 17

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

**WCAP-16675-NP, "AP1000 Protection and Safety Monitoring System Architecture
Technical Report," Revision 10**

[Non-proprietary version of WCAP-16675-P, Revision 10]

(Enclosure 17 consists of 85 pages, plus this cover page)

WCAP-16675-NP
Revision 10
APP-GW-GLR-147
Revision 7

AP1000[®] Protection and Safety Monitoring System
Architecture Technical Report
Nuclear Safety Related

Robert A. Scanlon*, Principal Engineer
Functional & Systems Engineering

September 2020

Reviewers: Richard M. Paese*, Fellow Licensing Engineer
Structural and Mechanical Licensing

William J. Renzelman*, Principal Engineer
Functional & Systems Engineering

Scott A. Faber*, Project Manager
Vogtle AP1000 I&C

Approver: Steven R. Billman*, Manager
Functional & Systems Engineering

This document may contain technical data subject to the export control laws of the United States. In the event that this document does contain such information, the Recipient's acceptance of this document constitutes agreement that this information in document form (or any other medium), including any attachments and exhibits hereto, shall not be exported, released or disclosed to foreign persons whether in the United States or abroad by recipient except in compliance with all U.S. export control regulations. Recipient shall include this notice with any reproduced or excerpted portion of this document or any document derived from, based on, incorporating, using or relying on the information contained in this document.

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

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

© 2020 Westinghouse Electric Company LLC
All Rights Reserved

REVISION HISTORY

RECORD OF CHANGES

Revision	Author	Description
5	Edward P. Schindhelm	For the detailed record of changes for Revision 5, please see the record copy of that revision.
6	Edward P. Schindhelm	For the detailed record of changes for Revision 6, please see the record copy of that revision.
7	Edward P. Schindhelm	For the detailed record of changes for Revision 7, please see the record copy of that revision.
8	Joseph D. Veturis	For the detailed record of changes for Revision 8, please see the record copy of that revision.
9	Robert A. Scanlon	<p>The following proprietary and non-proprietary documents are all aligned at the same design level and are technically equivalent:</p> <ul style="list-style-type: none"> • <u>Proprietary</u> WCAP-16675-P, Rev. 9 APP-GW-GLR-071, Rev. 9 • <u>Non-Proprietary</u> WCAP-16675-NP, Rev. 9 APP-GW-GLR-147, Rev. 6 <p>The following E&DCRs have been incorporated within this revision:</p> <ol style="list-style-type: none"> 1. APP-FSAR-GEF-045 <ol style="list-style-type: none"> a. Removed Table 2-1 b. Removed Figure 2-4 c. Added “WDT Window Watchdog Timer” to List of Acronyms and Definitions d. Updated Reference information and revision numbers, added Reference 40. e. Updated WDT text to clarify “relay” in Section 5.1.6 2. APP-FSAR-GEF-008 <ol style="list-style-type: none"> a. Updated Acronym and meaning of “DVD-ROM” to “DVD” in the List of Acronyms and Abbreviations and Section 5.2. b. Deleted Table 2-2 and Section 2.2.9.3

REVISION HISTORY (cont.)

RECORD OF CHANGES (cont.)

Revision	Author	Description
9 (cont.)		<p>c. Updated “ENABLED” to “ACTIVE” for MTP Function Enable setting in Section 2.2.6.</p> <p>d. Minor text modification in Section 3.1.2.</p> <p>e. Deleted the last bullet for DAS Manual Control in Section 3.4.2.</p> <p>3. APP-FSAR-GEF-019</p> <p>a. Updated List of Acronyms and Abbreviations.</p> <p>b. Updated List of Definitions.</p> <p>4. APP-FSAR-GEF-049 / APP-FSAR-GEF-067</p> <p>a. Modified text in Section 6 and Section 6.2 to clarify that diagnostics combined with on-line tests are used to verify system performance and are supported from the ITP and MTP.</p> <p>Additional updates to Reference revision numbers are made to align with SV0-ISIP-J0R-008, Rev. 7.</p> <p>Minor editorial update to correct spelling of “function” in Section 3.3.2.</p>
10	Robert A. Scanlon	<p>The following proprietary and non-proprietary documents are all aligned at the same design level and are technically equivalent:</p> <ul style="list-style-type: none"> • <u>Proprietary</u> WCAP-16675-P, Rev. 10 APP-GW-GLR-071, Rev. 10 • <u>Non-Proprietary</u> WCAP-16675-NP, Rev. 10 APP-GW-GLR-147, Rev. 7 <p>1. E&DCR APP-FSAR-GEF-169 Rev. 0 has been incorporated within this revision:</p> <p>a. Section 6.2.2: Modified second paragraph to clarify the path that the Trip Bistable Test signals take to be indicated on the MTP and Safety Display.</p> <p>2. RITS68890 has been incorporated to correct typos for WCAP-15927 (incorrectly identified as WCAP-15297) in reference 2</p>

REVISION HISTORY (cont.)

RECORD OF CHANGES (cont.)

10 (cont.)		and reference 40. Additional updates to Reference revision numbers are made to align with SV0-ISIP-JOR-009, Rev. 0.
---------------	--	--

FOREWORD

The AP1000[®] Protection and Safety Monitoring System (PMS) described in this document provides protection against unsafe reactor operation during steady-state and transient power operations. The PMS initiates selected protective functions to mitigate the consequences of design basis events. This document identifies the functional performance requirements and describes the PMS system. The PMS safety system is designed and built to conform to the applicable criteria, codes, and standards concerned with the safe generation of nuclear power.

APP-GW-GL-700, “AP1000 Design Control Document” (DCD) (Reference 1) was written to permit the use of either the Eagle protection system hardware described in the AP600 DCD or the Common Qualified (Common Q[™]) Platform. This document describes the Common Q implementation of the AP1000 PMS. The Common Q Platform is described in WCAP-16097-P-A, “Common Qualified Platform Topical Report” (Reference 2) and WCAP-16097-P-A, Appendix 4, “Common Qualified Platform Integrated Solution” (Reference 3). The Common Q Platform was accepted by the U.S. Nuclear Regulatory Commission (NRC) via the Safety Evaluation Reports in Reference 2.

Section 1 of this document summarizes the AP1000 PMS functional requirements, which received Design Certification, and are compatible with the Common Q hardware and software. Section 2 describes the Common Q architecture for the AP1000 PMS. Section 3 addresses the interfaces and communications between the safety system divisions and between the safety system and non-safety systems. Section 4 describes the Safety Display/Qualified Data Processing System (QDPS) display implementation. Section 5 is a brief description of the Common Q Platform that was described in more detail in References 2 and 3. Section 6 describes the maintenance, test and calibration features of the PMS implementation. Section 7 is the summary and conclusion.

The PMS architecture described in this report is the same as the PMS architecture described in WCAP-16438-P, “FMEA of AP1000 Protection and Safety Monitoring System” (Reference 21).

TABLE OF CONTENTS

REVISION HISTORY ii

RECORD OF CHANGES ii

FOREWORD v

LIST OF TABLES ix

LIST OF FIGURES x

LIST OF ACRONYMS AND ABBREVIATIONS xi

LIST OF TRADEMARKS xii

LIST OF DEFINITIONS xiii

REFERENCES xv

1 AP1000 PMS FUNCTIONAL REQUIREMENTS 1-1

 1.1 REACTOR TRIP FUNCTIONS 1-1

 1.2 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM FUNCTIONS 1-2

 1.3 QUALIFIED DATA PROCESSING SYSTEM FUNCTIONS 1-3

 1.4 COMPONENT CONTROL FUNCTIONS 1-3

2 AP1000 PROTECTION AND SAFETY MONITORING SYSTEM DESCRIPTION 2-1

 2.1 PMS ARCHITECTURE FOUR-DIVISION OVERVIEW 2-1

 2.2 PMS ARCHITECTURE 1 DIVISION DETAIL 2-3

 2.2.1 Nuclear Instrumentation Subsystem 2-4

 2.2.2 Bistable Processor Logic Subsystem 2-8

 2.2.3 Local Coincidence Logic Subsystem 2-12

 2.2.4 Integrated Communications Processor Subsystem 2-17

 2.2.5 Interface and Test Processor Subsystem 2-17

 2.2.6 Maintenance and Test Panel Subsystem 2-19

 2.2.7 Sequence of Events Subsystem 2-22

 2.2.8 Watchdog Timer Implementation 2-22

 2.2.9 Block to Prevent ADS and IRWST Injection Spurious Actuation 2-22

3 EXTERNAL SYSTEM INTERFACES & COMMUNICATIONS 3-1

 3.1 INTRA-DIVISIONAL COMMUNICATIONS VIA AF100 BUS 3-1

 3.1.1 Real-Time Data Distribution 3-1

 3.1.2 Access Control 3-2

 3.2 INTRA-DIVISIONAL AND INTER-DIVISIONAL COMMUNICATIONS VIA HIGH SPEED LINKS 3-2

 3.2.1 Planned Data Exchange 3-2

 3.2.2 Bistable Processor Logic to Local Coincidence Logic Communication 3-3

 3.2.3 Local Coincidence Logic to Integrated Logic Processor Communication 3-3

 3.2.4 Integrated Communication Processor to Integrated Communication Processor Communication 3-3

 3.2.5 Integrated Logic Processor to Safety Remote Node Controller 3-3

TABLE OF CONTENTS (cont.)

3.2.6	Interface and Test Processor to Interface and Test Processor Communication	3-3
3.3	COMMUNICATION BETWEEN SAFETY AND NON-SAFETY EQUIPMENT	3-3
3.3.1	Isolated Sensor Loop Signal to Non-Safety (Case A)	3-4
3.3.2	Isolated Analog and Digital Signals to Non-Safety (Case B).....	3-5
3.3.3	Isolated Unidirectional Datalink Signals to Non-Safety (Case C)	3-5
3.3.4	System-Level Safety Functions from RSR Fixed-Position Switches and Non-Safety Interlock of PMS Test Functions (Case D)	3-8
3.3.5	Non-Safety Control of Safety Components (Case E).....	3-9
3.4	MANUAL CONTROL OF SAFETY SYSTEMS AND COMPONENTS	3-10
3.4.1	Manual System-Level Control.....	3-10
3.4.2	Manual Component-Level Control.....	3-12
3.4.3	Justification for Use of Common Electronics for Manual and Automatic ESF Actuations.....	3-13
4	SAFETY DISPLAY AND QUALIFIED DATA PROCESSING SYSTEM	4-1
4.1	SAFETY DISPLAY FUNCTION	4-1
4.2	QUALIFIED DATA PROCESSING SYSTEM	4-3
5	PLATFORM DESCRIPTION.....	5-1
5.1	HARDWARE.....	5-1
5.1.1	Advant Controller 160 (AC160).....	5-1
5.1.2	S600 Input and Output Modules.....	5-4
5.1.3	Flat Panel Display System.....	5-6
5.1.4	Common Q Power Supply	5-7
5.1.5	Component Interface Module	5-8
5.1.6	I/O Termination Units.....	5-9
5.1.7	Safety Remote Node Controller	5-9
5.1.8	ADS and IRWST Injection Blocking Device	5-10
5.2	SOFTWARE DESCRIPTION	5-10
5.2.1	AMPL Programming Language	5-11
5.2.2	ACC Function Chart Builder	5-11
5.2.3	Configuration Management.....	5-12
5.2.4	Flat Panel Display Software and Tools.....	5-13
6	MAINTENANCE, TESTING AND CALIBRATION.....	6-1
6.1	SELF-DIAGNOSTIC TESTS.....	6-1
6.1.1	Processor and I/O Modules.....	6-1
6.1.2	Communication Modules	6-2
6.2	ON-LINE VERIFICATION TESTS	6-3
6.2.1	Sensor Input Check.....	6-3
6.2.2	Trip Bistable Test.....	6-4
6.2.3	Local Coincidence Logic Test	6-4
6.2.4	Initiation Logic Test.....	6-4
6.2.5	Programmable Logic Controller Execution Test	6-4
6.3	CALIBRATION.....	6-4
6.4	BYPASS AND PARTIAL TRIP CONDITIONS	6-5

TABLE OF CONTENTS (cont.)

	6.4.1	Bypass Condition.....	6-5
	6.4.2	Partial Trip Condition	6-6
7		SUMMARY AND CONCLUSION	7-1

LIST OF TABLES

None

LIST OF FIGURES

Figure 2-1. AP1000 PMS Architecture Four-Division Overview2-2

Figure 2-2. PMS Architecture 1 Division Detail.....2-6

Figure 2-3. Division Redundancy2-10

Figure 3-1. Data Flows between Safety and Non-Safety Equipment3-4

Figure 3-2. Example Implementation of Case C Data Flow3-7

Figure 3-3. Implementation of Case E Data Flow3-11

Figure 4-1. PMS Safety Displays.....4-2

Figure 5-1. AC160 Station5-2

Figure 5-2. PM646A Processor Module5-3

Figure 5-3. S600 I/O Module.....5-5

LIST OF ACRONYMS AND ABBREVIATIONS

Acronyms used in the document are defined in APP-GW-J9Y-001 (WNA-PS-00016-GEN), “Standard Acronyms and Definitions” (Reference 28), or included below to ensure unambiguous understanding of their use within this document.

1oo2	One-out-of-two
1oo3	One-out-of-three
2oo1	Two-out-of-one
2oo2	Two-out-of-two
2oo3	Two-out-of-three
2oo4	Two-out-of-four
ADS	Automatic Depressurization System
CDP	Cyclic Data Packet
Common Q	Common Qualified
CVS	Chemical and Volume Control System
DDS	Data Display and Processing System
DVD	Digital Versatile Disc
Enet	Ethernet
FOR	Fiber-Optic Receiver
Func	Function
I/E	Current-to-Voltage Isolator
Maint	Maintenance
MooN	M-out-of-N (see List of Definitions)
NISPA	Nuclear Instrumentation Signal Processing Assembly
PLS	Plant Control System (AP1000)
PMS	Protection and Safety Monitoring System
QDP	Qualified Data Processing
Qual	Qualified
RNC	Remote Node Controller
RNS	Residual Heat Removal System
SFS	Spent Fuel Pool Cooling System
SRAM	Static Random Access Memory
SRNC	Safety Remote Node Controller
TFT	Thin-Film Transistor
WDT	Window Watchdog Timer

LIST OF TRADEMARKS

Advant, Intel, microGUI, Ovation, Photon, QNX, and Windows are trademarks or registered trademarks of their respective owners. Other names may be trademarks of their respective owners.

AP1000 and Common Q are trademarks or registered trademarks of Westinghouse Electric Company LLC, its affiliates and/or its subsidiaries in the United States of America and may be registered in other countries throughout the world. All rights reserved. Unauthorized use is strictly prohibited. Other names may be trademarks of their respective owners.

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

LIST OF DEFINITIONS

Actuated Equipment:

The assembly of prime movers and driven equipment used to accomplish a protective function (such as solenoids, shutdown rods, and valves) (Reference 1, Section 7.1).

Actuation Device:

A component that directly controls the motive power for actuated equipment (such as circuit breakers, relays, and pilot valves) (Reference 1, Section 7.1).

Channel:

An arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined (IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" {Reference 7, Section 2}).

Component-Level Actuation:

The actuation of a single actuation device (component) (Reference 1, Section 7.1).

Division:

The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components (Reference 7, Section 2).

Fault Tolerant:

Pertaining to a system or component that is able to continue normal operation despite the presence of faults (IEEE Standard 100-2000, "IEEE 100 The Authoritative Dictionary of IEEE Standards Terms Seventh Edition" {Reference 29}).

Hardwired:

A dedicated (non-multiplexed) point-to-point connection between two devices via electrical wires or cables.

MooN:

When generically talking about PMS functions, MooN is used to describe the voting logic where M is the number of channels that are required to be actuated/tripped and N is the number of divisions where the voting logic exists. Therefore, when a channel of a MooN function is bypassed, the logic reverts to Moo(N-1). For example, a 2oo3 function will revert to 2oo2.

LIST OF DEFINITIONS (cont.)

Partial Trip:

The condition during which either redundant half of a protection channel is set to its tripped state. Partial trips are logically ORed into a single channel trip value at the local coincident logic (LCL) before being applied to its respective MooN channel vote.

Protection and Safety Monitoring System:

The aggregate of electrical and mechanical equipment, which senses generating station conditions and generates the signals to actuate reactor trip and engineered safety features, and which provides the equipment necessary to monitor plant safety-related functions during and following designated events (Reference 1, Section 7.1).

Protective Function:

Any one of the functions necessary to mitigate the consequences of a design basis event. Protective functions are initiated by the Protection and Safety Monitoring System logic and will be accomplished by the trip and actuation subsystems. Examples of protective functions are reactor trip and engineered safety features (such as valve alignment and containment isolation) (Reference 1, Section 7.1).

Safety System:

The aggregate of electrical and mechanical equipment necessary to mitigate the consequences of design basis events (Reference 1, Section 7.1).

System-Level Actuation:

The actuation of a sufficient number of actuation devices to affect a protective function (Reference 1, Section 7.1).

REFERENCES

1. APP-GW-GL-700, Rev. 19, "AP1000 Design Control Document," Westinghouse Electric Company LLC.
2. WCAP-16097-P-A (Proprietary), Rev. 3, "Common Qualified Platform Topical Report," (as modified by the Topical Report alternatives in WCAP-15927, Rev. 8), Westinghouse Electric Company LLC.
3. WCAP-16097-P-A (Proprietary), Appendix 4, Rev. 0, "Common Qualified Platform Integrated Solution," Westinghouse Electric Company LLC.
4. Deleted.
5. Deleted.
6. Deleted.
7. IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Inc., 1991.
8. WCAP-15776 (Non-Proprietary), Rev. 0, "Safety Criteria for the AP1000 Instrumentation and Control Systems," Westinghouse Electric Company LLC.
9. APP-PMS-J1-001, Rev. 18, "AP1000 Protection and Safety Monitoring System Functional Requirements," Westinghouse Electric Company LLC.
10. Deleted.
11. Deleted.
12. Deleted.
13. Deleted.
14. Deleted.
15. Deleted.
16. Deleted.
17. Deleted.
18. Deleted.
19. Deleted.

REFERENCES (cont.)

20. Deleted.
21. WCAP-16438-P (Proprietary), Rev. 9, "FMEA of AP1000 Protection and Safety Monitoring System," Westinghouse Electric Company LLC.
22. Regulatory Guide 1.97, Rev. 3, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident," U.S. Nuclear Regulatory Commission, May 1983.
23. IEEE Standard 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Inc., 2003.
24. IEEE Standard 384-1981, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuit," Institute of Electrical and Electronics Engineers, Inc., 1981.
25. IEEE Standard 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Inc., 1998.
26. NUREG-0800, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Section 9.5.1, "Fire Protection Program," U.S. Nuclear Regulatory Commission, July 1981.
27. Regulatory Guide 1.62, Rev. 0, "Manual Initiation of Protective Actions," U.S. Nuclear Regulatory Commission, October 1973.
28. APP-GW-J9Y-001, Rev. 3 (WNA-PS-00016-GEN, Rev. 8), "Standard Acronyms and Definitions," Westinghouse Electric Company LLC.
29. IEEE Standard 100-2000, "IEEE 100 The Authoritative Dictionary of IEEE Standards Terms Seventh Edition," Institute of Electrical and Electronics Engineers, Inc., 2000.
30. WCAP-16674-P (Proprietary), Rev. 9, "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components," Westinghouse Electric Company LLC.
31. WCAP-16096-P-A (Proprietary), Rev. 4, "Software Program Manual for Common Q Systems," Westinghouse Electric Company LLC.
32. Deleted.
33. WCAP-17179-P (Proprietary), Rev. 6, "AP1000 Component Interface Module Technical Report," Westinghouse Electric Company LLC.

REFERENCES (cont.)

- 34. APP-PMS-J3-300, Rev. 18, "AP1000 Detailed Functional Diagram Index," Westinghouse Electric Company LLC.
- 35. WCAP-15775, Rev. 8, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report," Westinghouse Electric Company LLC.
- 36. Regulatory Guide 1.47, Rev. 0, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," U.S. Nuclear Regulatory Commission, May 1973.
- 37. APP-PMS-J1-102, Rev. 10, "AP1000 Functional Diagram Reactor Trip Functions," Westinghouse Electric Company LLC.
- 38. APP-PMS-J3-303, Rev. 5, "AP1000 Detailed Functional Diagram Reactor Trip Division A," Westinghouse Electric Company LLC.
- 39. APP-PMS-J1-101, Rev. 24, "AP1000 Functional Diagrams Index and Symbols," Westinghouse Electric Company LLC.
- 40. WCAP-15927, Rev. 8, "Design Process for AP1000 Common Q Safety Systems," Westinghouse Electric Company LLC.

1 AP1000 PMS FUNCTIONAL REQUIREMENTS

The Protection and Safety Monitoring System (PMS) performs the reactor trip (RT) functions, the engineered safety features (ESF) actuation functions, and the Qualified Data Processing System (QDPS) functions.

During normal operation, administrative procedures and plant control systems serve to maintain the reactor in a safe state, preventing damage to the three barriers (fuel clad, reactor coolant system, and reactor containment building) that prevent the spread of radioactive material to the environment. Accident conditions causing one or more of the barriers to be threatened can occur. The PMS monitors key plant parameters and automatically initiates various protective functions to prevent violation of any of the three barriers, or if violation of a barrier cannot be prevented, to maintain the integrity of the remaining barriers. This ensures that, given a design basis event, the site boundary radiation releases will be below U.S. Nuclear Regulatory Commission (NRC) limits. The system performs its functions by actuating a variety of equipment and by monitoring the plant process using a variety of sensors and operations performing calculations, comparisons, and logic based on those sensor inputs. The PMS functional requirement documents discuss the protective functions that are performed and the requirements these functions place on the equipment that performs them.

1.1 REACTOR TRIP FUNCTIONS

The PMS generates an automatic reactor trip for the following conditions (APP-PMS-J1-102, "AP1000 Functional Diagram Reactor Trip Functions," Reference 37 and APP-PMS-J3-303, "AP1000 Detailed Functional Diagram Reactor Trip Division A," Reference 38):

1. Source Range High Neutron Flux.
2. Intermediate Range High Neutron Flux.
3. Power Range High Neutron Flux Low Setpoint.
4. Power Range High Neutron Flux High Setpoint.
5. Power Range High Positive Flux Rate.
6. Overtemperature Delta-T.
7. Overpower Delta-T.
8. Pressurizer Low-2 Pressure.
9. Low-2 Reactor Coolant Flow in 1/2 Loops.
10. Reactor Coolant Pump Low-2 Speed.
11. High-2 Reactor Coolant Pump Bearing Water Temperature in 1/4 Pumps.
12. Pressurizer High-2 Pressure.
13. High-3 Pressurizer Water Level.
14. Steam Generator 1 Water Level Low-2.
15. Steam Generator 2 Water Level Low-2.
16. Steam Generator 1 Water Level High-3.
17. Steam Generator 2 Water Level High-3.
18. Automatic Depressurization Systems (ADS) Actuation.
19. Core Makeup Tank (CMT) Injection Actuation.
20. Safeguards Actuation.
21. Passive Residual Heat Removal (PRHR) Actuation.

1.2 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM FUNCTIONS

AP1000® provides instrumentation and controls to sense accident situations and initiate engineered safety features (ESF). The occurrence of a limiting fault, such as a loss of coolant accident or a secondary system break, requires a reactor trip plus actuation of one or more of the engineered safety features. This combination of events prevents or mitigates damage to the core and reactor coolant system components, and provides containment integrity.

The PMS is actuated when safety system setpoints are reached for selected plant parameters. The selected combination of process parameter setpoint violations is indicative of primary or secondary system boundary challenges. Once the required logic combination is generated, the PMS equipment sends the signals to actuate appropriate ESF components.

The following is a list of the ESF system-level actuations initiated by the PMS (APP-PMS-J3-300, “AP1000 Detailed Functional Diagram Index,” Reference 34 and APP-PMS-J1-101, “AP1000 Functional Diagrams Index and Symbols,” Reference 39):¹

1. Safeguards Actuation.
2. Containment Isolation.
3. In-Containment Refueling Water Storage Tank (IRWST) Injection.
4. CMT Injection Actuation.
5. ADS Actuation (Stages 1-3 and Stage 4).
6. Reactor Coolant Pump Trip.
7. Main Feedwater Isolation.
8. PRHR Actuation.
9. Turbine Trip.
10. Containment Recirculation.
11. Steam Line Isolation.
12. Steam Generator Blowdown Isolation.
13. Passive Containment Cooling Actuation.
14. Startup Feedwater Isolation.
15. Boron Dilution Block.
16. Chemical and Volume Control System (CVS) Makeup Isolation.
17. Block Steam Dump.
18. Main Control Room Isolation, Air Supply Initiation, and Electrical load De-energization.
19. Auxiliary Spray, Purification Line, and Zinc/Hydrogen Addition Isolation.
20. Containment Air Filtration Isolation.
21. Refueling Cavity and Spent Fuel Pool Cooling System (SFS) Isolation.
22. CVS Letdown Isolation.
23. Pressurizer Heater Breakers Trip.
24. Steam Generator Relief Isolation.
25. Normal Residual Heat Removal Containment Isolation.
26. Containment Vacuum Relief Actuation.

1. References 34 and 39 are index sheets providing pointers to the functional logic diagrams.

1.3 QUALIFIED DATA PROCESSING SYSTEM FUNCTIONS

The AP1000 processing and display function is performed by equipment that is part of the PMS, Plant Control System (PLS), and the Data Display and Processing System (DDS).

The PMS provides signal conditioning, communications, and display functions for Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident" (Reference 22), Category 1 variables and for Category 2 variables that are energized from the Class 1E direct current (DC) uninterruptible power supply system. The PLS and the DDS provide signal conditioning, communications, and display functions for Category 3 variables and for Category 2 variables that are energized from the non-Class 1E DC uninterruptible power system. The DDS also provides an alternate display of the variables, which are displayed by the PMS. Electrical separation of the DDS and the PMS is maintained through the use of isolation devices in the interconnections between the two systems.

The portion of the PMS that is dedicated to providing the post-accident monitoring data for the safety-related displays located in the Main Control Room (MCR) is referred to as the Qualified Data Processing System (QDPS). The QDPS function is provided by a redundant configuration of Qualified Data Processing (QDP) cabinets and qualified displays.

The QDPS performs the following functions:

- Provides safety-related data processing.
- Provides the operator with sufficient operational data to support post-accident monitoring in the event of a failure of the other display systems.
- Provide data to the Real-Time Data Network for use by other systems in the plant, via the intra-divisional AF100 bus, MTP, and the Advant[®] Ovation[®] Interface (AOI) gateway.
- Processes data for MCR display, and to meet Regulatory Guide 1.97 (Reference 22) requirements.

1.4 COMPONENT CONTROL FUNCTIONS

Control of individual safety-related components that perform Class 1E functions is provided. Component control consists of the following functions:

1. Resolution of multiple demands for a given component from various systems
2. Application of manual component demands
3. Performance of the component protection logic (torque limit, anti-pump latch, etc.)
4. Reporting of component status to the plant information system
5. Local component control

The inputs required for control of individual components are:

1. System-level actuation commands from the reactor trip and ESF actuation logic.
2. System-level actuation commands from the fixed-position switches in the MCR and remote shutdown room (RSR).
3. Individual safety component control commands from the non-safety PLS for component actuations with no onerous consequences, with the exception of several normal residual heat removal system (RNS) isolation valves (for test, maintenance, restoration, and non-credited actuations).
4. Individual safety component control commands from the safety displays in the MCR for component actuations with onerous consequences and RNS Isolation.
5. Component feedback signals from the individual safety components.

The outputs to individual components consist of hardwired control signals to open or close a solenoid valve, air-operated valve, pneumatic-hydraulic valve, motor-operated valve, squib valve, or circuit breaker.

2 AP1000 PROTECTION AND SAFETY MONITORING SYSTEM DESCRIPTION

The PMS 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 PMS controls safety-related components in the plant that are operated from the MCR or remote shutdown workstation.

In addition, the PMS provides the equipment necessary to monitor the plant’s safety-related functions during and following an accident as required by Regulatory Guide 1.97 (Reference 22).

2.1 PMS ARCHITECTURE FOUR-DIVISION OVERVIEW

The AP1000 PMS consists of four redundant divisions, designated A, B, C, and D, as depicted on Figure 2-1. The PMS performs the necessary safety-related signal acquisition, calculations, setpoint comparison, coincidence logic, reactor trip/ESF actuation functions, and component control functions to achieve and maintain the plant in a safe shutdown condition. The PMS also contains maintenance and test functions to verify proper operation of the system. The PMS includes four redundant safety displays, one for each division, located on the Primary Dedicated Safety Panel (PDSP) in the MCR. Four redundant divisions are provided to satisfy single failure criteria and improve plant availability.

[

•

•

•

]a,c

WCAP-16097-P-A, “Common Qualified Platform Topical Report” and WCAP-16097-P-A, Appendix 4, “Common Qualified Platform Integrated Solution” (References 2 and 3) describe the Common Qualified (Common Q™) hardware platform, which comprises the PMS configuration for the AP1000. The Common Q Platform, described in References 2 and 3, was accepted by the NRC via the Safety Evaluation Reports in Reference 2.



a,c

Figure 2-1. AP1000 PMS Architecture Four-Division Overview

The Instrumentation and Control (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 (2oo3) logic from a two-out-of-four (2oo4) logic.

Four redundant measurements, using four separate sensors, are made for each variable used for reactor trip. One measurement is processed by each division. Analog signals are converted to digital form by analog-to-digital converters (ADCs) within the division's BPLs. Signal conditioning is applied to selected inputs following the conversion to digital form. Following necessary calculations and processing, the measurements are compared against the applicable setpoint for that variable. A partial trip signal for a parameter is generated if the channel's measurement exceeds its predetermined or calculated limit. Processing of variables for reactor trip is identical in each of the four redundant divisions of the protection system. [

] ^{a,c} The LCLs in each division are capable of generating a reactor trip signal if two or more of the redundant channels for a single variable are in the partial trip state.

The reactor trip signal from each of the four divisions of the PMS is sent to that division's reactor trip circuit breakers (RTCBs).

Each division controls two RTCBs. The reactor is tripped when two or more actuation divisions output a reactor trip signal opening their breakers. This automatic trip demand signal initiates the following two actions. It de-energizes the undervoltage (UV) trip attachments on the RTCBs, and it energizes the shunt trip (ST) devices on the RTCBs. Either action causes the breakers to trip. Opening the appropriate trip breakers in two or more divisions removes power to the rod drive mechanism coils, allowing the rods to fall into the core. This rapid negative reactivity insertion causes the reactor to shut down.

Bypass of a protection channel that generates a reactor trip signal is permitted because the single failure criterion is met even when one channel/division is bypassed. Bypassing two or more redundant channels/divisions is not allowed and is handled via the design.

2.2 PMS ARCHITECTURE 1 DIVISION DETAIL

Figure 2-2 is a block diagram illustrating one division of the PMS subsystems for the Common Q architecture. Each division of the PMS contains the following major subsystems:

- [
- 1.
 - 2.
 - 3.

] ^{a,c}

- [
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.

] ^{a,c}

The PMS subsystems contain the necessary equipment to perform the following functions:

- [
-
-
-
-
-
-
-
-

] ^{a,c}

2.2.1 Nuclear Instrumentation Subsystem

- [
-
-] ^{a,c}

In each division, the neutron flux is monitored with three detector ranges: Source Range (SR), Intermediate Range (IR), and Power Range (PR). The signals derived from these detectors provide an indication of reactor power from approximately 10E-9 to 200 percent. The detector signals are processed by preamplifiers (SR and IR) and the Nuclear Instrumentation Signal Processing Assembly (NISPA), and are used to provide nuclear startup and overpower protection. The IR is capable of measuring reactor power to 200 percent for PAMs purposes only.

Three types of neutron detectors are used to monitor the leakage neutron flux from a complete shutdown condition to 120 percent of full power. Detector types for these three ranges are:

- SR – BF3 proportional counter
- IR – fission chamber
- PR – uncompensated ion chamber

The SR channel covers six decades of leakage neutron flux. The lowest observed count rate depends on the strength of the neutron sources in the core and the core multiplication associated with shutdown reactivity. This generally is greater than two counts per second. The IR channel covers eight decades. IR detectors and instrumentation are chosen to provide overlap between the higher portion of the SR and the lower portion of the PR channels. The PR covers approximately two decades of the total instrument range. This is a linear range that overlaps the higher portion of the IR. The neutron detectors are installed in tubes located around the reactor vessel in the primary shield. The NI subsystem consists of the following hardware:

- SR detector, IR detector, and PR upper and lower detectors
- SR and IR preamplifiers
- NI system cabinet
- Field wiring, junction boxes, and containment penetrations

[

]a,c

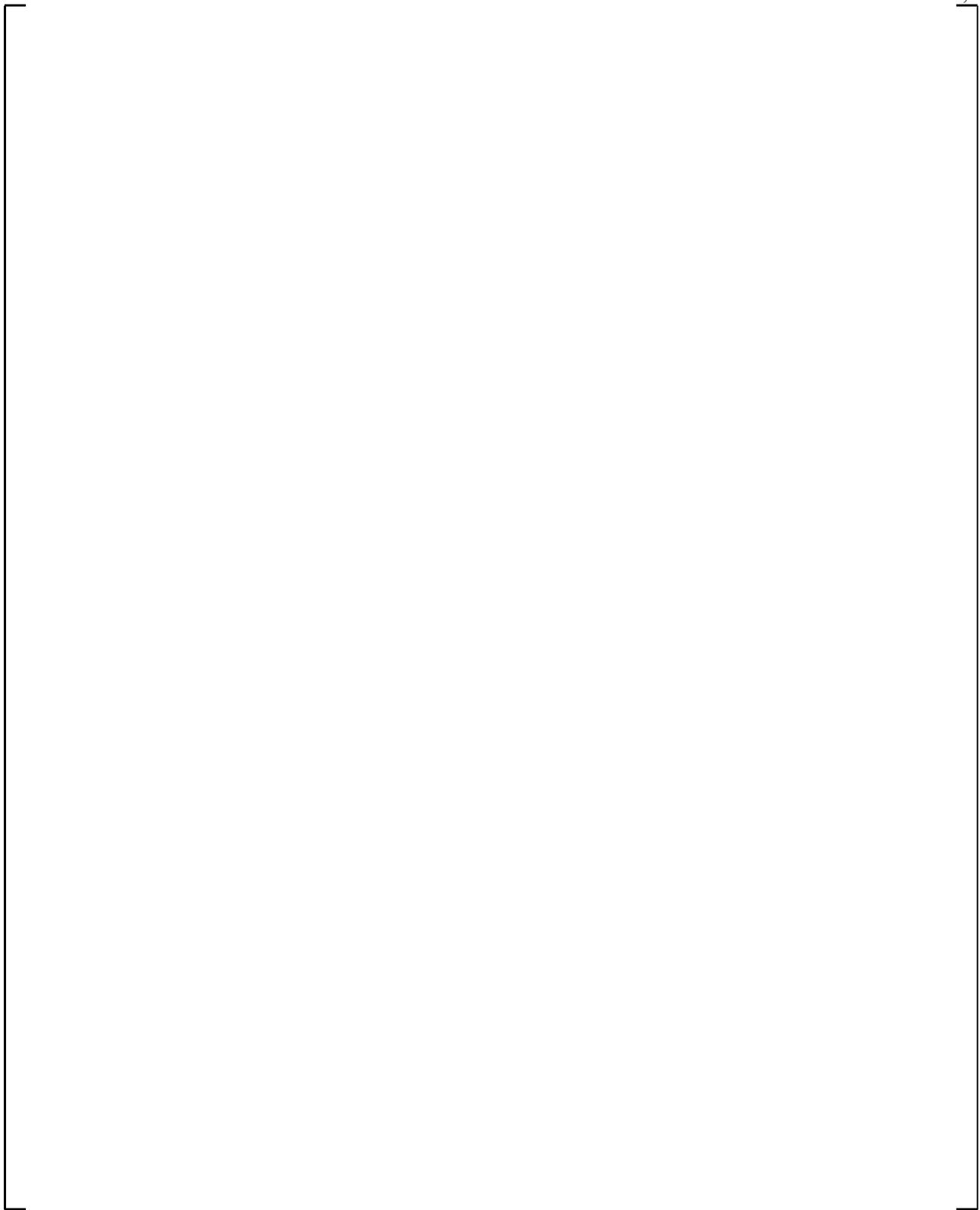


Figure 2-2. PMS Architecture 1 Division Detail

2.2.1.1 Neutron Detectors

2.2.1.1.1 Source Range Detector

The SR detector is used for startup and operation at very low reactor powers. High-voltage power to the SR detector is removed when the reactor is operating above the P10 permissive.

2.2.1.1.2 Intermediate Range Detector

The IR detector overlaps the operating range of the SR and PR channels.

2.2.1.1.3 Power Range Detector

The PR detectors provide the most accurate indication of reactor power over the range of 0.5 percent to 120 percent power. The PR channel is calibrated periodically at the current operating power level against calorimetric power.

2.2.1.2 Preamplifiers

2.2.1.2.1 Source Range Preamplifier

The SR preamplifier is located on a wall outside containment and receives the signal from the SR detector. The low-level signal is amplified and transmitted to the Nuclear Instrumentation Subsystem (NIS) by the SR preamplifier. The SR preamplifier receives its operating power from the NIS cabinet power supply. The SR preamplifier transmits its output signal to the NIS cabinet by multi-conductor cable. The SR preamplifier contains embedded test circuitry that can be remotely activated from the MTP.

2.2.1.2.2 Intermediate Range Preamplifier

The IR preamplifier is located on a wall outside containment and receives the signal from the IR detector. The low-level signal is amplified and transmitted to the NIS by the IR preamplifier. The IR preamplifier receives its operating power from the NIS cabinet power supply. The IR preamplifier transmits its output signal to the NIS cabinet by fiber-optic cables. The IR preamplifier contains embedded test circuitry that can be remotely activated from the MTP.

2.2.1.3 Nuclear Instrumentation Subsystem Cabinet

[

]a,c

[

] ^{a,c} The SR high-voltage power supply can be de-energized to prevent damage to the SR detector when reactor power exceeds the upper limit of the SR detector.

NIS signal processing and algorithms are performed by redundant BPL subracks in redundant BCCs. The Common Q hardware is described in References 2 and 3.

The NIS power supplies receive vital bus power and generate various DC voltages for use within the cabinet.

2.2.2 Bistable Processor Logic Subsystem

The PMS subsystems require data from field sensors and manual inputs (such as system-level blocks and resets) from the MCR to perform the protective function calculations. The results of the calculations drive the corresponding partial trip inputs of the reactor trip and ESF coincidence logic.

[

] ^{a,c} The description provided below illustrates the operation of one of the four identical divisions.

[

] ^{a,c}

The following description of the BPL subsystem applies equally to BPL-A1 and its redundant counterpart BPL-A2.

[

] ^{a,c}

[

]a,c

a,c

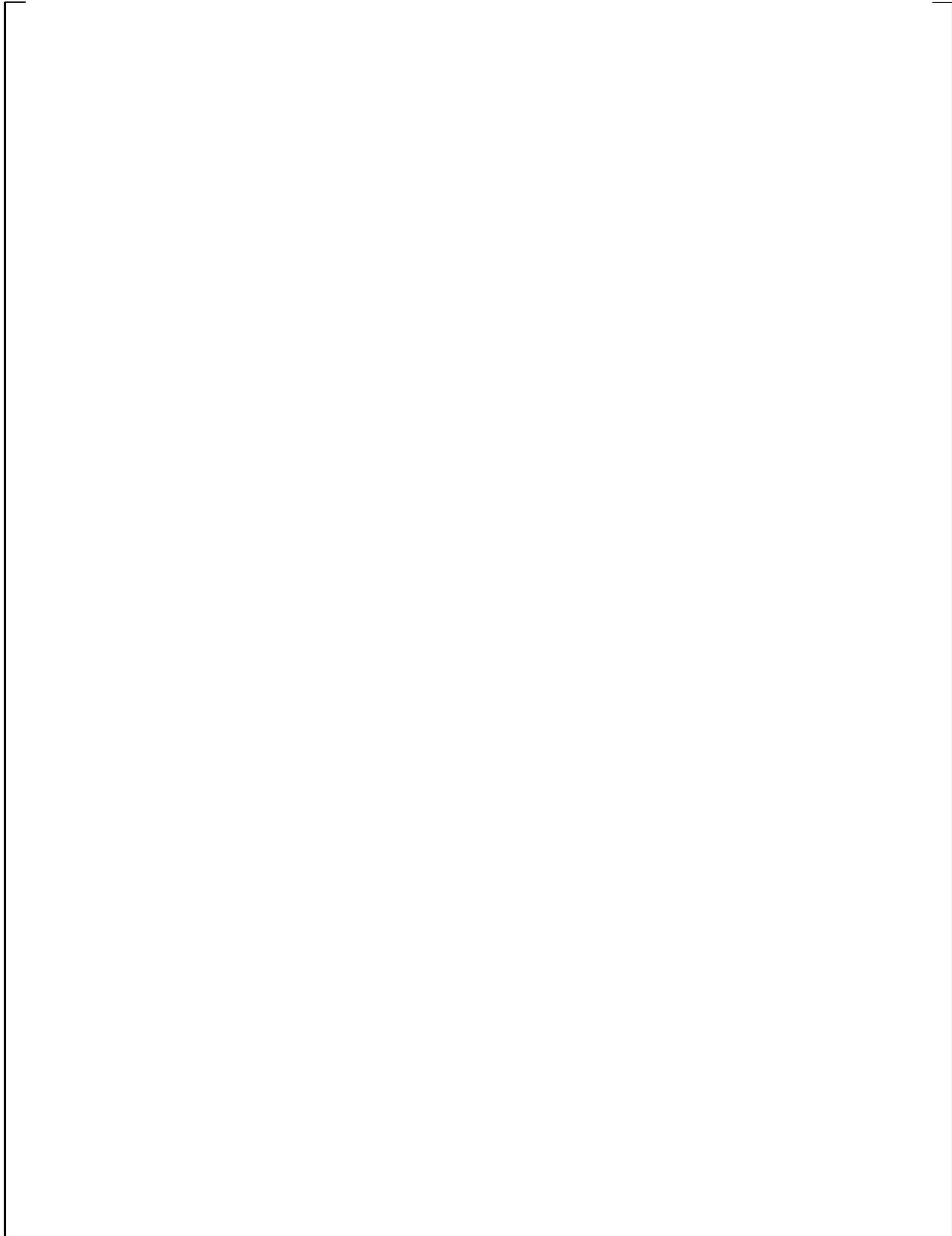


Figure 2-3. Division Redundancy

2.2.2.1 BPL Analog Inputs

The BPL subsystem interfaces with the process signals that measure the plant process parameters necessary to generate a reactor trip or ESF actuation and with the signals from the ex-core nuclear instrumentation. Analog input modules acquire the analog process signal information. Process signals are generally 4 to 20 mA or 0 to 10 VDC, and are obtained from the channel-specific process transmitters. Other inputs include SR, IR, and PR nuclear instrumentation power level signals, RCP speed pulse signals, and resistance temperature detector (RTD) inputs for temperature measurement.

2.2.2.2 BPL Digital Inputs

Digital input modules acquire the contact input signals from field sensors.

2.2.2.3 BPL Processing Module

The BPL processor modules (PMs) perform all pressure, temperature, level, flow, speed, and NI algorithms and compare the results to predefined limits. A partial reactor trip or ESF actuation signal is generated if the setpoint is reached. [

]a,c

2.2.2.4 BPL Analog Outputs

[

]a,c

2.2.2.5 BPL Digital Outputs

[

]a,c

2.2.2.6 BPL Communication

[

]a,c

2.2.2.7 BPL Cross-Division Communication

[

]a,c

[

] ^{a,c}

2.2.3 Local Coincidence Logic Subsystem

[

] ^{a,c}

The LCL subsystem acts to initiate a reactor trip or ESF actuation when a pre-determined condition in 2oo4 independent safety divisions reaches a partial trip or partial actuation state. The LCL also provides for the bypass of trip or actuation functions to accommodate periodic tests and maintenance. The LCL subsystem performs two primary functions:

1. The reactor trip coincidence logic performs the logic to combine the partial trip signals from the BPL subsystems and generates a fault tolerant trip output signal to the reactor trip switchgear and initiation logic.
2. The ESF coincidence logic performs the logic to combine the partial actuation signals from the BPL subsystems along with permissives, blocks, and resets to generate a fault tolerant actuation output signal to the ILP subsystems.

[

] ^{a,c}

2.2.3.1 Reactor Trip Coincidence Logic

[

] ^{a,c}

[

] ^{a,c} De-energizing the associated RTCB UV coil or energizing the RTCB ST coil forces the associated RTCB to open.

[

] ^{a,c}

2.2.3.1.1 Reactor Trip Initiation Logic

[

] ^{a,c}

[

]a,c

2.2.3.1.2 Reactor Trip Circuit Breakers

The RTCBs are used to initiate reactor shutdown. The RTCBs connect the electrical motive power, supplied from motor generator sets, to the rod control system. The rod control system holds the control rods in position as long as electrical power is available. When the PMS senses that established limits for safe operation of the plant have been, or are about to be, exceeded, a command is generated to de-energize the UV trip device and energize the ST device in the RTCBs. This opens the breakers, disconnecting the power to the rod control system. When power is removed, the control rods drop by gravity into the reactor core, initiating the shutdown process.

[

]a,c

2.2.3.1.3 Manual Reactor Trip

A manual reactor trip is an entirely hardware based function that is initiated from the MCR by redundant momentary switches. The switches interrupt the power from the voting logic, de-energizing the UV

interposing relays and trip attachments, and energizing the ST trip attachments in all four divisions. Figure 2-3 illustrates a simplified version of the implementation of the manual reactor trip function.

2.2.3.1.4 Availability

[

] ^{a,c}

2.2.3.2 Engineered Safety Features Coincidence Logic

The ESF subsystem performs two primary functions:

1. The ESF coincidence logic function performs system-level logic calculations, such as actuation of the passive residual heat removal system. It receives inputs from the BPL subsystems, the MCR and RSR fixed-position switches.
2. The ESF component control function consists of the ILPs, which perform the component fan-out for each ESF system-level actuation, and component interface modules (CIMs) that provide the capability for on/off control of individual safety-related plant components. The CIMs receive inputs from the ILPs and from the plant control system (PLS).

2.2.3.2.1 ESF Coincidence Logic Function

[

] ^{a,c} The primary functions of the ESF logic processors are to process inputs, calculate system-level actuation, combine the automatic and manual system level actuations and manual bypass data, and transmit the data to the ILPs. To perform the ESF coincidence logic calculations, the ESF processors require data from the BPL subsystems, and also use manual inputs (such as system-level blocks and resets) from the MCR and the remote shutdown workstation.

The ESF logic processors perform the following functions:

- Receive bistable data supplied by the four divisions of BPL subsystems and perform 2oo4 voting on this data.

- Implement system-level logic and transmit the output to the ILP processors for ESF component fan-out and actuation.
- Process manual system-level actuation commands received from the MCR and RSR.

Figure 2-3 illustrates the interconnection of BPL subsystems to ESF logic processors for the Common Q architecture.

2.2.3.2.2 Engineered Safety Features Component Control Function

The ESF component control function is implemented with redundant ILPs and CIMs that provide a distributed interface between the safety system and the plant operator for control of non-modulating safety-related plant components. Non-modulating control relates to the opening or closing of solenoid valves and solenoid pilot valves, and the opening or closing of motor-operated valves and dampers. The ESF component control function implements criteria established by the fluid systems designers for permissive and interlock logic applied to the component actuations. It also provides the plant operator with information on the equipment status, such as indication of component position (full closed, full open, valve moving), component control modes (manual, automatic, local, remote), or abnormal operating condition (power not available, failure detected).

[

]a,c

Figure 2-3 illustrates the communication between the ESF coincidence logic and the ESF control logic for the Common Q architecture.

2.2.4 Integrated Communications Processor Subsystem

[]^{a,c} The divisions are physically separated and electrically isolated from each other. The following description illustrates the operation of one of the four identical divisions.

[

] ^{a,c}

The data sent to the other PMS divisions and the data received from the other PMS divisions is used only by the QDPS for display in the MCR to meet Regulatory Guide 1.97 (Reference 22) Post-Accident Monitoring System requirements and for diagnostic purposes. This data is not used for any reactor trip or ESF actuation function.

[

] ^{a,c}

2.2.5 Interface and Test Processor Subsystem

[]^{a,c} The divisions are physically separated and electrically isolated from each other. The following description illustrates the operation of one of the four identical divisions.

[

] ^{a,c}

[

]a,c

[

]a,c

2.2.6 Maintenance and Test Panel Subsystem

[

]a,c The following description illustrates the operation of one of the four identical divisions.

The MTP provides the human-interface to the safety system and is used for maintenance and test functions. The MTP provides the means for the technician to perform the following functions:

[

-

]a,c

[

-
-
-
-
-
-
-
-

] ^{a,c}

Within each division of the safety system, one Flat Panel Display System, the MTP, provides access to calibration data, surveillance testing, establishment of conditions (surveillance test conditions, calibrations, functional bypass, etc.), and functional software modifications. The MTP is contained in the Maintenance and Test Cabinet (MTC) which is located in the I&C equipment room. A Function Enable keyswitch on the MTP must be set to the ‘ACTIVE’ position prior to any operation that may take a safety function out of service or change the status of a safety function (e.g., surveillance test conditions, calibrations, functional bypass, etc.). When the Function Enable keyswitch is enabled, a visual alarm is generated on the Safety Display in the MCR. When the Function Enable keyswitch is disabled, all surveillance test conditions are removed and all external inputs to the Safety System functions are restored.

Each MTP consists of a touch screen video display and a PC Node Box, as depicted in Figure 2-2. The MTP is described in References 2 and 3 and was accepted by the NRC via the Safety Evaluation Reports in Reference 2.

[

] ^{a,c}

The MTP also has non-volatile memory used for storing setpoints, calibration constants, and maintenance information to support system “warm” starts.

The MTP provides an interface between the safety and the non-safety systems, allowing data to be passed from the safety system to the non-safety system Real-Time Data Network.

2.2.6.1 Setpoint and Calibration Constant Changes

[

] ^{a,c}

2.2.6.2 Program Changes

The AC160 is designed to load software in two ways. One way is to program the AC160 over the AF100 bus. Even though this network and the only programming source (the MTP) are totally contained within a division of the PMS, this mode of programming is prevented. This is accomplished by using the AC160 Function Chart Builder tool to configure the equipment to not accept AF100 bus programming.

The other way to load software is by a serial connection between the division's MTP and the AC160 Class 1E PMs. Within a division, a cable is routed from the MTC to each cabinet containing a Class 1E PM646A. This configuration allows for software loading to any Class 1E PM within a division from the MTP. The software loading cable is normally disconnected on each end.

[

] ^{a,c}

To perform a software update, the cable (coming from the cabinet containing the target PM) in the MTC is connected to the MTP. The opposite end of the software loading cable is connected to the target AC160 PM646A and the software update is performed from the MTP. The cable is alternately connected to each PM in the cabinet requiring a software update. Upon completion of all software updates in the cabinet, both sides of the software download cable are disconnected. With the exception of the non-Class 1E (sequence of events) SOE subsystem, this process is repeated for each cabinet containing a PM requiring an update. To maintain independence, the SOE PMs are not loaded from the MTP, but from a separate laptop.

2.2.6.3 Interface to Plant Control System

[

] ^{a,c}

2.2.7 Sequence of Events Subsystem

The PMS BPL and LCL subsystems provide SOE points to the PLS for SOE recording. [

]a,c

2.2.8 Watchdog Timer Implementation

[

]a,c

2.2.9 Block to Prevent ADS and IRWST Injection Spurious Actuation

[

]a,c

[

]a,c

2.2.9.1 Independence

[

] ^{a,c}

2.2.9.2 Clearing of the ADS and IRWST Injection Block

[

] ^{a,c}

3 EXTERNAL SYSTEM INTERFACES & COMMUNICATIONS

Communication within the safety system consists primarily of the four intra-divisional safety communication networks and safety datalink interfaces. A summary of the safety-to-non-safety system communications is provided in this report. A more detailed description of safety-to-non-safety system communications is provided in WCAP-16674-P, “AP1000 I&C Data Communication and Manual Control of Safety Systems and Components” (Reference 30).

3.1 INTRA-DIVISIONAL COMMUNICATIONS VIA AF100 BUS

Within each PMS division, the intra-divisional AF100 bus provides the means to exchange data between the Class 1E cabinets within the division, including data that has been received from external systems. This bus is part of the Westinghouse Common Q platform (see References 2 and 3) and is referred to as the Common Q network. The AF100 is a high-performance, deterministic communication bus, intended for communication between AC160 Controllers and Flat Panel Display Systems within the same division. The AF100 bus is not used for reactor trip or ESF actuation. The transmission rate is 1.5 Mbit/second or faster. The network provides real-time data distribution of data within a division. Real-time data distribution is defined as the scheduled periodic broadcast of real-time data pertaining to the plant processes. On the AF100 bus, real-time data distribution is referred to as process data transfer. [

]a,c

The AF100 process data transfer is a deterministic protocol which has priority over the non-deterministic message transfers. Message transfers are used for such off-line functions as interrogating the Programmable Logic Controller (PLC) internal error buffer. Such message transfers are non-deterministic such that their interruption by process data transfers has no significant impact on the system. [

]a,c

An AF100 bus is totally contained within each division of the Safety System. The physical extent of each AF100 bus is limited to its corresponding I&C equipment room, the MCR, and the raceways between the two. On-site access is not provided in any other location. There is no offsite access to the PMS.

3.1.1 Real-Time Data Distribution

Real-time data distribution is accomplished using process data transfer communication on the AF100 bus. [

]a,c

[

]a,c

The Advant Ovation® Interface (AOI) gateway in each PMS division transfers certain real-time data from a division’s AF100 bus to the non-safety Real-Time Data Network to support control and information system functions performed in the non-safety system. This functionality is discussed in more detail in Section 3.3.

3.1.2 Access Control

The four PMS intra-divisional Common Q networks are only accessible in the divisional equipment rooms and in the MCR. Network fiber optic cabling between each of the equipment rooms and the MCR is in an enclosed raceway. Access is not available in any of the other Operation and Control Centers. The networks are not accessible from off-site locations.

3.2 INTRA-DIVISIONAL AND INTER-DIVISIONAL COMMUNICATIONS VIA HIGH SPEED LINKS

The PMS uses point-to-point serial links to communicate certain data within and across PMS divisions. These links are part of the Westinghouse Common Q Platform (see References 2 and 3) and are referred to as the Common Q HSLs. The HSL is a serial RS 422 link using High-Level Datalink Control (HDLC) protocol with a 3.1 Mbits/second transfer rate. Each Common Q PM has one independent transmit link (output to two ports) and two independent receive links. The transmit and receive links are independent of each other. Each is a purely unidirectional point-to-point link without acknowledgement from the receiver. The data is optically isolated if it leaves the cabinet suite. The optical isolation is provided by the use of fiber-optic media converters and fiber-optic cable.

3.2.1 Planned Data Exchange

HSL data communications between two Common Q PMs is referred to as planned data exchange.

The planned data exchange mode is when two processors are connected via the HSL for the exchange of predefined data packets. Processors on each end of the HSL are configured to send/receive a predefined set of data. [

]a,c

3.2.2 Bistable Processor Logic to Local Coincidence Logic Communication

The PMS uses Common Q HSLs to transfer the partial trips, partial actuations, and related status information calculated in the BPL controllers to the LCL controllers. These links are used both locally within a division and externally across divisions. The links going across divisions use fiber-optic media converters and fiber-optic cable to provide the electrical isolation required by IEEE 603, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations” (Reference 7). The links are true point-to-point links and provide the communication isolation envisioned in IEEE 7-4.3.2, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations” (Reference 23), Annex E.

3.2.3 Local Coincidence Logic to Integrated Logic Processor Communication

The PMS uses Common Q HSLs to transfer ESF system-level actuations and related status information calculated in the LCL controllers to ILPs that actually control the safety components. These links are only used locally within a division.

3.2.4 Integrated Communication Processor to Integrated Communication Processor Communication

The PMS uses Common Q HSLs to transfer data to support the QDPS function and data to support cross-division diagnostics between divisions. These links are only used externally across divisions. The links going across divisions use fiber-optic media converters and fiber-optic cable to provide the electrical isolation required by IEEE 603 (Reference 7). The links are true point-to-point links and provide the communication isolation envisioned in IEEE 7-4.3.2 (Reference 23), Annex E.

3.2.5 Integrated Logic Processor to Safety Remote Node Controller

The PMS uses Common Q HSLs to transfer ESF component-level actuations and related status information between the ILP controllers and the safety components. These links are used locally within a division.

3.2.6 Interface and Test Processor to Interface and Test Processor Communication

The PMS uses Common Q HSLs to transfer data between divisions to support diagnostics and tests. These links are only used externally across divisions. The links going across divisions use fiber-optic media converters and fiber-optic cable to provide the electrical isolation required by IEEE 603 (Reference 7). The links are true point-to-point links and provide the communication isolation envisioned in IEEE 7-4.3.2 (Reference 23), Annex E.

3.3 COMMUNICATION BETWEEN SAFETY AND NON-SAFETY EQUIPMENT

The PMS implements data flows between safety and non-safety equipment using divisionalized unidirectional gateways and individual analog and digital signals as shown in Figure 3-1. Five cases are identified in the figure and labeled Case A through Case E. The cases are discussed in more detail in the following sections.

3.3.1 Isolated Sensor Loop Signal to Non-Safety (Case A)

Analog inputs required for both control and protection functions (e.g., Pressurizer Pressure) are processed independently with separate input circuitry. The input signals are classified as safety-related and are, therefore, isolated in the PMS cabinets before being sent to the PLS as individual hardwired analog signals. This is identical to the type of interface in existing Westinghouse plants. An example of this type of interface is shown as Case A on Figure 3-1.

Qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by Reference 7). They also provide functional isolation by preventing the non-safety system from adversely affecting the safety function.

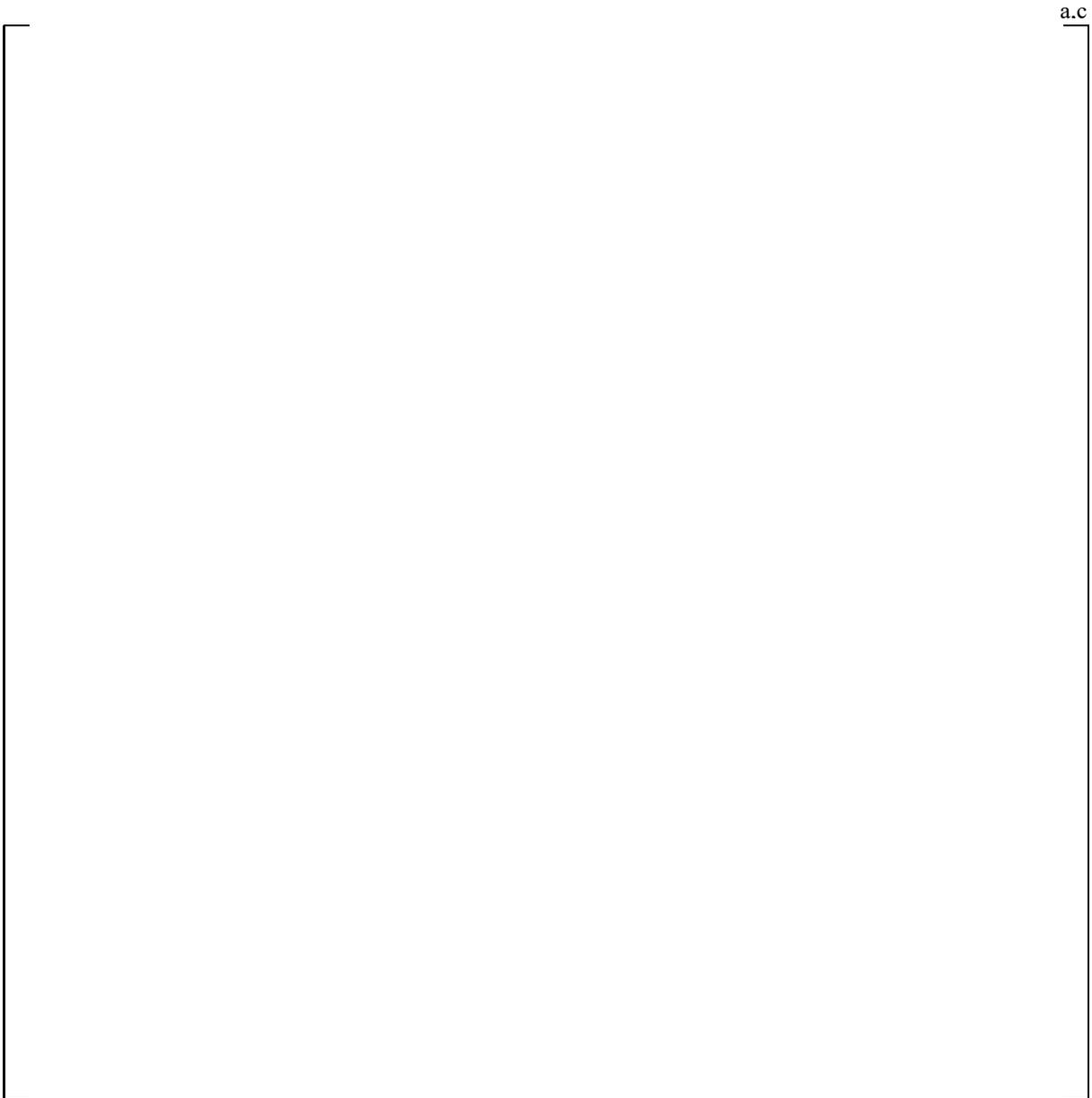


Figure 3-1. Data Flows between Safety and Non-Safety Equipment

3.3.2 Isolated Analog and Digital Signals to Non-Safety (Case B)

The PMS also provides data to non-safety equipment pertaining to analog and discrete digital signals calculated within the PMS (e.g., Over-Temperature ΔT Margin to Trip). These signals are classified as safety-related and are, therefore, isolated in the PMS cabinets before being sent to the non-safety equipment as individual hardwired analog or discrete digital signals. Typically, the resulting signals are sent to the PLS. Additionally, the outputs of certain PMS CIMs also directly actuate selected non-safety components (e.g., pressurizer heater block and feed water pump trip). These isolated hardwired analog or discrete digital signal interfaces (whether to the PLS or to non-safety components) are identical to those in existing Westinghouse plants. An example of this type of interface (between the PMS and PLS) is shown as Case B on Figure 3-1.

Qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by IEEE 603 {Reference 7}). They also provide functional isolation by preventing the non-safety system from adversely affecting the safety function.

3.3.3 Isolated Unidirectional Datalink Signals to Non-Safety (Case C)

Various process-related signals (analog input signals, analog signals calculated within the PMS, digital signals calculated within the PMS and SOE signals) are sent to the DDS for information system (plant computer) purposes. Non-process signals are also provided to the DDS for information system purposes. The non-process outputs inform the DDS of cabinet entry status, cabinet temperature, DC power supply voltages, and subsystem diagnostic status, etc. There are also process-related signals that are sent from PMS to PLS that do not require the low transmission latency or the control system segmentation provided by the dedicated signal interfaces described for Cases A and B.

The AOI gateway in each PMS division connects the division's internal network to the non-safety Real-Time Data Network, which supports the remainder of the I&C system. Each gateway has two subsystems. One is the safety subsystem, which is part of the PMS division and interfaces to the Common Q network. The other is the non-safety subsystem, which is part of DDS and interfaces to the Emerson Ovation Network. The two subsystems are connected by a fiber-optic link. This type of interface is shown as Case C on Figure 3-1.

The flow of information between the two gateway subsystems is strictly from the safety subsystem to the non-safety subsystem. The unidirectional nature of the gateway is assured by the use of a single unidirectional fiber to connect the two gateway subsystems. Within the safety system, the fiber is connected to an optical transmitter. Within the non-safety system, the fiber is connected to a fiber-optic receiver. This arrangement provides electrical isolation between the systems (as required by IEEE 603 {Reference 7}) and prevents all data flow (data, protocols, and handshaking) from the non-safety system to the safety system (providing the communication isolation envisioned by IEEE 7-4.3.2 {Reference 23}, Annex E). It also provides functional isolation by preventing the non-safety system from adversely affecting the safety function. This implementation is shown in Figure 3-2.

The safety software for the AOI gateway has two parts. The first part is the Ethernet driver that is part of the QNX[®] operating system. The QNX operating system was commercially dedicated and the dedication report was accepted by the NRC as part of the Common Q Safety Evaluation Report process.

The second part of the AOI gateway software was developed by Westinghouse. This software followed the process specified for “Important to Safety” software in WCAP-16096-P-A, “Software Program Manual for Common Q Systems” (Reference 31) (the SPM), for safety software. The SPM was accepted by the NRC as part of the Safety Evaluation Report (SER) process for the Common Q Platform.

The AOI uses a physically unidirectional transmission fiber-optic datalink from the PMS to the non-safety system. The AOI gateway has no protection function in the PMS. The reliability of the PMS to perform its safety function is not dependent on the AOI gateway being functional.

For SOE signals such as partial trip signals, reactor trip signals, and engineered safety feature (ESF) actuation signals, each division provides the signals to the SOE system/interface via a unidirectional fiber-optic link. The flow of information is strictly from the safety subsystem to the non-safety SOE system/interface. The unidirectional nature of the link is assured by the use of a single unidirectional fiber. The safety end of the fiber is connected to an optical transmitter. The non-safety end of the fiber is connected to a fiber-optic receiver. This arrangement provides electrical isolation between the safety and non-safety portions of the system (as required by IEEE 603-1991 {Reference 7}) and prevents all data flow (data, protocols, and handshaking) from non-safety to safety (providing the communication isolation envisioned by IEEE 7-4.3.2 {Reference 23}, Annex E). It also provides functional isolation by preventing the non-safety equipment from adversely affecting the safety function. This type of interface is a variation of Case C in Figure 3-1.

a,c



Figure 3-2. Example Implementation of Case C Data Flow

3.3.4 System-Level Safety Functions from RSR Fixed-Position Switches and Non-Safety Interlock of PMS Test Functions (Case D)

In the RSR, the non-safety manual controls of system-level safety functions (actuators, manual blocks and resets, manual reactor trip) originate from dedicated switches. The individual discrete digital signals are classified as non-safety-related and are, therefore, isolated in the PMS cabinets before being used. At the RSR, a fiber-optic transmitter sends the switch contact state over the fiber-optic cable. In the PMS, the fiber-optic receiver recreates the switch contact state on its discrete output signal to the AC160 rack in the Safety System. Electrical isolation is provided via the fiber-optic connection. There is no metallic path to conduct an electrical fault in to the PMS. This type of interface is shown as Case D on Figure 3-1.

Qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by IEEE 603 {Reference 7}).

Functional isolation provided by logic within the PMS prevents this data flow from inhibiting the safety function. First, the functionality associated with these controls is disabled until operation is transferred from the MCR to the RSR. Thus, these controls are disabled except in the extremely unlikely situation of having to evacuate the MCR. This transfer is accomplished by the divisionalized Class 1E transfer switches, which are connected directly to the BPL subsystems in each division. Additionally, when the controls are enabled, their functionality is limited to that defined in the PMS functional design because the information transferred is only in the form of discrete digital signals (i.e., there is no computer software-based communication). Specifically, the manual system-level ESF actuators and the manual reactor trip inputs can only initiate safety functions, not inhibit them. The manual system-level blocks are subject to initiation permissives and to automatic removal. The manual system-level resets of the latched-in manual system-level actuation signals and the latched-in automatic system-level actuation signals (upon return to normal) only remove the system-level actuation signals; they do not cause any components to change state. An additional signal is required to cause a component to change state.

To reduce the chance of the spurious actuation of a function that would require simultaneous operation of dual switches in the MCR, dual switches (each with its own fiber) are also provided for that function in the RSR. Two simultaneous failures would be required to cause a spurious actuation.

Certain PMS test functions are subject to interlocks from non-safety equipment. The purpose of these interlocks is to assure that the plant is properly aligned for the test. The individual hardwired discrete digital signals are classified as non-safety-related and are, therefore, isolated in the PMS cabinets before being used.

Qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by IEEE 603-1991 {Reference 7}) and prevent all but the required data flow from the non-safety equipment to the safety system (providing the communication isolation envisioned by IEEE 7-4.3.2 {Reference 23}, Annex E).

Functional isolation provided by logic within the PMS prevents this data flow from inhibiting the safety function. The functionality associated with these signals only affects the ability to perform tests. The interlocks do not affect automatic or manual safety functions.

3.3.5 Non-Safety Control of Safety Components (Case E)

PLS provides component-level soft controls in the MCR/RSR for most safety components. Additionally, PLS provides automatic control of some safety components for non-safety functions. The non-safety to safety data flows are not implemented using communication links; rather, they are implemented using discrete digital signals. However, to reduce the number of signals (cables) that must be run from the non-safety system to the safety system, the non-safety system's remote I/O capability is used to deliver the signals to the safety system and to accept component status signals from the safety system. Specifically, a remote I/O node from the non-safety system is physically located within each division of the safety system. The remote I/O node is electrically isolated from the non-safety system by the fiber-optic remote I/O bus. The node is powered by the safety system and the portions of the node not performing a safety function are qualified as associated Class 1E equipment. This type of interface is shown as Case E on Figure 3-1.

The Associated Class 1E equipment, including the Remote Node Controller (RNC) shall meet the requirements of IEEE Standard 384-1981, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuit" (Reference 24), Clauses 5.5.2 and Clause 5.5.3. Specifically, the equipment shall be part of the safety system qualification program that will demonstrate that when it is subject to environmental, electromagnetic, and seismic stressors, it does not degrade the Class 1E circuits below an acceptable level. The environmental, electromagnetic, and seismic stressors used for these tests are the same as those used to qualify the Class 1E equipment in the same cabinet.

The remote I/O node includes one or more Class 1E CIMs. Internally, these modules contain the equivalent of a discrete digital output module. The resulting discrete digital output signals, corresponding to the demands from the non-safety system, are made available to field programmable gate array (FPGA) based priority logic also contained in the CIM.

The priority logic within the CIM combines the non-safety demands with Class 1E automatic actuation signals and Class 1E manual actuation signals from the PMS subsystem. The prioritization is system-based with all PMS demands having priority over PLS demands.

The CIMs also contain the equivalent of a discrete digital input module. It is used to read component status and internal CIM status. This information is made available to the non-safety system. Thus, at the point of interface to the priority logic, there are two unidirectional data flows: (1) demands going from non-safety to safety and (2) status going from safety to non-safety. Each of these data flows is implemented as simple discrete digital signals not as a communication link.

As mentioned above, the remote I/O bus that is used to connect the non-safety system to the associated Class 1E remote node is fiber-optic. This arrangement provides electrical isolation between the safety system and the non-safety system as required by IEEE 603 (Reference 7). The remote I/O node controller and the communication function within the CIM implement the communications, and only the resulting discrete digital signals interface with the Class 1E priority logic in the CIM. The simple discrete signal interface within the CIM provides the communication isolation envisioned by IEEE 7-4.3.2 (Reference 23), Annex E. Although the remote I/O bus uses bidirectional communications, the simple discrete signal interface between the communication function and the Class 1E priority logic assures that the only data reaching the logic are the intended commands. The priority logic within the CIM provides functional isolation by implementing the priority logic and by only implementing the functionality defined in the PMS functional design. This implementation is shown in Figure 3-3. More information on the CIM is presented in Section 5.

3.4 MANUAL CONTROL OF SAFETY SYSTEMS AND COMPONENTS

The AP1000 I&C system provides for the manual control of the system-level safety functions and component-level safety functions.

3.4.1 Manual System-Level Control

Several mechanisms are provided to initiate the system-level actuation of ESF functions. Once the functions are actuated, the associated plant components move to their actuated state. Upon removal of the system-level actuation, the plant components remain in their actuated state until they are restored to their unactuated state by component-level controls. Controls are also provided for other ESF system-level commands such as blocks and resets.

- PMS Manual ESF System-Level Actuations from the MCR – The normal mechanism to actuate the ESF system is to use dedicated switches located in the MCR. Switches are located on the PDSP and the Secondary Dedicated Safety Panel (SDSP). The MCR system-level actuation switches are cabled directly from the switches in the MCR to the LCL located in the bistable coincidence cabinets in each instrument room. These switches are processed by the LCL in each PMS division. The resulting commands then fan-out to the ILPs and the CIMs implementing the actuated function.
- PMS Manual ESF System-Level Blocks and Resets from the MCR – The normal mechanism to control ESF blocks and resets is to use soft controls located on the divisionalized safety displays in the MCR. The safety displays are located on the PDSP. These commands are transmitted over the intra-division Common Q Network and are processed by the LCL in the PMS division.
- DDS Manual ESF System-Level Actuations from the RSR – In the event of an evacuation of the MCR, the mechanism to actuate the ESF system is to use the non-Class 1E dedicated switches located in the RSR. The signals pass through qualified isolators in the PMS. The isolators provide electrical and communication isolation. These switches are processed by the LCL in each PMS division. Logic in the LCL provides functional isolation. First, the controls are disabled unless operation is transferred to the RSR. Second, the functionality is limited to that defined in the PMS functional design. From the LCL, the commands fan-out to the ILPs and the CIMs implementing the actuated function.
- Diverse Actuation System (DAS) Manual ESF System-Level Actuations from the MCR – In the event of a postulated common mode failure of the PMS, certain ESF functions can be actuated through diverse means. Dedicated switches for these functions are located on the DAS Panel in the MCR. These switches allow the ESF functions to be actuated through a path independent of the PMS and the DAS automatic actuation logic; for example, through a separate pilot solenoid on air-operate valves, through separate igniters on squib valves, and through separate inputs to the motor control center for motor-operated valves. All switches on the DAS panel are disabled until the DAS panel is enabled by a separate switch in the MCR.

a,c



Figure 3-3. Implementation of Case E Data Flow

3.4.2 Manual Component-Level Control

Normal manual component-level control of safety components is provided by the PMS or PLS. PMS component control is provided for components that meet any of the following criteria:

- Component actuation could cause a breach in the reactor coolant boundary
- Component actuation could cause an over-pressurization of a low pressure system
- Component actuation cannot be reversed from the control room (e.g., squib valves)
- Operator action is required to manipulate controls to maintain safe conditions after the protective actions are completed
- Valves that require jogging

Components meeting these criteria are listed in Section 7.2 of WCAP-16674-P (Reference 30).

For safety components that have normal manual component-level control from PLS:

- PLS Manual ESF Component-Level Control from the MCR – The normal mechanism to control these ESF components at the component level is to use soft controls from the non-safety workstations located in the MCR. The soft control commands are transferred over the non-safety Real-Time Data Network to a non-safety controller. The controller then sends the command to the appropriate CIMs in the PMS via the remote I/O bus. The fiber-optic remote segment of the remote I/O bus provides electrical isolation. The communication function within the remote node controller (RNC) and the CIM provide communication isolation. The CIM priority logic function provides functional isolation.
- PLS Manual ESF Component-Level Control from the RSR – In the event of an evacuation of the MCR, the mechanism to control these ESF components at the component-level is to use soft controls from the non-safety workstations located in the RSR. They are implemented in the same manner as described for those in the MCR.
- PLS Manual ESF Component-Level Control from the Equipment Rooms – Safety components that have normal manual component-level control from PLS can also be controlled at the component level using dedicated switches located on CIMs that are part of PMS and are located in the equipment rooms. These switches have priority over other PLS and PMS demands.

For safety components that have normal manual component-level control from the PMS:

- PMS Manual ESF Component-Level Control from the MCR – The normal mechanism to control these ESF components at the component level is to use soft controls located on the divisionalized safety displays in the MCR. The soft controls use a multi-step sequence to reduce the chance of spurious actuation. The safety displays are located on the Primary Dedicated Safety Panel. These commands are transmitted over the intra-division Common Q network and are processed by the ILPs in that PMS division.

- PMS Manual ESF Component-Level Control from the Equipment Rooms – In the event of an evacuation of the MCR, the mechanism to control these ESF components at the component-level is to use dedicated maintenance and test switches located on CIMs in the equipment rooms.

3.4.3 Justification for Use of Common Electronics for Manual and Automatic ESF Actuations

The AP1000 meets the requirements of Reference 7. The single failure requirement is met through the use of divisional redundancy.

In addition to the single failure criterion, Paragraph 6.2.1 in Reference 7 requires manual means to actuate, at the division level, the automatically-initiated protective actions. The manual means “shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment...” The requirement for “minimum of equipment” does not specify whether or not the equipment can be common to the automatic initiation.

Regulatory Guide 1.62, “Manual Initiation of Protective Actions” (Reference 27), states that “the amount of equipment common to both manual and automatic initiation should be kept to a minimum.”

For the AP1000, manual ESF system-level actuation is accomplished through dedicated manual actuation switches in the control room. These switches are processed by high quality, Class 1E software. Manual actuation logic includes permissives, resets, and sequencing logic that are a function of the plant conditions as shown in Figure 7.2-1 of APP-GW-GL-700, “AP1000 Design Control Document” (Reference 1). The implementation of the manual actuation depends on a relatively small number of digital components. If no digital circuitry was included in the manual actuation circuitry, there would be a significant amount of additional circuitry, relays, timers, and wiring, thus, more than a “minimum of equipment” would be utilized.

ESF system-level and component-level actuation is accomplished from the following sources:

- Automatic system-level actuation by the safety system
- Manual system-level actuation from the MCR
- Manual component-level actuation from the MCR
- Manual system-level actuation from the RSR
- Manual component-level actuation from the RSR
- Manual component-level actuation from the CIM
- Automatic system-level actuation from the DAS
- Manual system-level actuation from the DAS

These sources need to be combined with a method for prioritization and the DAS actuation is required to be diverse. If signals from all of these sources were combined at the final actuation device, and if no digital circuitry was included, there would be a significant amount of additional circuitry needed for each component, further exceeding the “minimum of equipment” requirement.

The AP1000 design minimizes the use of common equipment by using common digital circuits in Level 2 LCL and Level 3 ILP and CIM to arbitrate the prioritization (permissives, blocks, resets, etc.) and actuation of ESF components from the sources identified above.

Implementation of this functionality at the component-level (below Level 3) would require hundreds of individual component control switches, latching relays, fan-out relays, prioritization relays, timers, discrete circuits, and wiring. Implementation of this functionality at Level 3 would also require fan-out relays, prioritization relays, timers, discrete circuits, and wiring. The use of relays instead of digital circuits would be very complicated and difficult to maintain. Periodic testing of relays is costly, difficult, and contributes to the potential for human error.

Many of the manual controls must interact with signals generated within the PMS. Some of the manual actuations are interlocked with signals generated automatically within the Level 1 BPL logic (e.g., Manual Stage 4 Automatic Depressurization System (ADS) actuation that is interlocked with either the third stage ADS actuation signal or low Reactor Coolant System (RCS) wide range pressure signals (see Figure 7.2-1, Sheet 15 of 21 of Reference 1).

Implementation of this functionality at Level 2 provides a much simpler design. Digital circuits have higher reliability than relays. For the AP1000 design, the functions performed in the LCL and ILP are redundant within each division. The internal redundancy is provided in the design to facilitate the following:

- Continuous monitoring of processor performance
- Use of signal quality assignments
- Online testability with half of a division in test while the other half remains operational
- Self-revealing diagnostics
- Reduces the potential for limiting condition(s) for operation because the minimum number of operable channels can be maintained under many failure scenarios

In AP1000, the ESF system-level actuation enters the process at the same point as in a conventional Westinghouse plant (i.e., where the prioritization logic is performed).

Reference 27 states that “action-sequencing functions and interlocks... associated with the final actuation devices and actuated equipment may be common if individual manual initiation at the component or channel level is provided in the control room.” Reference 27 does not specify that the manual initiation at the component-level is required to be safety grade.

In AP1000, component-level actuation in the control room is accomplished via soft control for each component as discussed in subsection 3.4.2. Safety component control is provided for components that meet any of the following criteria:

- Component actuation could cause a breach in the reactor coolant boundary
- Component actuation could cause an over pressurization of a low pressure system
- Component actuation cannot be reversed from the control room (e.g., squib valves)
- Operator action is required to manipulate controls to maintain safe conditions after the protective actions are completed
- Valves that require jogging

Component control of the other safety components is accomplished through non-safety controls.

The following provides additional information regarding AP1000 design compliance with revisions to software common cause failure requirements in IEEE Standard 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Reference 25).

The 1998 revision of IEEE Standard 603 (Reference 25) contains Paragraph 5.16, which addresses software common-mode failures. This paragraph allows the use of manual actuation and non-safety-related systems, components, or both, as a means to accomplish the function that would otherwise be defeated by a software common cause failure. Reference 25 points to Reference 23 to determine if diversity is necessary.

NUREG-0800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*, Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems"

(Reference 26), provides guidance for diversity that applies to AP1000 at the plant level.

The AP1000 DAS provides a combination of automatic and manual controls to address software common cause failures in accordance with WCAP-15775, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report" Reference 35.

The AP1000 DAS provides manual initiation of reactor trip and selected functions. The manual actuation function of the DAS is implemented by hard-wiring the controls located in the MCR directly to the final loads in a way that completely bypasses the PMS path and the DAS automatic logic. These DAS manual actuation circuits are a non-safety equivalent to the hard-wired manual reactor trip circuitry and meet the requirements in Paragraph 5.16 of Reference 25, and Reference 26 as described in the previous two paragraphs.

Based on these points, AP1000 complies with Reference 7 and is a good, reliable, and sound design based on the technology available today.

a,c



Figure 4-1. PMS Safety Displays

[

] ^{a,c} Manual control of all other safety components is accomplished from the non-safety operator workstations, via the non-safety Real-Time Data Network, RNC, and CIM.

For NI calibration, the safety display provides the operator the ability to enter, store, and change the gain and offset for the NI PR upper flux signal and lower flux signal. No calibration of the SR or IR is required.

4.2 QUALIFIED DATA PROCESSING SYSTEM

The QDPS of the PMS provides data to support the safety-related display of selected parameters in the control room.

Two QDPS subsystems are provided in the PMS architecture. One QDPS subsystem is located in Division B and the other QDPS subsystem is located in Division C. The divisions are physically separated and electrically isolated from each other. The description provided below illustrates the operation of one of the two identical QDPS subsystems.

The QDPS subsystems are a redundant configuration, as shown in Figure 4-1.

The QDPS subsystems perform the following functions:

- Provide safety-related data processing.
- Provide the operator with sufficient operational data to support post-accident monitoring in the event of a failure of the other display systems.
- Provide data to the Real-Time Data Network for use by other systems in the plant, via the intra-divisional AF100 bus and the MTP, as previously described.
- Process data for MCR display, and to meet Regulatory Guide 1.97 (Reference 22) requirements.

PMS Divisions B and C each contain one QDPS subsystem, designated “QDPS” as shown in Figure 4-1. Each QDPS subsystem contains a communication module for the interface between the QDPS subsystem and the intra-divisional AF100 bus.

The QDPS subsystem contains one PM. The PM performs data reduction and calculations of group values, subcooled margin, and inadequate core cooling conditions.

Each QDPS subsystem also contains analog input modules. The analog input modules provide the interface between the dedicated and shared sensors and the PM.

Plant data is input to the QDPS subsystem in several ways:

- Dedicated sensors directly connected to the QDPS subsystem
- Shared sensors that have protective functions as well as QDPS functions
- Plant data from other PMS divisions

Dedicated sensors are connected directly to the analog input modules in the QDPS subsystem. These sensors do not perform any reactor trip or ESF actuation function and are used only for various QDPS functions.

[

]a,c

The QDPS variables to be displayed are identified in APP-PMS-J1-001, "AP1000 Protection and Safety Monitoring System Functional Requirements" (Reference 9).

Power is provided to the QDPS subsystems from the Class 1E DC and uninterruptible power supply (UPS) system for 72 hours after a loss of all AC power (station blackout). After 72 hours, the ancillary diesel generators provide power for the QDPS subsystem.

5 PLATFORM DESCRIPTION

5.1 HARDWARE

This section provides a description of the major components of the Common Q hardware platform used for the AP1000 PMS. The Common Q Platform was developed by Westinghouse for use in multiple safety-related systems such as the Reactor Protection System, Post-Accident Monitoring System, Core Protection Calculator System, Engineered Safety Features Actuation System, Diesel Load Sequencer, and Plant Protection Systems.

The Common Q Platform is Class 1E. Therefore, all of its building blocks are Class 1E. The PMS architecture incorporates the Common Q Platform and other safety system platform Class 1E components as shown in the following list:

- AC160 with PM646A
- S600 input and output modules
- Flat Panel Display System for human-machine interface consisting of the MTP and safety display
- Power supply
- CIM
- Termination units
- SRNC
- Cabinets

The Common Q Topical Reports (References 2 and 3) have been reviewed by the NRC. The NRC Safety Evaluation Reports (SERs) approving the use of Common Q for safety-related applications are contained in Reference 2. In addition, in November 2002, the Swedish regulatory body, SKi, provided Unit 1 at Oskarshamn nuclear power plant (NPP) approval to load fuel with Westinghouse Common Q product used in the Reactor Protection System. The Common Q product was extensively reviewed, led by the Oskarshamn NPP. The review also included a third-party evaluation performed by Colenco Power Engineering, Ltd. Furthermore, on behalf of Oskarshamn NPP, Westinghouse utilized TÜV product service for an independent evaluation of the Common Q software. The Common Q hardware was independently assessed by two independent certified organizations: Wyle Laboratories in the United States and DELTA Development Technology AB in Sweden.

5.1.1 Advant Controller 160 (AC160)

The AC160 controller is used for executing the protection algorithms in safety-related system applications.

The Westinghouse AC160 (see Figure 5-1) is a high-performance modular controller with multiprocessing capability for logic control. It can be used standalone, or as an integrated controller in a distributed control system, communicating with other Advant power equipment. The PM used in the Common Q applications is the PM646A.

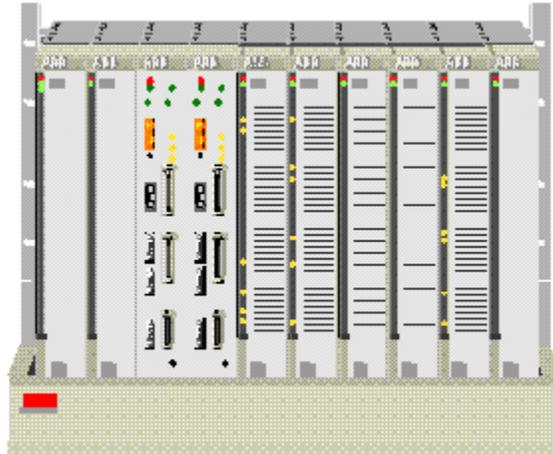


Figure 5-1. AC160 Station

AC160 is fully modular with modules mounted in 19-inch subracks. A typical Common Q configuration consists of PM(s), I/O modules, and communication modules contained in one or more subracks. Each subrack can accommodate up to 10 modules.

To provide scalability in performance and reliability, up to six PMs can be used concurrently in one controller. The PMs within an AC160 controller share data with each other using the global memory resident on the AF100 bus Communication Interface Module (Model CI631).

Each PM supports two high-speed communication links (i.e., HSLs). The HSLs are used to communicate data to other PMs in the same or other divisions of the safety system. These datalinks are electrically isolated using fiber-optic cable.

The processors are programmed in the Advant Master Programming Language (AMPL). In addition to the logic constructs, this language provides logic block interfaces to the AF100 bus, global memory, I/O, and the HSL.

The PM has a built-in, independent WDT module that provides annunciation and a channel trip if a protective function is rendered inoperable due to processor failures.

Fiber-optic media converters are used for electrical isolation of data communication connections to/from other safety channels and non-safety systems.

The configuration possibilities of AC160 cover a wide range of functions, such as logic and sequence control, data and text handling, arithmetic, reporting, and regulatory control. Several AC160 stations may be connected via the AF100 bus. The AF100 bus is a high-performance serial communications system featuring fast, real-time exchange of process data between the application programs in different AC160 stations.

Using redundant PMs and redundant main power supplies, increased reliability and availability of the AC160 can be achieved.

AC160 is fully modular. The subracks are normally installed in cabinets. All process connections are made to screw terminals on connection units or by crimp contacts.

With the excellent performance it offers, the following wide range of functions are supported, including logical control, analog signal processing, and feedback control:

- Logical operations and time delays
- Sequential control
- Feedback control
- Arithmetical operations
- Pulse counting
- Communication via AF100

The central processing unit (CPU) module PM646A (see Figure 5-2) is a powerful multiprocessing CPU module for the AC160 system for the control and supervision of processes and equipment in power plant environments. The PM646A is based on 32-bit Motorola MC68360 processors. The PMs are placed in positions 3 through 8 of the basic station, and it is possible to have more than one PM in one station (multiprocessing). These PMs can be combined in pairs in CPU-redundancy mode, or they can be independent from each other with up to six PMs placed in one station or in a combination of several stations. The PM646A module contains two 32-bit microprocessor boards: a processor section and a communications section.

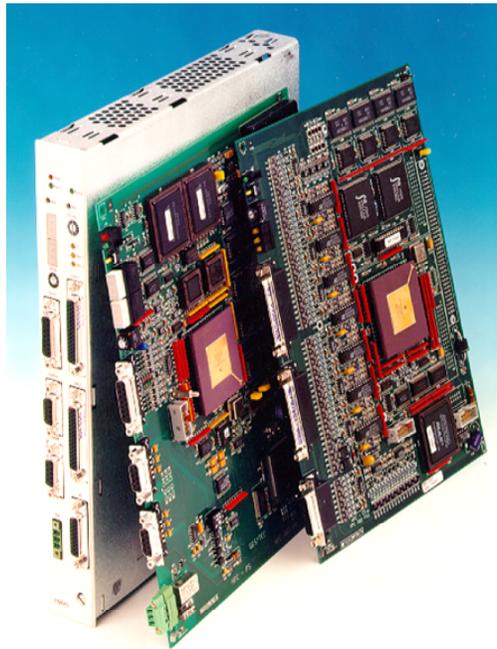


Figure 5-2. PM646A Processor Module

Processor section:

- Contains application code
- Non-volatile flash programmable read only memory (PROM) for application program
- Sends data to CI631 communication interface module for use on the AF100 bus
- Contains RS232 programming port
- Performs most of the self-diagnostics (WDT and memory checking)
- Stores data to be transmitted via HSL in dual-port memory for use by the communications section
- Retrieves HSL receive data from dual-port memory stored by communications section
- User configurable cycle time (2 milliseconds to 20 seconds)

Communications section:

- Handles the two HSL communication ports (RS422 Interface, 3.1 Mbits/second communication protocol meets IEEE 7-4.3.2 {Reference 23} communications requirements)
- Stores information received by HSLs in dual-port memory for use by processor section
- Retrieves information in dual-port memory for transmission out of HSL

Fast data communication between PMs in different stations or between two PMs is provided with the HSL connectors located on the front panel of the PM646A. This HSL connection is used to transmit data between two controllers without using the AF100 bus. It is a fast point-to-point connection between the controllers. The receive and transmit channels use a subset of the HDLC protocol.

5.1.2 S600 Input and Output Modules

The AC160 uses the S600 I/O system. The S600 family of input and output modules contains all the traditional cards such as analog inputs (including differential inputs, thermocouples, and RTDs), analog outputs, digital inputs, digital outputs, rotational/speed sensing inputs, and pulse counting.

S600 I/O modules (see Figure 5-3) typically contain 16 or 32 input or output channels, depending on the module. The I/O modules are placed in the AC160 controller subrack. I/O modules can also be inserted into the controller extension subrack. The extension subracks communicate with the main AC160 controller subrack via a hardwired bus extension. Process signals are connected to the front of the I/O modules via prefabricated cables from the field terminal blocks or termination units.

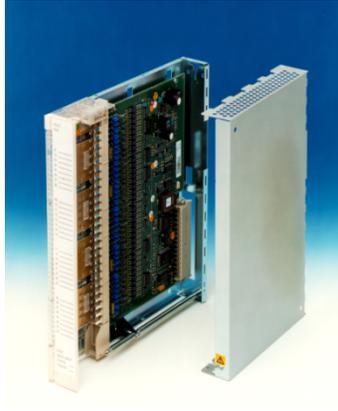


Figure 5-3. S600 I/O Module

The system software in the AC160 automatically supervises and checks that all I/O modules are operating correctly at system startup and by the application interfacing with the module during normal operation. The status of the module is indicated by two light emitting diodes (LEDs): RUN (green during normal operation) and FAULT (red when a fault is detected). More detailed diagnostic information is available by means of the MTP.

S600 I/O modules can be replaced during system operation (hot swap). The modules are housed in a sheet-steel enclosure that protects the circuit boards. The enclosure has openings at the top and bottom for air convection. The prefabricated cable carrying the process signals from the field terminal blocks is connected to the front edge of the I/O module, and is removable to facilitate module replacement.

The S600 I/O modules can be connected in a redundant configuration to improve the reliability of critical control loops.

The S600 I/O module types utilized in the safety system equipment are discussed in the following sections:

5.1.2.1 Analog Input Modules

The analog input modules convert analog input signals from transmitters to digital values required by the controller module.

- AI688 – 16 differential input channels, 0/4-20 mA, 0-1 V, 0-10 V.
- AI687 – 16 thermocouple input channels, Types J, K, and E with cold reference junction compensation.
- AI687 – 8 RTD input channels, Pt100 and Pt200.
- AI687 – 16 different input channels, 0-100 mV.

The 0/4-20 mA inputs are accommodated by current-to-voltage conversion in the I/O termination units.

5.1.2.2 Analog Output Modules

The analog output module converts the digital signals from the controller module to the analog signals needed for control, indication, etc.:

- AO650 – 8 channels, 0/4-20 mA, +/- 20 mA, 0/1-5 V, 0-10 V, +/- 10 V into load impedance of less than or equal to 600 Ohms (current output), and greater than or equal to 1.2 kOhm (voltage output), 12-bit resolution.

5.1.2.3 Digital Input Modules

The digital input modules convert the binary signals from the field to the internal signal levels required by the controller module.

- DI621 – 32 channels, 48 VDC, opto-isolated in groups of 8.

5.1.2.4 Digital Output Modules

The digital output modules convert the digital signals from the controller module to the binary or contact output signals needed for control, indication, etc.

- DO620 – 32 channels, 48 VDC, 600 mA, transistor source output, opto-isolated in groups of 8.
- DO630 – 16 channels, 230 VDC/AC, 2.4 A, relay contact output, coil-to-contact isolation.

5.1.2.5 Pulse Counting, Rotational Speed Input Processing

The pulse counter module registers and processes fast pulse signals at repetition rates up to 100 kHz.

- DP620 – 5 channels, 5 V, 24 V, +13 mA, less than 100 kHz, Up/Down Counting, Frequency/Difference Measurement, Position, Rotation/Speed.

5.1.2.6 Total S600 I/O Capacity Per Control Station

- I/O channels (soft limit) up to 1500.
- I/O modules (soft limit) up to 75.

Qualified signal isolators are utilized to provide signal isolation for analog and digital signals where required to satisfy the requirements for independence and isolation.

5.1.3 Flat Panel Display System

The Flat Panel Display System (FPDS) is the human-machine interface for the Common Q safety system. It consists of a touch screen video display and a PC Node Box. The FPDS is qualified and licensed for Class 1E applications. When mounted in a system cabinet, the FPDS is usually referred to as the MTP. When mounted in the MCR, it is referred to as the safety display.

5.1.3.1 Touch Screen Display

The video display is a qualified thin-film transistor (TFT) color display with capacitive touch screen capability. Three sizes are available: 12-inch, 15-inch, and 19-inch diagonal measurement. Two sizes are used in the PMS. The 15-inch display is used for the MTP display. Because of its larger viewing area, the 19-inch display is used for safety displays in the MCR. Touch screen functionality is not implemented on the safety displays.

5.1.3.2 PC Node Box

The PC Node Box is the interface between the AF100 bus and the flat panel video display.

The PC Node Box contains the following components:

- Industrial Computer

The dual boot computer contains an Intel[®] embedded systems group processor with non-volatile flash memory. The qualified QNX operating system software provides the graphical user interface and is used for on-line mode and during surveillance testing. A Windows[®]-based application (MTP only) is used for off-line mode to load AC160 software or to perform AC160 diagnostics.

- AF100 Communication Interface Module
- Digital Input/Output Interface
- Removable Storage Device
- Input/Output Ports, Keyboard, and Mouse

5.1.4 Common Q Power Supply

The Common Q power supply is a modular power supply system. Various modules are available to accommodate different output voltages. Input power to the Common Q power supply system is 85 to 264 VAC at a line frequency of 45 to 65 Hz, or 90 to 350 VDC.

Power supply modules are single output supplies that can range from 180 to 480 watts output ratings. Voltages from 5 to 56 VDC can be supported.

The power supply can support single or dual power feeds. Redundant power supply configurations are supported by diode auctioneering. Faults in one redundant supply do not affect the other redundant supply from operating normally. Redundant modules can be replaced while the power supply remains energized without disturbing the powered system. The redundant power supply is monitored by the system, and failures are detected and alarmed. The power supply has over-voltage and over-current protection, soft start, and a high power factor. The power supply is normally mounted in the top of a cabinet.

5.1.5 Component Interface Module

[

-
-
-
-
-
-
-
-
-

]a,c

5.1.6 I/O Termination Units

I/O termination units provide an interface between the S600 I/O modules and the field circuits. There is a separate type of termination unit to interface to each of the I/O module types. Each type of termination unit provides termination points for the field wiring, including individual terminals for cable shields. Each type of unit also provides signal disconnects and test points to support system testing and maintenance. In addition, the following features are provided:

- AI687 Termination Unit – Provides separate connection for signal sharing. Configurations include thermocouples and RTD inputs.
- AI688 Termination Unit – Provides loop power (30 V), isolated per module. Provides separate connection for signal sharing. Configurations include 0-10 V and 4-20 mA (with current-to-voltage dropping resistors) inputs.
- AO650 Termination Unit – Provides termination, disconnects, and test points only.
- DI621 Termination Unit – Provides contact wetting voltage (48 V) and ground fault detection, isolated per four groups of eight inputs each. Provides separate connection for signal sharing.
- DO620 Termination Unit – Output power (externally supplied) is fused and distributed to four groups of eight outputs each.
- Termination Unit with Y-Feedthrough – Provides two output points for each input point.
- High Speed Link Termination Unit – Provides copper-to-copper or copper-to-fiber interfaces to fan-out the HSL signal from the PM646A.
- Reactor Trip Matrix Termination Unit – Provides the ability to manually test the RTCB via the UV and ST coils. Monitors the PM646A WDT relay contact output to provide preferred failure mode operation. Provides interface between the manual reactor trip switches and the RTCB.

5.1.7 Safety Remote Node Controller

The SRNC provides an interface between the AC160 controller and the CIM. The main functions of the SRNC are:

- Receive data from the AC160 controller via a high-speed serial datalink
- Error checking on high-speed serial data
- Transmit data to the CIM via a serial bus
- Receive data from the CIM via a serial bus
- Transmit data to the AC160 controller via a high-speed serial datalink

5.1.8 ADS and IRWST Injection Blocking Device

The ADS and IRWST Injection Blocking Device design uses conventional analog components that do not rely on software. Apart from its inputs and outputs and power source, the ADS and IRWST Injection Blocking Device does not share other PMS components.

The ADS and IRWST Injection Blocking Device in each division requires the following inputs:

- 4-20 mA inputs from two narrow range upper-level sensors (one on each CMT).
- Contact inputs from one MCR override switch.
- Contact inputs from one MCR/RSW transfer switch.
- Contact inputs from two undervoltage relays from battery chargers.

[

-

]a,c

5.2 SOFTWARE DESCRIPTION

This section provides a description of the Common Q AC160 software platform used for the safety-related systems.

The AC160 software consists of a real-time operating system, task scheduler, diagnostic functions, communication interfaces, and user application programs, all of which reside on flash PROM in the PM646A. The application program in an AC160 coexists with the other AC160 system software programs such as the diagnostic routines and communication interfaces. The task scheduler schedules the execution of all these different entities. The base software includes the executable code for the standard set of logic blocks (PC elements). In addition, custom PC elements can be created as an extension to the base software.

Application programming is accomplished by configuring and interconnecting items from a library of predefined function blocks, called PC elements, and Database (DB) elements. The PC elements and DB elements are combined into programs that form a complete control function.

Application programming is done on an Intel processor based personal computer using the AMPL Control Configuration (ACC) software development environment. The target code is generated and saved to a write only compact disc. The MTP includes a DVD drive to support loading of the target code.

5.2.1 AMPL Programming Language

Process control applications are configured in AMPL, a function block language with graphic representation that is especially developed for process control applications. The language is characterized by each function being seen as a building block with inputs and outputs.

A program written in AMPL is referred to as an AMPL program and the building blocks are called PC elements. The range of ready-to-use PC elements is wide and powerful. Control loops can be combined with motor control, startup, and shutdown sequences and fast interlocking logic (with cycle time down to 2 milliseconds), all in the same control program and using the same high-level function block oriented language, AMPL. Custom PC elements can also be written in a high-level language (C) and added to the library.

In addition to functional PC elements, AMPL contains a number of structural elements for division of an AMPL program into suitable modules, which can be managed and executed individually. The modules can be given different cycle times and priorities so that both fast and slow control operations can be managed by the same AMPL program.

The inputs and outputs of an element are connected to the inputs and outputs of other elements or to process I/O points. Picking these elements and making these connections constitute the configuration work.

The resulting AMPL program can then be documented graphically.

5.2.2 ACC Function Chart Builder

The Function Chart Builder of ACC enables development of AMPL application programs graphically, using a tree editor, a function chart editor, or a combination of both. The combination is particularly powerful in that the tree-structured view provides a hierarchical overview for efficient navigation, while the function chart view provides the functional details and a perfect basis for programming and program editing. Configuration in AMPL is essentially a matter of inserting program elements, or type circuits, onto diagram sheets and connecting these elements to other elements and to objects in the database. Program element manuals are available as part of the built-in help. Other important productivity features include repetition of the latest command, repetition of the latest setting, and the inclusion of an apply button in dialog boxes wherever appropriate.

Features of the Function Chart Builder include AC160 using the corresponding libraries.

The following functions are provided by the ACC Function Chart Builder:

- Tree editor for control program structures
- Editing of function charts
- PC (AMPL) source code editing and syntax checking in node mode (Syntax errors can be listed together with the code in a second window to facilitate corrections.)
- Automatic consistency to the engineering database
- Symbolic addressing of signals
- Use of calculated symbols (parameters)
- Generation and back-translation of application programs and database source code (can be used for transfer purposes between different process stations and engineering systems. The graphic representation after back-translation from the target station is the same as if the program was entered directly into the Function Chart Builder, ensuring engineering consistency.)
- Graphical documentation of application programs in function chart representation and in tree representation
- Database and cross-reference documentation in list representation
- Testing and fault tracing
- Dynamic display of variables; display and modification of parameters with function chart representation (off-line mode)
- Forcing of inputs and outputs (in the development stage only)
- Reading/setting of date and time

5.2.3 Configuration Management

Application software modifications are accomplished via the ACC engineering tool via one of two modes: off-line or on-line.

5.2.3.1 Off-line Mode

In the off-line mode, the application function charts are modified to obtain the desired functionality with the ACC engineering tool disconnected from the Advant Controller station. Extensive self-checks within the engineering tool preclude illegal programming operations. When the modified function chart is completed, new source code is generated in an American National Standard Code for Information

Interchange (ASCII) text format for archiving. New target code (machine code) for the entire application program is also compiled by ACC.

At this point, the ACC tool is connected to the Advant Controller to be modified. The connection can be made directly to the controller’s CPU module or remotely via the Advant field communications network. The latter connection using the AF100 is prevented. Via ACC, the controller’s application program is blocked (alarm received) and the new target code is downloaded and saved into the CPU module’s flash PROM (non-volatile memory). Numerous self-checks are conducted to ensure the download is completed successfully.

The new application program is unblocked and testing is conducted to validate the functionality of the modified program. The extent of validation testing is determined by the verification and validation (V&V) plan approved for the software modification.

5.2.3.2 On-line Mode

In on-line mode, the ACC engineering tool is connected to the Advant Controller during modification of program function charts. This permits the controller to remain operational throughout the modification process. While disabled on installed system controllers, this feature is very useful for debugging software modifications on a test platform prior to deployment in the plant.

In the on-line mode, operational target code is only re-compiled and downloaded for the portion of the program that is modified. In addition to the self-checks described for the off-line mode, numerous confirmatory messages are provided to prevent inadvertent actions.

Following modification, validation testing would be conducted as determined by the respective V&V plan.

5.2.4 Flat Panel Display Software and Tools

The Common Q FPDS software is a QNX-based multiprocessing system that is designed such that displays are dynamically updated from data acquired from the AF100 bus interface. The types of displays that can be developed for the FPDS include trends, lists, alphanumeric process displays, and maintenance displays. The QNX Photon® microGUI® product is the runtime engine for the display application on the FPDS. In addition to the display application, other processes in the FPDS support receiving and transmitting data on the AF100 bus for the display application and other processes, sending configured data over the AOI, and monitoring the software integrity of the FPDS. The display application is created on a software developer’s platform using the QNX Photon Application Builder.

6 MAINTENANCE, TESTING AND CALIBRATION

Maintenance and testing of the PMS consists of two types of tests: self-diagnostic tests and on-line verification tests. The self-diagnostic tests are built into the AC160 equipment and consist of numerous automatic checks to validate that the equipment and software are performing their functions correctly. Self-diagnostics, as well as on-line verification tests that can be manually initiated are used to verify that the safety system is capable of performing its intended safety function.

6.1 SELF-DIAGNOSTIC TESTS

6.1.1 Processor and I/O Modules

A variety of self-test diagnostic and supervision functions are performed by the PMS processors and I/O modules to continuously monitor their operations. Each of the modules has its own diagnostic functions. The PM monitors the system as a whole by collecting all the diagnostic information and checking the consistency of the hardware configuration with the application software currently installed.

During power-up, the functions of the processor and the contents of the application and system flash PROM are checked as well as the internal Static Random Access Memory (SRAM) of the processor.

The processor system software includes diagnostic routines, which check the processor and the system during initialization and ensure system integrity during the execution of the application program.

The processor checks the consistency of the module configuration specified by the DB elements and the actual configuration of the modules. This check is performed each time a module is switched on before it is automatically switched to the RUN mode. If the module installed does not correspond to the type of module specified by the module DB element, then the module is not switched to the RUN mode and the error is indicated on the associated DB element.

Each module is equipped with the two LED indicators: FAULT and RUN. During normal operation, the green LED RUN is lit on all modules. The red LED FAULT illuminates only if a problem occurs on the module.

While the application program is running, the diagnostic routines continue checking operation without delaying or influencing the execution. Each processor (e.g., BPL, LCL, ILP) is monitored by the use of background diagnostics for the processor and I/O module faults. Failures on I/O modules are first detected by the individual module, which then passes failure status information to the processor (error buffer) where it is stored and acted upon. The supervision functions of the equipment are subdivided into the following groups:

- Problem detection
- Signaling the nature of the problem
- Automatic reaction to the problem

The status of the modules and the I/O signals is indicated by the associated DB element. Missing modules are also signaled by the function supervising the configuration on the associated DB element. The status signals on the DB elements can be processed by the application program in the same way as other signals.

The I/O modules supervise whether or not the process termination edge connector is correctly inserted. If the edge connector is withdrawn, operation of the I/O module is immediately inhibited (i.e., it is no longer in the RUN state), and the error is indicated on the associated DB element module and the DB element's channel in the processor. If the process connector is not inserted, the module cannot be switched to RUN mode.

The software also monitors whether the processor has sufficient capacity to perform its functions within the times specified. If it does not, the processor inhibits the application program.

[

]a,c

6.1.2 Communication Modules

The purpose of the AF100 bus communication modules is to provide communication between subsystems (e.g., BPL, LCL, ILP, MTP, ITP). The AF100 bus supports two different types of communications: process data and message transfer. Process data are dynamic data used to monitor and control the process, while message transfer is used for program loading (disabled for AP1000) and system diagnostics.

The communications modules are individually supervised by their own internal diagnostics and additional run-time diagnostics. In addition, the PM performs continuous background diagnostics of the communications modules and automatically detects errors during operation. The PM contains the error messages in the error buffer for system troubleshooting.

Each communications module is equipped with LEDs located on the front of the module to display the status of the module and operational state of the network. The LEDs provide initialization and operational information as follows:

- FAULT LED (Red) indicates a module failure (i.e., hardware or cable problem).
- RUN LED (Green) indicates normal operation and in RUN-mode.

- TRAFFIC LED (Green) is set when the communications module finds another device on the network.
- MASTER LED (Yellow) is set when the communications module is the bus master on the AF100 bus. Because every communications module is capable of being a bus master on the network, this LED can be seen to migrate between communications modules on the network.
- CONFIG OK LED (Yellow) indicates that the communications module has the same configuration as the current master communications module, therefore allowing it to participate in the sharing of the master responsibilities.

6.2 ON-LINE VERIFICATION TESTS

Via the MTP in conjunction with the ITP, the I&C technician can perform manually initiated on-line verification tests to exercise the safety system logic and hardware to verify proper system operation. The ITP and the MTP also provide support for the detection and annunciation of faults by self-diagnostics. Within each PMS division, the ITP interfaces with the NIS subsystem, BPL subsystem, LCL subsystem, ILP subsystem, MTP, and the RTCB initiation relays to monitor and test the operational state of the PMS. The ITP together with the MTP provides support for on-line self-diagnostics and testing for the verification of PMS operability.

The on-line verification tests consist of the following tests:

- Sensor Input Check
- Trip Bistable Test
- Local Coincidence Logic Test
- Initiation Logic Test

Each of these tests is described in the following sections.

6.2.1 Sensor Input Check

[

]a,c

6.2.2 Trip Bistable Test

The BPL subsystem PM, bistable logic algorithms, communications modules, and interfacing wiring/networks can be tested by the ITP using manually initiated tests.

Via the MTP, ITP, and AF100 intra-division bus, the I&C technician can apply a test signal to the input of the BPL processor to force the bistable to trip. This trip is sent to the reactor trip and/or ESF LCL PMs for processing. The ITP sends the bistable trip signals from the LCLs in all four divisions to the AF100 to be displayed on the MTP and Safety Display. The displays indicate a successful transmission of the trip to the appropriate LCLs.

6.2.3 Local Coincidence Logic Test

The reactor trip and ESF LCL PM, coincidence logic algorithms, digital output modules, communications modules, and interfacing wiring/networks can be tested by the ITP using manually initiated tests.

Each LCL subsystem contains four reactor trip logic processors and two ESF logic processors. All of the processors perform the 2oo4 coincidence logic for reactor trip or Engineered Safety Features Actuation System (ESFAS), respectively. Each RT processor controls a separate digital output where the digital outputs from each processor are wired in selective 2oo4 contact matrix initiation logic for the RTCB UV and ST coil outputs. This allows the ITP to test one RT processor at a time and cause a single digital output to actuate without causing a UV or ST trip. The ITP detects if one of the legs is open and thus knows if the test was successful. This test verifies that the logic and digital outputs are functioning correctly to perform their safety function.

6.2.4 Initiation Logic Test

As part of the manually initiated LCL reactor trip testing, the I&C technician, via the ITP and MTP, can manually force the four LCL reactor trip logic processors to set their digital output module outputs to their trip state. This causes the reactor trip breakers in that division to open. The ITP processor monitors the state of the RTCBs and transmits it to the other divisions' LCLs. Administrative procedures prevent access to more than one MTP at a time, thereby preventing inadvertent tripping of more than one division of RTCBs.

6.2.5 Programmable Logic Controller Execution Test

During normal operation, the MTP and ITP monitor failure and diagnostic information from the BPL, LCL, and ILP subsystem processors as an indication of their continued operation (execution of programs). Upon detection of a failure, the ITP will generate an alarm.

6.3 CALIBRATION

Calibration of the Common Q hardware is limited to the NIS and temperature input signals.

Each NIS subsystem PR channel receives inputs from upper and lower ex-core detectors. For each detector input, the NI algorithm contains provisions for gain and offset calibration coefficients so that the upper and lower flux measurements can be adjusted for full-power operation. Since this calibration is normally performed once each shift, the capability for this calibration is provided to the operator via the safety displays in the MCR. Using the safety display, the operator navigates to the NIS calibration display and enters the calculated gain and offset coefficients for the upper and lower detectors in that division. Since each safety display is associated with a PMS division, the NIS calibration operation must be repeated four times, once for each PMS division.

For all other analog inputs, as well as pulse inputs and analog outputs, periodic manual calibration is not necessary. Calibration verification is performed for analog inputs, pulse inputs, and analog outputs. If an analog input module does not meet accuracy requirements, the module is replaced.

Calibration verification is also performed for the power supply voltages. If the associated power supply fails the calibration verification, it can be adjusted to restore the required output.

6.4 BYPASS AND PARTIAL TRIP CONDITIONS

[

]a,c

6.4.1 Bypass Condition

[

]a,c

[

]a,c

Automatic indication of bypass status is provided in the MCR in accordance with Regulatory Guide 1.47, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems” (Reference 36). [

]a,c

6.4.2 Partial Trip Condition

Manual partial trips may be established for each of the individual bistable outputs in a similar manner to the manual partial bypasses. No limit is applied for the number of partial trip conditions in the safety system. Partial trip conditions in two or more divisions of the safety system will cause the associated reactor trip breakers to trip. The Function Enable keyswitch is required to be enabled prior to setting manual partial trips.

If any un-bypassed partial trip condition (i.e., normal processing partial trips) exists, the LCL process station initiates a message on the division's AF100 bus indicating that a partial trip condition has been established. This causes a corresponding partial trip indication in the MCR.

7 SUMMARY AND CONCLUSION

[

•

•

•

•

•

•

•

]a,c

Southern Nuclear Operating Company

ND-21-0486

Enclosure 19

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

WCAP-17179-NP, "AP1000 Component Interface Module Technical Report," Revision 6

[Non-proprietary version of WCAP-17179-P, Revision 6]

(Enclosure 19 consists of 53 pages, plus this cover page)

WCAP-17179-NP
APP-GW-GLR-144
Revision 6

AP1000[®] Component Interface Module Technical Report

Stephen G. Bransfield*
Principal Engineer, Standard Hardware Components

April 2016

Technical Reviewer: Jeffrey L. Arndt*
Senior Engineer, Standard Hardware Components

Licensing Reviewer: Richard M. Paese*
Principal Licensing Engineer, US Licensing & Regulator Support

Approver: Robert B. Phillips*
Manager, Standard Hardware Components

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

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

© 2016 Westinghouse Electric Company LLC
All Rights Reserved

REVISION HISTORY**RECORD OF CHANGES**

Revision	Author	Description
0	Thomas W. Tweedle	Initial Release
1	Thomas W. Tweedle	<p>This update incorporates the following changes:</p> <ul style="list-style-type: none"> • Added additional CIM technical overview information to Section 2.1. This information includes a description of the CIM/SRNC feedback signals, and the differences between the SRNC and Ovation[®] RNC. This section has been updated as part of RAI-SRP7.0-ICE-06. • Added additional information for the Z port connections, subsection 2.3.1.1.4. This section has been updated per RAI-SRP7.0-ICE-01. • Added additional information on CIM addressing inputs and their functions, subsection 2.3.1.1.5. This section has been updated per RAI-SRP7.0-ICE-08. • Updated description of the CIM priority logic, including the block overload description, subsection 2.3.1.2.4. This section has been updated per RAI-SRP7.0-ICE-04. • Updated information on CIM modes of operation, subsection 2.3.1.2.8. This section has been updated per RAI-SRP7.0-ICE-05. • Updated information on SRNC modes of operation, subsection 2.3.2.2.6. This section has been updated per RAI-SRP7.0-ICE-05. • Updated the definitions page to define additional terms relating to the CIM/SRNC operational modes. These definitions have been updated per RAI-SRP7.0-ICE-05. • Updated the Westinghouse/CS Innovations development process to describe the high quality software development process (Section 2.7) and Figure 2-10. This section and figure have been updated per RAI-SRP7.0-ICE-11. • Updated Figure 2-3, “CIM Block Diagram,” for clarity of isolation points. This figure has been updated per RAI-SRP7.0-ICE-07. • Added References 22 and 23 to support updated text in applicable sections. • Fixed minor typographical and grammatical errors. <p>This update is a Class 3 DCP implementation.</p>

REVISION HISTORY (cont.)**RECORD OF CHANGES (cont.)**

Revision	Author	Description
2	Thomas W. Tweedle	<p>This update incorporates the following changes:</p> <ul style="list-style-type: none"> • The definition of “default state” is revised in the definitions section per RAI-SRP7.0-ICE-05. • Deleted the CIM development process description, Section 2.7, per RAI-SRP7.0-ICE-11. • Added additional information to Section 2.5.3 to describe the failure modes of the HSL/X bus links between PMS and the CIMs. This additional information is per RAI-SRP7.0-ICE-03. • Updated CIM block diagram, Figure 2-3, to more clearly define the isolation points. This update is per RAI-SRP7.0-ICE-07. • Deleted cyber security information. This information is deleted as a result of RAI-SRP-DAS-11 which states that all cyber security information shall be deleted from various technical reports, including the CIM technical report. <p>This update is a Class 3 DCP implementation.</p>
3	Stephen G. Bransfield	<p>Made following changes per DCP APP-GW-GEE-3892: Added “Black Box Testing” to the DEFINITIONS Revised Section 2.9.4, Human Diversity, to align with AP1000 PMS-DAS Diversity White Paper, IC-12-041.</p>
4	Stephen G. Bransfield	<p>The bracketing in Section 2.9 modified. Incorporates E&DCR No. APP-GW-GEF-709.</p>
5	Stephen G. Bransfield	<p>Revised revision levels of Reference 13; WCAP-15775 to Rev. 5 and Reference 22; WCAP-17184 to Rev. 6. Incorporates E&DCR No. APP-GW-GEF-748</p>

REVISION HISTORY (cont.)**RECORD OF CHANGES (cont.)**

Revision	Author	Description
6	Stephen G. Bransfield	<p>This revision affects the following documents:</p> <p><u>Proprietary</u> WCAP-17179-P Revision 6 APP-GW-GLR-143 Revision 6</p> <p><u>Non-Proprietary</u> WCAP-17179-NP Revision 6 APP-GW-GLR-144 Revision 6</p> <p>Incorporated the following changes per DCP APP-GW-GEE-5133: CAPAL 100014591:</p> <ul style="list-style-type: none"> • Sections 2.1, 8th para; 2.3.1.1.4, 2nd para; and 2.3.1.2.4, 2nd para; revised the incorrect assertion that the Z port is not used in the AP1000 application. Changed to “A subset of CIMs receives a Z port input from the PMS in the AP1000 application.” • Section 2.3.1.2, 1st para. Revised 6105-20004 to 6105-20014, and added associated title and Reference citation. • Section 2.3.2.2, Revised 6105-10004 to 6105-10014, and added associated title and Reference citation. <p>CAPAL 100002233:</p> <ul style="list-style-type: none"> • Section 2.5.1.1.2, 1st section. Revised “1.5 Vdc” to “2.5 Vdc”. • Section 2.5.1.1.2, 3rd section. Revised “1.5 Vdc” to “2.5 Vdc”. <p>CAPALs 100023921 and 100038964:</p> <ul style="list-style-type: none"> • Section 2.9.4, 1st para. 2nd sentence. Revised “The functionality of the CIM and DAS are different, and this reduces the chances that a common cause fault can be made in both designs.” to “The functionality of the CIM and DAS are not similar, and this reduces the chances that a common error can be made in both designs.” • Section 2.9.4, 1st para. 3rd sentence. Revised “The FPGA Logic used in the DAS, as compared to the FPGA logic used in the CIM, is humanly diverse with respect to the following lifecycle activities:” to “The FPGA Logic used in the DAS maintains human diversity with respect to the FPGA logic used in the CIM for the following lifecycle activities:”

REVISION HISTORY (cont.)**RECORD OF CHANGES (cont.)**

Revision	Author	Description
6 (cont.)	Stephen G. Bransfield	<p>Revised Section 2.3.1.1.4, 2nd para; to add “when not utilized by the plant” to 2nd sentence.</p> <p>Revised Section 2.3.1.2, 2nd para; to correct location of Logic Figures.</p> <p>Revised Section 2.5.1.1.1, 4th para; to remove reference to CS Innovations proprietary.</p> <p>Revised Section 2.5.1.1.1, 6th para; to remove reference to CS Innovations proprietary.</p> <p>Revised Front Matter: (ACRONYMS and DEFFINITIONS) to indicate Advanced Logic Systems, ALS and AP1000[®] are registered trademark. Also added seven acronyms and one definition. Minor reference wording for “Default State” definition.</p> <p>Revised Front matter (REFERENCES) to update revision levels to #8, #9, #15, #16, #18 thru #21 and #23. Added: (new) #26 and citation.</p> <p>Moved content of REFERENCES #13, #14, #15 and #22 to new BIBLIOGRAPHY section and labeled REFERENCES #13, #14, #15 and #22 “Deleted”. Added appropriate Bibliog citations.</p> <p>Entire document – Per current trademark guidelines, all usage of term AP1000 is to be bold.</p>

TABLE OF CONTENTS

LIST OF TABLES	viii
LIST OF FIGURES	ix
ACRONYMS AND TRADEMARKS	x
DEFINITIONS	xii
REFERENCES	xiv
BIBLIOGRAPHY	xvi
1 INTRODUCTION	1-1
1.1 PURPOSE	1-1
1.2 SCOPE	1-1
2 TECHNICAL DESCRIPTION	2-1
2.1 CIM SYSTEM OVERVIEW	2-1
2.2 CIM SYSTEM DESCRIPTION	2-2
2.3 HARDWARE DESCRIPTION	2-4
2.3.1 Component Interface Module	2-4
2.3.2 Safety Remote Node Controller	2-12
2.3.3 Transition Panels	2-16
2.3.4 Base Plates	2-17
2.3.5 Branch Terminator	2-21
2.4 SYSTEM INTERFACES	2-21
2.4.1 Communications Interfaces	2-21
2.4.2 Class 1E/Non-1E Isolation	2-22
2.4.3 Discrete Interfaces	2-22
2.4.4 Actuators Controlled by CIM	2-22
2.5 SYSTEM DIAGNOSTICS AND FAULT INDICATIONS	2-23
2.5.1 Diagnostics	2-23
2.5.2 Fault Indications	2-26
2.5.3 X Bus Failures	2-29
2.6 SYSTEM OPERATION	2-29
2.6.1 Time Response	2-29
2.6.2 CIM and SRNC Operational Modes	2-29
2.7 EQUIPMENT QUALIFICATION	2-29
2.8 RELIABILITY	2-30
2.8.1 FMEA	2-30
2.8.2 MTBF	2-30
2.9 DIVERSITY	2-30
2.9.1 Design Diversity	2-30
2.9.2 Equipment Diversity	2-31
2.9.3 Functional Diversity	2-31
2.9.4 Human Diversity	2-31
2.9.5 Signal Diversity	2-31

TABLE OF CONTENTS (cont.)

2.9.6 Software Diversity.....2-32

2.9.7 Diversity Summary.....2-32

2.10 HUMAN FACTORS AND MAINTENANCE CONSIDERATIONS.....2-32

2.11 OPERATING HISTORY2-33

3 REGULATORY COMPLIANCE3-1

3.1 IEEE 603.....3-1

3.2 DI&C-ISG-043-1

3.2.1 DI&C-ISG-04, Section 1, “Interdivisional Communications”3-1

3.2.2 DI&C-ISG-04, Section 2, “Command Prioritization”3-3

TABLE OF CONTENTS (cont.)

LIST OF TABLES

Table 2-1 CIM LED Designations2-6
Table 2-2 SRNC LED Designations2-12

TABLE OF CONTENTS (cont.)**LIST OF FIGURES**

Figure 2-1	CIM System	2-3
Figure 2-2	CIM Output Devices	2-5
Figure 2-3	CIM Block Diagram	2-11
Figure 2-4	SRNC Block Diagram	2-15
Figure 2-5	Double Width Transition Panel	2-16
Figure 2-6	Single Width Transition Panel	2-17
Figure 2-7	CIM Base Plate with CIMs Installed	2-18
Figure 2-8	SRNC Base Plate with SRNCs Installed	2-20
Figure 2-9	Overlap Testing	2-24

ACRONYMS AND TRADEMARKS

Acronyms used in the document are defined in WNA-PS-00016-GEN, “Standard Acronyms and Definitions” (Reference 16), or included below to ensure unambiguous understanding of their use within this document.

Acronym	Definition
ABB	Asea Brown Boveri, Inc.
AC160	Advant Controller 160
ALS	Advanced Logic System
AOV	Air Operated Valve
CIM	Component Interface Module
CRC	Cyclic Redundancy Check
DAS	Diverse Actuation System
DC	Direct Current
DC/DC	Direct Current to Direct Current
DWTP	Double Width Transition Panel
EIA	Electronic Industries Alliance (now disbanded)
EMC	Electromagnetic Compatibility
ESD	Electrostatic Discharge
FMEA	Failure Mode and Effects Analysis
FPGA	Field Programmable Gate Array
HSL	High Speed Link
I&C	Instrumentation and Control
I/O	Input/Output
ISG	Interim Staff Guidance
LED	Light Emitting Diode
MOV	Motor Operated Valve
MTBF	Mean Time Before Failure
NRC	Nuclear Regulatory Commission
PCB	Printed Circuit Board
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
RNC	Remote Node Controller
RX	Receive
SOV	Solenoid Operated Valve
SRNC	Safety Remote Node Controller
SWTP	Single Width Transition Panel
TIA	Telecommunications Industry Association
TWI	Two Way Interface
TX	Transmit
Vdc	Voltage Direct Current

ACRONYMS AND TRADEMARKS (cont.)

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

Advanced Logic System, ALS, and AP1000[®] are trademarks or registered trademarks of Westinghouse Electric Company LLC, its affiliates and/or its subsidiaries in the United States of America and may be registered in other countries throughout the world. All rights reserved. Unauthorized use is strictly prohibited. Other names may be trademarks of their respective owners.

Ovation[®] is a registered trademark of Emerson Process Management.

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

DEFINITIONS

Term	Definition
AC160	Asea Brown Boveri (ABB) Advant [®] Controller Series 160. An ABB open control system family product line.
Black Box Testing	The testing of a component or system in the target hardware without reference to the internal structure of the component or system. Testing focuses solely on the outputs generated in response to selected inputs and execution conditions.
CIM System	A system of Component Interface Module (CIM) components that work together to provide component control with command prioritization from safety and non-safety systems. The CIM system components consist of the CIM, Safety Remote Node Controller (SRNC), Double Width Transition Panel (DWTP), Single Width Transition Panel (SWTP), and branch terminator.
Default State	<p>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.</p> <p>The default state of the CIM output devices is described in R004.50, “Component Interface Module Hardware Requirements Specification,” WNA-DS-01271-GEN, (Reference 8). [</p> <p style="text-align: center;">] ^{a,c}</p> <p>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 Specification” WNA-DS-01272-GEN, (Reference 9). [</p> <p style="text-align: center;">] ^{a,c}</p>
Operational Mode	A mode of operation where the power supplied to the Field Programmable Gate Array (FPGA) is within the predetermined acceptable range. In this mode, the CIM and SRNC are fully functional and operational.

DEFINITIONS (cont.)

Term	Definition
Ovation	A real-time monitoring and control system product of Emerson Process Management.
PM646A	The processor module that is used in the AC160 application.
Reset Mode	[
] ^{a,c}
RS422 or RS485	<p>Standard communication interfaces. These former Electronic Industries Alliance (EIA) standards are now maintained by the Telecommunications Industry Association (TIA) and define electrical characteristics of drivers and receivers used in digital communication systems.</p> <p>RS422 utilizes a single driver circuit and up to 10 receivers in a balanced digital interface circuit point-to-point or multi-drop topology.</p> <p>RS485 is an improvement over RS422 and allows for up to 32 loads (drivers or receivers) in a balanced digital interface circuit multipoint system.</p>
Two Way Interface (TWI) Connector	A standard connector that is used in the CIM system.

REFERENCES

1. IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Inc.
2. Deleted.
3. "Interim Staff Guidance, Digital Instrumentation and Controls, DI&C-ISG-04, Task Working Group #4, Highly-Integrated Control Rooms – Communications Issues (HICRc)," U.S. Nuclear Regulatory Commission, September 2007.
4. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems," Lawrence Livermore Nuclear Laboratory, December 1994.
5. Deleted.
6. 10 CFR 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," U.S. Nuclear Regulatory Commission, August 2007.
7. Regulatory Guide 1.106, Rev. 1, "Thermal Overload Protection for Electric Motors on Motor-Operated Valves," U.S. Nuclear Regulatory Commission, March 1977.
8. WNA-DS-01271-GEN (Proprietary), Rev. 10, "Component Interface Module Hardware Requirements Specification," Westinghouse Electric Company LLC.
9. WNA-DS-01272-GEN (Proprietary), Rev. 9, "Safety System Remote Node Controller Requirements Specification," Westinghouse Electric Company LLC.
10. Deleted.
11. Deleted.
12. Deleted.
13. Deleted.
14. Deleted
15. Deleted
16. WNA-PS-00016-GEN (Proprietary), Rev. 7, "Standard Acronyms and Definitions," Westinghouse Electric Company LLC.
17. Deleted.

REFERENCES (cont.)

18. 6105-10003 (Proprietary), Rev. 4, "SRNC Hardware Specification," Westinghouse Electric Company LLC.
19. 6105-20003 (Proprietary), Rev. 4, "CIM Hardware Specification," Westinghouse Electric Company LLC.
20. 6105-10004 (Proprietary), Rev. 13, "SRNC FPGA Software Requirements Specification," Westinghouse Electric Company LLC.
21. 6105-20004 (Proprietary), Rev. 17, "CIM FPGA Software Requirements Specification," Westinghouse Electric Company LLC.
22. Deleted.
23. APP-PMS-J4-102 (Proprietary), Rev. 14, "AP1000 Protection and Safety Monitoring System Software Requirements Specification," Westinghouse Electric Company LLC.
24. 6105-10014 (Proprietary), Rev. 5, "SRNC FPGA Software Design Description," Westinghouse Electric Company LLC.
25. 6105-20014 (Proprietary), Rev. 5, "CIM FPGA Software Design Description," Westinghouse Electric Company LLC.
26. WNA-DS-02331-GEN (Proprietary), Rev. 2, "Component Interface Module Logic Specification," Westinghouse Electric Company LLC.

BIBLIOGRAPHY

The following is a list of sources that were considered in preparing this document. Revisions cited were consulted at the time of writing. Revisions to the documents listed below do not require a revision to this document; therefore users should consult the latest approved revision.

1. WCAP-15775 (Non-Proprietary), Rev. 5, "AP1000 Instrumentation and Control Defense-In-Depth and Diversity Report," Westinghouse Electric Company LLC.
2. WCAP-17184-P (Proprietary), Rev. 6, "AP1000[®] Diverse Actuation System Planning and Functional Design Summary Technical Report," Westinghouse Electric Company LLC.
3. WCAP-15776, Rev. 0, "Safety Criteria for the AP1000 Instrumentation and Control Systems," Westinghouse Electric Company LLC.
4. WCAP-16438-P (Proprietary), Rev. 6, "FMEA of AP1000 Protection and Safety Monitoring System," Westinghouse Electric Company LLC.

1 INTRODUCTION

1.1 PURPOSE

The purpose of this report is to describe the Component Interface Module (CIM) system components. The intent of this technical report is to obtain U.S. Nuclear Regulatory Commission (NRC) review and approval for use of the CIM system components in the **AP1000** nuclear safety-related instrumentation and control (I&C) application, and to identify the bounding conditions under which approval is granted.

The CIM system components 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. The CIM system components have been developed as nuclear safety-related (Class 1E) products by CS Innovations, a 10 CFR Part 50, Appendix B supplier (Reference 6) and wholly owned subsidiary of Westinghouse Electric Company.

1.2 SCOPE

The scope of this report is limited to the CIM system components. These components include the hardware and their associated external interfaces []^{a,c} described in Section 2.2. This technical report considers the CIM system applied in the **AP1000**.

2 TECHNICAL DESCRIPTION

2.1 CIM SYSTEM OVERVIEW

The CIM system is designed to interface a field component to the Protection and Safety Monitoring System (PMS) and the Plant Control System (PLS). The CIM priority logic function arbitrates between PMS and PLS demands. The CIM component control logic generates a component demand based on the priority logic outputs and field component feedback signals.

Communication with the PMS is accomplished with the Safety Remote Node Controller (SRNC) assembly. []^{a,c} The SRNC module accepts a high speed link (HSL) connection. []^{a,c}

The SRNC communicates with each CIM through a safety bus known as the X bus. The X bus is an independent, bidirectional link between the CIM and the SRNC. The PMS communication link is known as the X port. The SRNC assembly and X bus structure is depicted in Figure 2-1.

The PMS can send an open, close, or stop demand. In addition to the PMS demands received over port X, the PMS can also send three configuration commands to the CIM. These commands are port Y enable, maintenance mode, and output test enable. []^{a,c}

The CIM feedback and status signals are transmitted to the SRNC via the X bus. The CIM and SRNC status and feedback signals are transmitted to Common Q via the HSL. []^{a,c}

The CIMs communicate with the PLS through an Ovation[®] Remote Node Controller (RNC). The Ovation RNC bus is known as the Y bus. The CIM can receive PLS demands from the RNC and transmit status feedback information to the RNC.

The Ovation RNC and the SRNC are physically different modules, designed and built by different companies. The Ovation equipment is a standard Emerson Process Management product. The SRNC (and CIM) have been developed by CS Innovations for the **AP1000** application. The SRNC modules do not fit into or connect with the Ovation RNC modules or base plate assembly. The Ovation RNC connection is a fiber optic connection, while the SRNC connection is a DB-25 copper connection. The physical differences between the Ovation RNC and SRNC preclude maintenance errors.

A manual control located on each CIM provides local maintenance and test features for each field component. []^{a,c} A status bit is sent to the PMS and PLS processors when local mode is enabled.

The CIM has two Z port inputs that can be used for connection with a high priority system. A subset of CIMs receives a Z port input from the PMS in the **AP1000** application.

2.2 CIM SYSTEM DESCRIPTION

The CIM system comprises one to thirty-two CIMs assembled on one to sixteen CIM base plates, two SRNCs assembled on one SRNC base plate, one double width transition panel (DWTP), up to two single width transition panels (SWTP), and one to four branch terminating devices. The CIM system can have one to four branches of CIMs; each branch can have one to eight CIMs. Each CIM controls one component, and each CIM base plate can accommodate one or two CIMs. The SRNC base plate provides for two SRNC modules that comprise the redundant safety system communication.

The DWTP connects two branches of CIMs to the SRNC base plate, redundant 24 volts direct current (Vdc) power supplies and the non-safety Ovation RNC. The DWTP also provides two connectors for interconnection with the SWTP. The SWTP connects one branch of CIMs to the DWTP.

The CIM base plate back plane printed circuit board (PCB) distributes the X and Y buses to each CIM and extends the X and Y buses to the next base plate. The CIM back plane PCB also distributes redundant power supply feeds to each CIM and extends the power supply feeds to the next base plate. The base plate connects the CIM to the field component through the use of terminal blocks, facilitating rapid maintenance and repair activities without disturbing field wiring.



a,c

Figure 2-1. CIM System

2.3 HARDWARE DESCRIPTION

The five standard components of the CIM system are described below.

2.3.1 Component Interface Module

[]^{a,c}

2.3.1.1 Module Level Functional Description

2.3.1.1.1 Power Supply

The CIM supports a redundant 24 Vdc power supply feed. The redundant power supply feed is []^{a,c} utilized within the CIM. Transient voltage suppression is provided for over voltage protection. [

]^{a,c}

2.3.1.1.2 Field Input Circuits

The CIM supports []^{a,c} digital inputs that can receive field component feedback information.

[

]^{a,c} The status of each field input is available to the PMS and the PLS.

[

]^{a,c}

2.3.1.1.3 Local Control Input Circuits

The CIM includes a local control interface located on the front panel of the CIM. [

]^{a,c} The status of the local control []^{a,c} is available to the PMS and the PLS for indication of CIM status.

2.3.1.1.4 Z Port Input Circuits

The CIM supports two digital inputs that can receive commands from a high priority system.

[

]^{a,c}

[]

]^{a,c} The design of the Z port terminal connections are dissimilar to the connections used for the X and Y ports. The Z port terminal block connections are designed to mitigate a short circuit condition across the terminal connectors. Normal maintenance activities do not utilize the Z port input connections, thus precluding a maintenance error.

2.3.1.1.5 Address Input Circuits

[

]^{a,c}

2.3.1.1.6 Output Circuits

The CIM has two outputs to interface with the field device. [

]^{a,c}

]^{a,c}

Figure 2-2. CIM Output Devices

2.3.1.1.7 LED Indicators

The CIM has twenty-one light emitting diodes (LEDs) located on the front panel for indication of the module status. [

]^{a,c}

2.3.1.2 FPGA Level Functional Description

[

] ^{a,c}

2.3.1.2.1 X Bus Communication Functions

The X bus communication function provides the communications interface between the CIM and SRNC.

[

] ^{a,c} The X bus protocol is described

in subsection 2.4.1.2.

[

] ^{a,c}

2.3.1.2.2 Y Bus Communication Functions

The Y bus communication function provides the communications interface between the CIM and Ovation RNC. The Y bus protocol is described in subsection 2.4.1.3.

[

] ^{a,c}

[

] ^{a,c}

2.3.1.2.3 Communication Buffers

[

] ^{a,c}

2.3.1.2.4 Priority Logic

[

] ^{a,c}

The priority logic function takes inputs from the X port, Y port, Z port and local control port. [

] ^{a,c}

The priority logic module has [] ^{a,c} output signals that interface to the component control logic.

[

] ^{a,c}

2.3.1.2.5 Component Control Logic

The component control logic interfaces the field component with the []^{a,c} priority logic. The component control logic utilizes []^{a,c} feedbacks from the field component. []

[]^{a,c} The PLS and the PMS monitor the available feedback from the component and can generate discrepancy detection signals if the component motion does not start or if the component does not reach the commanded state in a predetermined amount of time.

[]

[]^{a,c}

2.3.1.2.6 LED Control Module

The LED control module is used to interface the CIM FPGA with twenty-one LED indicators (subsection 2.3.1.1.7). The LED control module receives status and control information from the field inputs, outputs, internal logic states and test functions to determine the status of each indicator.

2.3.1.2.7 FPGA Test Functions

The CIM FPGA contains []^{a,c} test features for the safety system actuation path. These test features are described in subsection 2.5.1.1.1.

2.3.1.2.8 Operational Modes of the CIM

The CIM has design features to provide deterministic operation of the CIM. []

[]^{a,c}

[

|

]a,c



a,c

Figure 2-3. CIM Block Diagram

2.3.2 Safety Remote Node Controller

[]^{a,c}

2.3.2.1 Module Level Functional Description

2.3.2.1.1 Power Supply

The SRNC supports a redundant 24 Vdc power supply feed. The redundant power supply feed is []^{a,c} utilized within the SRNC. Transient voltage suppression is provided for over voltage protection. []

] ^{a,c}

2.3.2.1.2 LED Indicators

The SRNC has seven light emitting diodes (LEDs) located on the front panel for indication of the module status. []

] ^{a,c}

Table 2-2 SRNC LED Designations		

a,c

2.3.2.2 FPGA Level Functional Description

[]^{a,c}

*** This record was final approved on 9/23/2020 5:37:30 PM. (This statement was added by the PRIME system upon its validation)

2.3.2.2.1 HSL Communication Functions

The HSL communication functions interface the SRNC to the PM646A. [

] ^{a,c}

2.3.2.2.2 X Bus Communication Functions

[

] ^{a,c}

2.3.2.2.3 Communication Buffers

[

] ^{a,c}

2.3.2.2.4 LED Control Module

The LED control module is used to interface the SRNC FPGA with seven LED indicators (subsection 2.3.2.1.2). The LED control module receives status and diagnostic information to determine the status of each indicator.

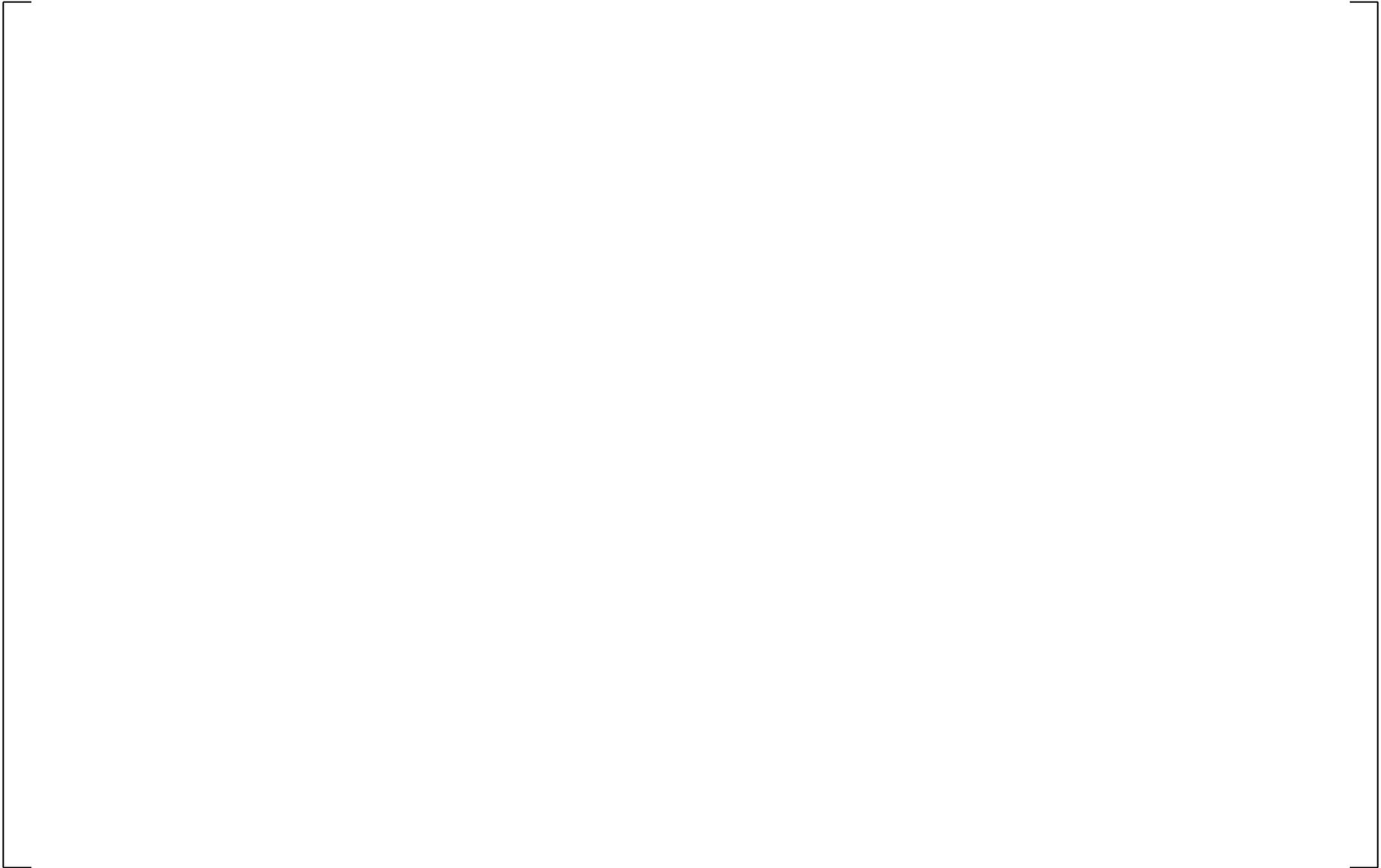
2.3.2.2.5 FPGA Test Functions

The SRNC FPGA contains []^{a,c} test features for the safety system actuation path. These test features are described in subsection 2.5.1.1.1.

2.3.2.2.6 Operational Modes of the SRNC

The SRNC has design features to provide deterministic operation of the SRNC. []

[]^{a,c}



a,c

Figure 2-4. SRNC Block Diagram

2.3.3 Transition Panels

2.3.3.1 Double Width Transition Panel

The DWTP connects []^{a,c} CIM base plates to the SRNC base plate, Ovation RNC assembly, and redundant 24 Vdc power feeds. []

] ^{a,c}] ^{a,c}

Figure 2-5. Double Width Transition Panel

2.3.3.2 Single Width Transition Panel

The SWTP connects one CIM base plate branch to the DWTP. []

] ^{a,c}



Figure 2-6. Single Width Transition Panel

2.3.4 Base Plates

The CIM and SRNC base plates provide a physical mounting location for the CIM and SRNC modules.

[]^{a,c}

2.3.4.1 CIM Base Plate

[

] ^{a,c}

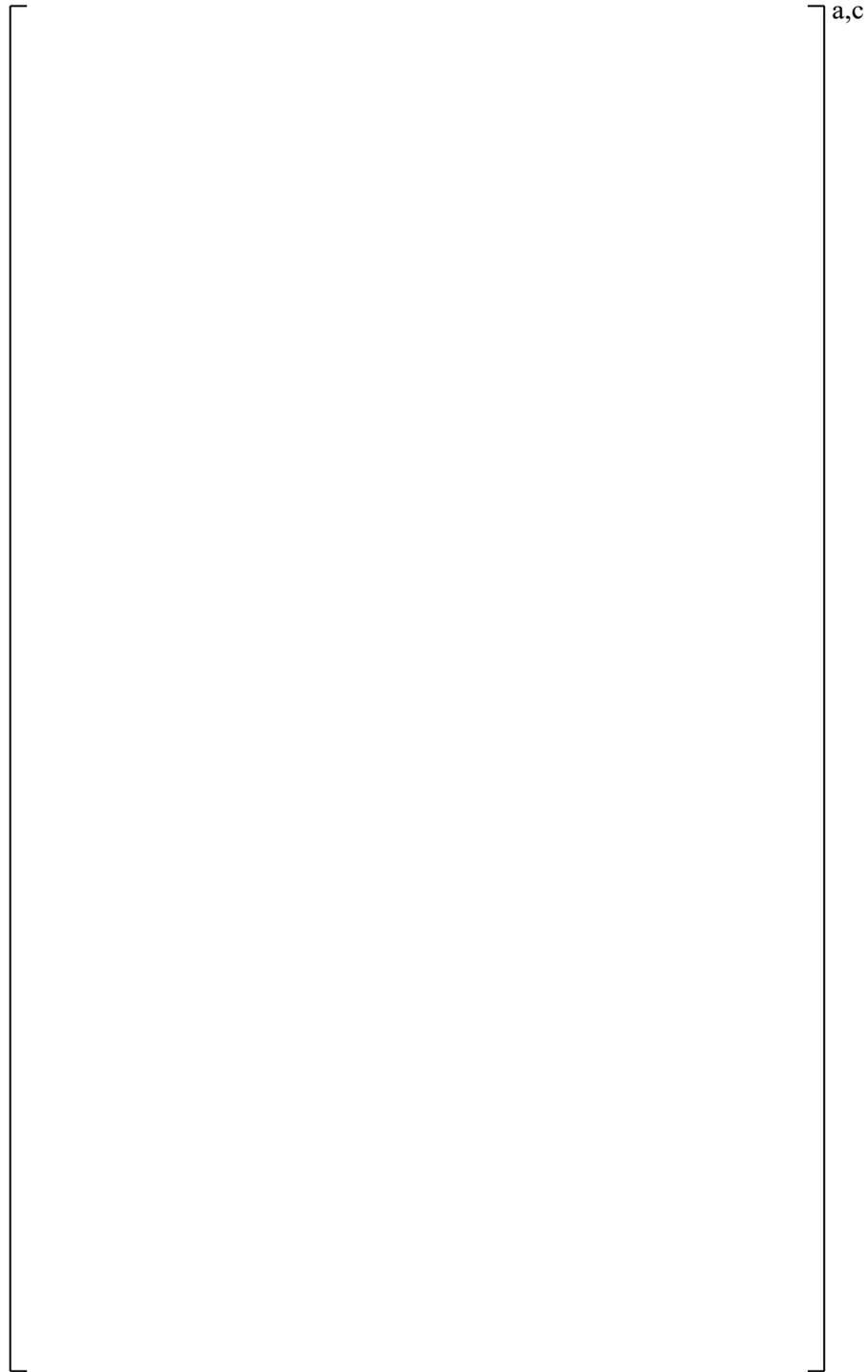


Figure 2-7. CIM Base Plate with CIMs Installed

Note: This figure is for illustrative purposes only and may not represent the final configuration or connection as installed into the PMS.

2.3.4.2 SRNC Base Plate

[

] ^{a,c}

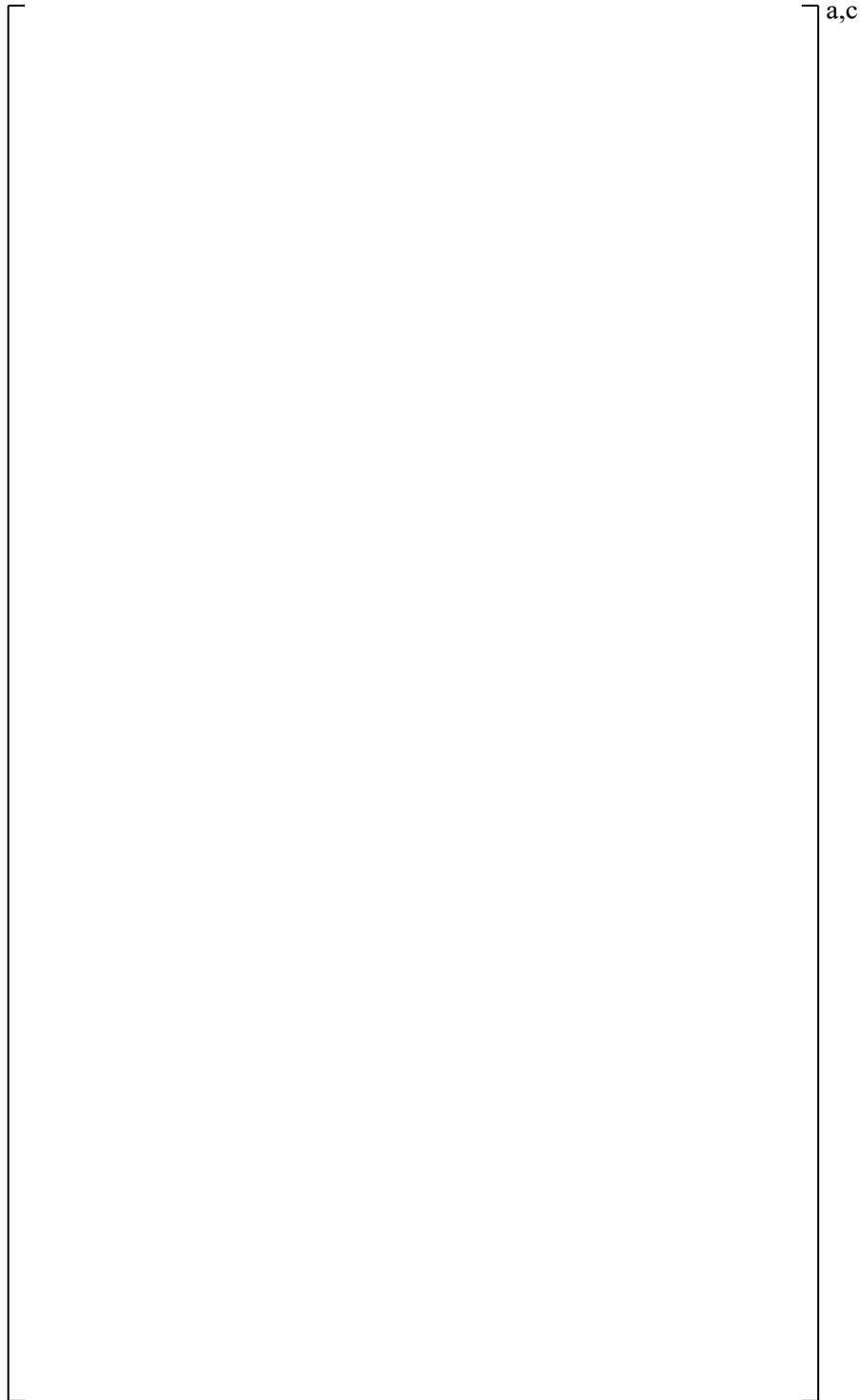


Figure 2-8. SRNC Base Plate with SRNCs Installed

Note: This figure is for illustrative purposes only and may not represent the final configuration or connection as installed into the PMS.

2.3.5 Branch Terminator

The branch terminator is installed on the last CIM base in each branch. [

] ^{a,c}

2.4 SYSTEM INTERFACES

2.4.1 Communications Interfaces

2.4.1.1 High Speed Link

The PM646A processor and SRNC module communicate with the HSL protocol. [

] ^{a,c}

2.4.1.2 X Bus

The communication protocol that CIMs and the SRNC use to communicate is the X bus protocol.
[

] ^{a,c}

2.4.1.3 Y Bus

The communication protocol that is used with the PLS is the Ovation I/O bus. [

] ^{a,c}

2.4.2 Class 1E/Non-1E Isolation

[

] ^{a,c}

2.4.3 Discrete Interfaces

The CIM has four sets of discrete interfaces that are used for control and connection with plant components. The field input circuits (subsection 2.3.1.1.2) connect with status feedback indicators that receive component status information. The local control input circuits (subsection 2.3.1.1.3) provide a local interface for the CIM. [^{a,c}

The Z port input circuits (subsection 2.3.1.1.4) connect with a high priority system. The CIM outputs (subsection 2.3.1.1.5) interface the CIM open and close commands to the field device.

2.4.4 Actuators Controlled by CIM

The CIM interfaces with components of the following types:

- Motor Control Centers
- AOVs
- SOVs
- Circuit Breakers
- Squib Valves

[

] ^{a,c}

2.5 SYSTEM DIAGNOSTICS AND FAULT INDICATIONS

2.5.1 Diagnostics

2.5.1.1 Continuous Diagnostics

2.5.1.1.1 Safety Path Testing

[

] ^{a,c}

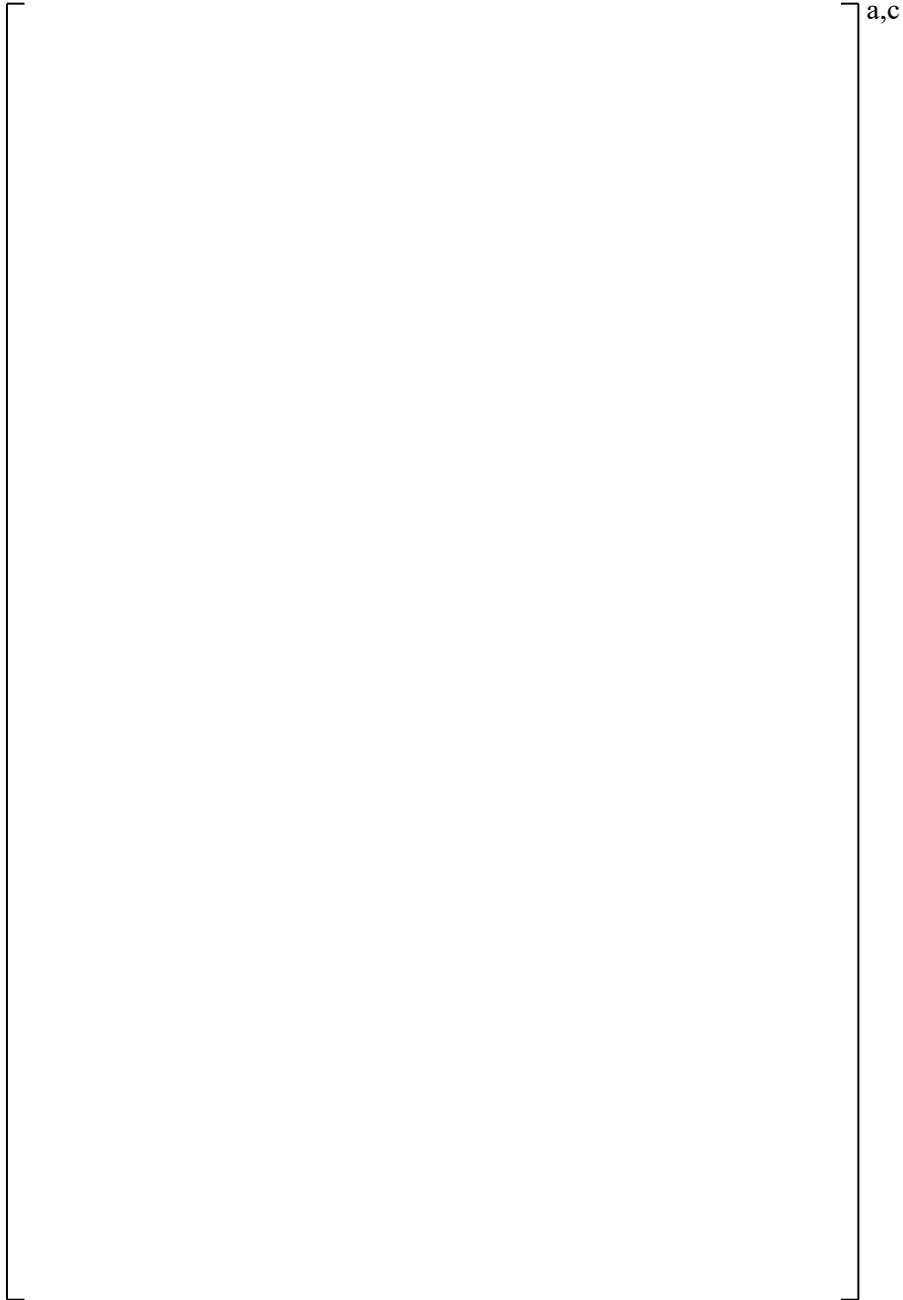


Figure 2-9. Overlap Testing

[

] a,c

[

|

] ^{a,c}

2.5.1.1.2 Additional Continuous Diagnostics

The following sections detail additional diagnostics for the CIM and SRNC modules that support safety path testing.

SRNC – Power Supply Monitors

The SRNC monitors the 24 Vdc power supply feed [] ^{a,c} to ensure the supplied voltage is within the operating range of the SRNC. If the voltage is not within range, the SRNC will visually indicate this condition on the front panel status LEDs, as well as transmit this condition to the PMS and the PLS.

| [

] ^{a,c}

CIM – Ground Fault Detection

The field feedback inputs are provided with ground fault detection capabilities. A ground fault occurs if there is current flow between the field input channel and earth ground. This condition is transmitted to the PMS and the PLS.

CIM – Power Supply Monitors

The CIM monitors the 24 Vdc power supply feed to ensure the supplied voltage is within the operating range of the CIM. [

] ^{a,c}

[

] ^{a,c}

2.5.1.2 Periodic Diagnostics

[

] ^{a,c}

2.5.2 Fault Indications

2.5.2.1 Local Indications

Specific fault indications are indicated locally on CIM and SRNC front panel LED display. The fault indications are listed as follows. For an explanation of the front panel indicators, see subsection 2.3.1.1.7 for the CIM and subsection 2.3.2.1.2 for the SRNC.

CIM:

- [] ^{a,c}
- 24V-A LED indicator not lit: The 24V-A power supply feed does not have a voltage applied that is in the operating range of the CIM.
- 24V-B LED indicator not lit: The 24V-B power supply feed does not have a voltage applied that is in the operating range of the CIM.
- Flashing Z-Port LED indicator: Ground fault or 48 Vdc wetting power supply failure.
- Flashing Field Input LED indicator: Ground fault or 48 Vdc wetting power supply failure.
- X bus indicator not lit: The CIM is not communicating on the X bus.
- Y bus indicator not lit: The CIM is not communicating on the Y Bus.

SRNC:

- 24V-A LED indicator not lit: The 24V-A power supply feed does not have a voltage applied that is in the operating range of the CIM.
- 24V-B LED indicator not lit: The 24V-B power supply feed does not have a voltage applied that is in the operating range of the CIM.
- X bus indicators: LED indicators are provided for the X bus branches. The indicator is not lit when the SRNC is not communicating on the specific X bus branch.
- HSL indicator not lit: The SRNC is not communicating across the HSL.

2.5.2.2 Remote Indications

Specific fault indications are sent to the PMS and the PLS via each respective communication link. The following list details the fault indications that are sent:

CIM:

- [

] ^{a,c}

- [

] ^{a,c}

SRNC:

- [

] ^{a,c}

2.5.3 X Bus Failures

[

] ^{a,c}

2.6 SYSTEM OPERATION

2.6.1 Time Response

Time response of the CIM system is defined by the requirements listed in References 8 and 9.

2.6.2 CIM and SRNC Operational Modes

Operational mode of the CIM and SRNC modules will begin once the transition from reset mode has occurred (subsections 2.3.1.2.8 and 2.3.2.2.6). The operational mode of the CIM and SRNC is not affected during different modes (test, normal operation, etc.) the plant may operate in. The CIM priority and component control logic does not change for any plant operational mode.

2.7 EQUIPMENT QUALIFICATION

The CIM system components will undergo two sets of equipment qualification tests. The first set will be completed under the CS Innovations process. [

] ^{a,c} The second set of tests will be conducted under the Westinghouse process.

[

] ^{a,c}

[

] ^{a,c}

2.8 RELIABILITY

2.8.1 FMEA

The Failure Mode and Effects Analysis (FMEA) is a qualitative evaluation which identifies failure modes that contribute to a system's unreliability. The FMEA identifies significant single failures and their effects or consequences on the system's ability to perform its functions. [

] ^{a,c}

2.8.2 MTBF

[

] ^{a,c}

2.9 DIVERSITY

WCAP-15775, "AP1000 Instrumentation and Control Defense-In-Depth and Diversity Report" (Bibliog 1), provides a diversity evaluation for the overall plant design. WCAP-17184, "AP1000 Diverse Actuation System Planning and Functional Design Summary Technical Report" (Bibliog 2), addresses the diversity that is provided in the I&C system. The following evaluation will focus on the diversity requirements for the CIM and SRNC and support the two aforementioned diversity evaluations.

The CIM and SRNC provide the control of the safety-related components through the PMS. This actuation path must be diverse from the path that is provided in the Diverse Actuation System (DAS). The Advanced Logic System (ALS) is the core of the DAS. This evaluation will focus on the diversity between the CIM and ALS, and evaluates each of the elements of diversity included in NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems" (Reference 4).

2.9.1 Design Diversity

Design diversity is the use of different methods to solve similar problems. Both the DAS and CIM are based on FPGA technology, but different FPGAs are used. [

] ^{a,c}

The architectures of the DAS and CIM are different. The DAS architecture is based on input, output, and logic boards that are in a card rack. [

] ^{a,c}

2.9.2 Equipment Diversity

Equipment diversity is the use of different hardware to perform similar safety functions. For the purposes of equipment diversity, “different” means sufficiently dissimilar as to significantly decrease vulnerability to a common failure. As described previously, the DAS and CIM use different FPGAs in different architectures. There are no common hardware modules used in the CIM and DAS designs, the internal communication is different and the power supply is different.

2.9.3 Functional Diversity

Two systems are functionally diverse if they perform different physical functions though they may have overlapping safety effects. [

] ^{a,c} The CIM and DAS both actuate plant components, but the actuation paths are different.

2.9.4 Human Diversity

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

The functionality of the CIM and DAS are not similar, and this reduces the chances that a common error can be made in both designs. The FPGA Logic used in the DAS maintains human diversity with respect to the FPGA logic used in the CIM, for the following lifecycle activities:

- Design Activities (i.e., different FPGA logic design teams for activities such as the preparation of design specifications and development of the application logic in the hardware descriptive language)
- Implementation Activities (i.e., different FPGA logic design teams for activities required to physically program the FPGA chip such as simulation, synthesis and “place and route” tasks)
- Black Box Test Activities (i.e., different IV&V test teams).

2.9.5 Signal Diversity

Signal diversity is the use of different sensed parameters to initiate protective action. [

] ^{a,c} The inputs are different, and there are no common signals between the two designs.

2.9.6 Software Diversity

Software diversity is the use of different programming or algorithms to perform the same or similar functions. The CIM and SRNC do not contain any software. The functionality of the DAS and CIM are different, and there are no algorithms that are in common between the two designs. [

] ^{a,c}

2.9.7 Diversity Summary

All of the elements must be evaluated to determine if adequate diversity is provided. By partitioning and assigning design tasks, different designers were used for the CIM and DAS designs. There is no common logic used in the DAS and CIM designs. The designs perform fundamentally different functions, and this provides diversity in signals and functions that are used. There is no common hardware used in the design. This includes the use of different FPGAs. Based on all of the elements of diversity, sufficient diversity between the CIM and DAS is provided.

2.10 HUMAN FACTORS AND MAINTENANCE CONSIDERATIONS

The following human factors considerations have been incorporated into the designs of the CIM and SRNC modules. These human factors considerations support maintenance and test features for PMS.

- [

] ^{a,c}

- Module Replacement

The CIM and SRNC base plates have been designed with rigid metal guides to ensure proper module alignment and mating with the backplane. The modules have two thumb screw fasteners to secure the module into the base plate assembly.

- Module Indicators

The CIM and SRNC indicators are straightforward in their design to minimize the chance of misinterpretation. Failures and off-normal conditions are clearly indicated by the behavior of the module indicators.

- Pre-configured Modules

CIM and SRNC FPGA cores are configured prior to shipment and cannot be altered by the customer. This approach improves configuration control of CIM system components and prevents maintenance errors.

- Electrostatic Discharge (ESD)

The CIM and SRNC are qualified for ESD resistance.

- Local Controls

The CIM local controls are designed for their ease of use and indication. [

] ^{a,c}

- Test Points

The CIM base plate is designed with test points and field disconnect terminal blocks to aid in maintenance and troubleshooting activities. The field disconnects and test points can be used to test the signal path without disconnecting any field wiring from the base plate.

2.11 OPERATING HISTORY

The CIM function has been previously utilized in operating nuclear power plants. The CIM system components are newly designed assemblies and thus have no operating history. The first planned use of the redesigned CIM system assemblies is for the **AP1000** application.

3 REGULATORY COMPLIANCE

3.1 IEEE 603

IEEE 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations” (Reference 1), establishes the minimum functional design criteria for the power, instrumentation, and control portions of nuclear power generating station safety systems. The criteria established in IEEE 603 provide a means for promoting safe practices for design and evaluation of safety system performance and reliability. [

] ^{a,c}

3.2 DI&C-ISG-04

The NRC Task Working Group #4, “Highly Integrated Control Rooms – Communications Issues” (Reference 3), has provided interim NRC staff guidance on the review of communications issues. The interim NRC staff guidance contains three sections: Interdivisional Communications, Command Prioritization, and Multidivisional Control and Display Stations. The third section provides guidance for control displays, which is not applicable to components of the CIM system.

3.2.1 DI&C-ISG-04, Section 1, “Interdivisional Communications”

Section 1 of DI&C-ISG-04 (Reference 3) provides guidance on communications, including transmission of data and information, among components in different electrical safety divisions and communications between a safety division and equipment that is not safety-related. This interim staff guidance (ISG) does not apply to communications within a single division. The ISG provides twenty staff positions in this section. The following statements are the responses to each of the twenty staff positions provided in the ISG.

[

] ^{a,c}

[

] ^{a,c}

[

] ^{a,c}

3.2.2 DI&C-ISG-04, Section 2, “Command Prioritization”

Section 2 of DI&C-ISG-04 (Reference 3) provides guidance applicable to a prioritization device, which receives device actuation commands from multiple safety and non-safety sources, and sends the command having highest priority on to the actuated device. The ISG provides ten staff positions in this section. The following statements are the responses to each of the ten staff positions provided in the ISG.

[

] ^{a,c}

Southern Nuclear Operating Company

ND-21-0486

Enclosure 20

Vogtle Electric Generating Plant (VEGP) Units 3 and 4

**Westinghouse Electric Company Application for Withholding Proprietary Information
from Public Disclosure and Accompanying Affidavit CAW-20-5095**

(Enclosure 20 consists of 3 pages, plus this cover page)

Westinghouse Non-Proprietary Class 3

CAW-20-5095
Page 1 of 3AFFIDAVIT

COMMONWEALTH OF PENNSYLVANIA:

COUNTY OF BUTLER:

- (1) I, Zachary S. Harper, have been specifically delegated and authorized to apply for withholding and execute this Affidavit on behalf of Westinghouse Electric Company LLC (Westinghouse).
- (2) I am requesting the proprietary portions of WCAP-17179-P, Revision 6 be withheld from public disclosure under 10 CFR 2.390.
- (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 10 CFR 2.390, 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 and is not customarily disclosed to the public.
 - (ii) 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 technical evaluation justifications 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.

Westinghouse Non-Proprietary Class 3

CAW-20-5095

Page 2 of 3

AFFIDAVIT

- (5) Westinghouse has policies in place to identify proprietary information. 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.
- (6) The attached documents are bracketed and marked to indicate the bases for withholding. The justification for withholding 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

AFFIDAVIT

lower case letters refer to the types of information Westinghouse customarily holds in confidence identified in Sections (5)(a) through (f) of this Affidavit.

I declare that the averments of fact set forth in this Affidavit are true and correct to the best of my knowledge, information, and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: 9/18/2024


Zachary S. Harper, Manager
Licensing Engineering