October 24, 2003

Mr. Gregg R. Overbeck
Senior Vice President, Nuclear
Arizona Public Service Company
P. O. Box 52034
Phoenix, AZ 85072-2034

SUBJECT: PALO VERDE NUCLEAR GENERATING STATION, UNITS 1, 2, AND 3 - ISSUANCE OF AMENDMENTS ON THE CORE PROTECTION CALCULATOR SYSTEM UPGRADE (TAC NOS. MB6726, MB6727, AND MB6728)

Dear Mr. Overbeck:

The Commission has issued the enclosed Amendment No. 150 to Facility Operating License No. NPF-41, Amendment No. 150 to Facility Operating License No. NPF-51, and Amendment No.150 to Facility Operating License No. NPF-74 for the Palo Verde Nuclear Generating Station, Units 1, 2, and 3, respectively. The amendments consist of changes to the Technical Specifications (TSs) in response to your application dated November 7, 2002 (102-04864), as supplemented by letters dated April 25 (102-04931), July 10 (102-04964), July 30 (102-04976), August 13 (102-04985), September 18 (102-04995), and October 1 (102-05006), 2003.

The amendments revise TS 3.2.4, "Departure From Nucleate Boiling Ratio (DNBR)," TS 3.3.1, "Reactor Protective System (RPS) Instrumentation - Operating," TS 3.3.3, "Control Element Assembly Calculators (CEACs)," and TS 5.4.1, "Administrative Controls - Procedures." The revisions are to Limiting Conditions for Operation (LCOs), LCO Actions, LCO Surveillance Requirements, and the procedures used to modify the core protection calculator addressable constants.

The amendments support the replacement of the Core Protection Calculator System (CPCS) at the three units. As stated in your application, the replacement CPCS will perform functionally identical safety-related algorithms as the existing CPCS, although on a newer platform, and the CPCS design function will remain unchanged. Because the replacement CPCS for each unit will be installed in refueling outages for the three units over at least a year, starting with the Unit 2 fall 2003 outage, the amendments have the TSs containing both the current requirements for the old CPCS and the new requirements for the replacement CPCS with the phrases "(Before CPC Upgrade)" and "(After CPC Upgrade)" on the TSs to show which requirements apply to which case.

A meeting was held on May 14, 2003, and two trips were taken to Windsor, CT, and the plant site on June 16-20 and July 14-17, 2003, respectively. Summaries were issued on the meeting and the trips on June 24, and September 8, 2003. respectively.

The proprietary reports submitted in your letters of April 25 and September 18, 2003, were addressed in our letters of June 17 and October 15, 2003, respectively, to Mr. Ian C. Richard of Westinghouse Electric Company LLC.

As requested in your letter dated October 1, 2003, the enclosed revised pages of the TSs are being issued with the same amendment number for all three units. Therefore, Amendment No. 149, which was the power uprate amendment for Unit 2 only, will never be used for Units 1 and 3.

A copy of the related Safety Evaluation is also enclosed. The Notice of Issuance will be included in the Commission's next biweekly *Federal Register* notice.

Sincerely,

/RA/

Jack Donohew, Senior Project Manager, Section 2
Project Directorate IV
Division of Licensing Project Management
Office of Nuclear Reactor Regulation

Docket Nos. STN 50-528, STN 50-529,
and STN 50-530

Enclosures:
1. Amendment No. 150 to NPF-41
2. Amendment No. 150 to NPF-51
3. Amendment No. 150 to NPF-74
4. Safety Evaluation

cc w/encls: See next page

As requested in your letter dated October 1, 2003, the enclosed revised pages of the TSs are being issued with the same amendment number for all three units. Therefore, Amendment No. 149, which was the power uprate amendment for Unit 2 only, will never be used for Units 1 and 3.

A copy of the related Safety Evaluation is also enclosed. The Notice of Issuance will be included in the Commission's next biweekly *Federal Register* notice.

Sincerely,
/RA/
Jack Donohew, Senior Project Manager, Section 2
Project Directorate IV
Division of Licensing Project Management
Office of Nuclear Reactor Regulation

Docket Nos. STN 50-528, STN 50-529,
and STN 50-530

Enclosures:
1. Amendment No. 150 to NPF-41
2. Amendment No. 150 to NPF-51
3. Amendment No. 150 to NPF-74
4. Safety Evaluation

cc w/encls: See next page

DISTRIBUTION
PUBLIC
PDIV-2 r/f
G. Hill (6)
RidsNrrDlpmLpdiv (HBerkow)
RidsNrrPMMFields
RidsNrrLAMMcAllister
RidsNrrDripRorp (TBoyce)
RidsAcrsAcnwMailCenter
RidsOgcRp
RidsRgn4MailCenter (L. Smith)
EMarinos CGraham
Juhle MKowal
DFTrimble REckenrode

*See IROB and SRXB memos dated 07/07/2003 and 09/04/2003, respectively
**See previous concurrence TS: ML033020268 NRR-100 PKG.: ML033030618
ACCESSION NO: ML033030363 NRR-058

OFFICE	PDIV-2/PM	PDIV-1/LA	SRXB/SC	IROB/SC	EEIB/SC	OGC MTL	PDIV-2/SC
NAME	JDonohew	MMcAllister	JUhle*	DTrimble*	EMarinos**	MLemoncelli	SDembek
DATE	10/21/03	10/24/03	09/04/03	07/07/03	10/07/03	10/23/03	10/24/03

OFFICE	IROB-A/SC
NAME	TBoyce**
DATE	10/15/03

OFFICIAL RECORD COPY
DOCUMENT NAME: C:\MYFILES\Copies\PVerde AMDs 150(3).wpd

ARIZONA PUBLIC SERVICE COMPANY, ET AL.

DOCKET NO. STN 50-528

PALO VERDE NUCLEAR GENERATING STATION, UNIT 1

AMENDMENT TO FACILITY OPERATING LICENSE

Amendment No. 150
License No. NPF-41

1. The Nuclear Regulatory Commission (the Commission) has found that:

   A. The application for amendment by the Arizona Public Service Company (APS or the licensee) on behalf of itself and the Salt River Project Agricultural Improvement and Power District, El Paso Electric Company, Southern California Edison Company, Public Service Company of New Mexico, Los Angeles Department of Water and Power, and Southern California Public Power Authority dated November 7, 2002, as supplemented by letters dated April 25, July 10, July 30, August 13, September 18, and October 1, 2003, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act) and the Commission's regulations set forth in 10 CFR Chapter I;

   B. The facility will operate in conformity with the application, the provisions of the Act, and the rules and regulations of the Commission;

   C. There is reasonable assurance (i) that the activities authorized by this amendment can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the Commission's regulations;

   D. The issuance of this amendment will not be inimical to the common defense and security or to the health and safety of the public; and

   E. The issuance of this amendment is in accordance with 10 CFR Part 51 of the Commission's regulations and all applicable requirements have been satisfied.

2. Accordingly, the license is amended by changes to the Technical Specifications as indicated in the attachment to this license amendment, and paragraph 2.C(2) of Facility Operating License No. NPF-41 is hereby amended to read as follows:

(2) Technical Specifications and Environmental Protection Plan

The Technical Specifications contained in Appendix A, as revised through Amendment No. 150, and the Environmental Protection Plan contained in Appendix B, are hereby incorporated into this license. APS shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan, except where otherwise stated in specific license conditions.

3. This license amendment is effective as of the date of issuance and shall be implemented for Unit 1 no later than prior to entry of Unit 1 into Mode 4 during the restart from the Unit 1 Spring 2004 refueling outage.

FOR THE NUCLEAR REGULATORY COMMISSION

/RA/
Stephen Dembek, Chief, Section 2
Project Directorate IV
Division of Licensing Project Management
Office of Nuclear Reactor Regulation

Attachment: Changes to the Technical Specifications

Date of Issuance: October 24, 2003

ARIZONA PUBLIC SERVICE COMPANY, ET AL.

DOCKET NO. STN 50-529

PALO VERDE NUCLEAR GENERATING STATION, UNIT 2

AMENDMENT TO FACILITY OPERATING LICENSE

Amendment No. 150
License No. NPF-51

1. The Nuclear Regulatory Commission (the Commission) has found that:

   A. The application for amendment by the Arizona Public Service Company (APS or the licensee) on behalf of itself and the Salt River Project Agricultural Improvement and Power District, El Paso Electric Company, Southern California Edison Company, Public Service Company of New Mexico, Los Angeles Department of Water and Power, and Southern California Public Power Authority dated November 7, 2002, as supplemented by letters dated April 25, July 10, July 30, August 13, September 18, and October 1, 2003, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act) and the Commission's regulations set forth in 10 CFR Chapter I;

   B. The facility will operate in conformity with the application, the provisions of the Act, and the rules and regulations of the Commission;

   C. There is reasonable assurance (i) that the activities authorized by this amendment can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the Commission's regulations;

   D. The issuance of this amendment will not be inimical to the common defense and security or to the health and safety of the public; and

   E. The issuance of this amendment is in accordance with 10 CFR Part 51 of the Commission's regulations and all applicable requirements have been satisfied.

2. Accordingly, the license is amended by changes to the Technical Specifications as indicated in the attachment to this license amendment, and paragraph 2.C(2) of Facility Operating License No. NPF-51 is hereby amended to read as follows:

(2) Technical Specifications and Environmental Protection Plan

The Technical Specifications contained in Appendix A, as revised through Amendment No. 150, and the Environmental Protection Plan contained in Appendix B, are hereby incorporated into this license. APS shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan, except where otherwise stated in specific license conditions.

3. This license amendment is effective as of the date of issuance and shall be implemented for Unit 2 within 90 days of the date of issuance, but no later than prior to entry of Unit 2 into Mode 4 during the restart from the Unit 2 Fall 2003 refueling outage.

FOR THE NUCLEAR REGULATORY COMMISSION

/RA/
Stephen Dembek, Chief, Section 2
Project Directorate IV
Division of Licensing Project Management
Office of Nuclear Reactor Regulation

Attachment: Changes to the Technical Specifications

Date of Issuance: October 24, 2003

ARIZONA PUBLIC SERVICE COMPANY, ET AL.

DOCKET NO. STN 50-530

PALO VERDE NUCLEAR GENERATING STATION, UNIT 3

AMENDMENT TO FACILITY OPERATING LICENSE

Amendment No. 150
License No. NPF-74

1. The Nuclear Regulatory Commission (the Commission) has found that:

   A. The application for amendment by the Arizona Public Service Company (APS or the licensee) on behalf of itself and the Salt River Project Agricultural Improvement and Power District, El Paso Electric Company, Southern California Edison Company, Public Service Company of New Mexico, Los Angeles Department of Water and Power, and Southern California Public Power Authority dated November 7, 2002, as supplemented by letters dated April 25, July 10, July 30, August 13, September 18, and October 1, 2003, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act) and the Commission's regulations set forth in 10 CFR Chapter I;

   B. The facility will operate in conformity with the application, the provisions of the Act, and the rules and regulations of the Commission;

   C. There is reasonable assurance (i) that the activities authorized by this amendment can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the Commission's regulations;

   D. The issuance of this amendment will not be inimical to the common defense and security or to the health and safety of the public; and

   E. The issuance of this amendment is in accordance with 10 CFR Part 51 of the Commission's regulations and all applicable requirements have been satisfied.

2. Accordingly, the license is amended by changes to the Technical Specifications as indicated in the attachment to this license amendment, and paragraph 2.C(2) of Facility Operating License No. NPF-74 is hereby amended to read as follows:

(2) Technical Specifications and Environmental Protection Plan

The Technical Specifications contained in Appendix A, as revised through Amendment No. 150, and the Environmental Protection Plan contained in Appendix B, are hereby incorporated into this license. APS shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan, except where otherwise stated in specific license conditions.

3. This license amendment is effective as of the date of issuance and shall be implemented for Unit 3 no later than prior to entry of Unit 3 into Mode 4 during the restart from the Unit 3 Fall 2004 refueling outage.

FOR THE NUCLEAR REGULATORY COMMISSION

/RA/
Stephen Dembek, Chief, Section 2
Project Directorate IV
Division of Licensing Project Management
Office of Nuclear Reactor Regulation

Attachment: Changes to the Technical Specifications

Date of Issuance: October 24, 2003

ATTACHMENT TO LICENSE AMENDMENT NOS. 150, 150, AND 150

FACILITY OPERATING LICENSE NOS. NPF-41, NPF-51, AND NPF-74

DOCKET NOS. STN 50-528, STN 50-529, AND STN 50-530

Replace the following pages of the Appendix A Technical Specifications with the attached revised pages. The revised pages are identified by amendment number and contain marginal lines indicating the areas of change.

REMOVE	INSERT
3.2.4-1	3.2.4-1
3.2.4-2	3.2.4-2
----------	3.2.4-3
----------	3.2.4-4
3.3.1-1	3.3.1-1
3.3.1-2	3.3.1-2
3.3.1-3	3.3.1-3
3.3.1-4	3.3.1-4
3.3.1-5	3.3.1-5
3.3.1-6	3.3.1-6
3.3.1-7	3.3.1-7
3.3.1-8	3.3.1-8
3.3.1-9	3.3.1-9
3.3.1-10	3.3.1-10
----------	3.3.1-11
----------	3.3.1-12
----------	3.3.1-13
----------	3.3.1-14
----------	3.3.1-15
----------	3.3.1-16
----------	3.3.1-17
----------	3.3.1-18
----------	3.3.1-19
----------	3.3.1-20
3.3.3-1	3.3.3-1
3.3.3-2	3.3.3-2
3.3.3-3	3.3.3-3
3.3.3-4	3.3.3-4
----------	3.3.3-5
----------	3.3.3-6
----------	3.3.3-7
----------	3.3.3-8
5.4-1	5.4-1
----------	5.4-2

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 150 TO FACILITY OPERATING LICENSE NO. NPF-41

AMENDMENT NO. 150 TO FACILITY OPERATING LICENSE NO. NPF-51

AMENDMENT NO. 150 TO FACILITY OPERATING LICENSE NO. NPF-74

ARIZONA PUBLIC SERVICE COMPANY, ET AL.

PALO VERDE NUCLEAR GENERATING STATION, UNITS 1, 2, AND 3

DOCKET NOS. STN 50-528, STN 50-529, AND STN 50-530

1.0 INTRODUCTION

By application dated November 7, 2002, as supplemented by letters dated April 25, July 10, July 30, August 13, September 18, and October 1, 2003, Arizona Public Service Company (APS, the licensee), requested changes to the Technical Specifications (TSs) for Palo Verde Nuclear Generating Station (PVNGS), Units 1, 2, and 3.

The proposed amendments would revise TS 3.2.4, "Departure From Nucleate Boiling Ratio (DNBR)," TS 3.3.1, "Reactor Protective System (RPS) Instrumentation - Operating," TS 3.3.3, "Control Element Assembly Calculators (CEACs)," and TS 5.4.1, "Administrative Controls - Procedures." The revisions are to Limiting Conditions for Operation (LCOs), LCO Actions, LCO Surveillance Requirements, and the procedures used to modify the core protection calculator (CPC) addressable constants.

The amendments support the replacement at the three units of the existing Core Protection Calculator System (CPCS), also called the legacy system, with a Westinghouse Common Qualified (Common Q) digital platform CPCS. The licensee intends to replace the CPCS in all three PVNGS units due primarily to parts obsolescence associated with the existing equipment. The CPCS will be replaced with a functionally equivalent, digital Common Qualified (or Common-Q) CPCS provided by Westinghouse Electric Power LLC (CE Nuclear Power LLC).

As stated in the application, the replacement CPCS will perform functionally identical safety-related algorithms as the existing CPCS, although on a newer platform, and the CPCS design function will remain unchanged. Because the replacement CPCS for each unit will be installed in refueling outages for the three units over at least a year, starting with the Unit 2 fall 2003 outage, the licensee has proposed to have the TSs contain both the current requirements for the old CPCS and the new requirements for the replacement CPCS, with the phrases "(Before CPC Upgrade)" and "(After CPC Upgrade)" on the TSs to show which requirements apply to which case.

A meeting was held on May 14, 2003, and two trips were taken to Windsor, CT, and the plant site on June 16-20 and July 14-17, 2003, respectively. Summaries were issued on the meeting

and the trips on June 24, and September 8, 2003. respectively. Requests for additional information are contained within the meeting and trip summaries.

The proprietary reports submitted in the letters of April 14 and September 18, 2003, were addressed in the NRC staff's letters of June 7 and October 15, 2003, respectively, to Westinghouse Electric Company LLC.

The supplemental letters dated August 13, September 18, and October 1, 2003, provided additional information that clarified the application, did not expand the scope of the application as, and did not change the NRC staff's proposed no significant hazards consideration determination as published in the *Federal Register* on August 18, 2003 (68 FR 49527).

2.0 REGULATORY EVALUATION

10 CFR 50, Appendix A, General Design Criterion (GDC) 10 requires that specified acceptable fuel design limits (SAFDLs) are not exceeded during steady state operation, normal operational transients, and anticipated operational occurrences (AOOs). This is accomplished by having a departure from nucleate boiling (DNB) design basis (i.e., a 95/95 probability/confidence level criteria) that DNB will not occur on the limiting fuel rods, and by requiring that fuel centerline temperature stays below the melting temperature. The reactor core safety limits are established to preclude violation of these criteria. Automatic enforcement of the reactor core safety limits is provided by the reactor protection system (RPS), which includes a number of reactor trip functions, two of which are the DNBR - low (low DNBR) and local power density (LPD) - high (high LPD) reactor trips.

As part of the RPS, the CPCS generates a reactor trip signal when the DNBR or the LPD approach their specified limiting safety system settings. The reactor trips protect against violating core SAFDLs during AOO's. In meeting GDC 10, the replacement CPCS must continue to satisfy these functional requirements.

NUREG-0800, the U.S. Nuclear Regulatory Commission (NRC) Standard Review Plan (SRP), Revision 4, dated June 1997, defines the acceptance criteria for this review. Specifically, Section 7 of the SRP addresses the requirements for instrumentation and control (I&C) systems in light-water nuclear power plants. The procedures for review of digital systems appear principally in SRP Appendices 7.0-A, 7.1-A; Sections 7.1, 7.8, and 7.9; and Branch Technical Positions (BTPs) HICB-14, HICB-17, and HICB-21. SRP Appendix 7.1-C and Sections 7.2 through 7.7 provide additional criteria that the NRC staff applied in the review.

The suitability of a digital platform for use in safety systems depends on the quality of its components, design quality, and system implementation aspects such as real-time performance, independence, and online testing. Because this equipment was being supplied as Appendix B qualified equipment, the NRC staff used the provisions of Institute of Electrical and Electronics Engineers (IEEE) Standard 603 and IEEE Standard 7-4.3.2, as well as the guidance contained in Chapter 7 of the SRP in its review.

In particular, the NRC staff considered the following regulations, codes and standards to evaluate the PVNGS digital to digital upgrade of the CPCS

- Title 10 section 50.55a(a)(1) of the Code of Federal Regulations (CFR)
- 10 CFR 50.55a(h)
- 10 CFR 50, Appendix A, “General Design Criteria for Nuclear Power Plants” (GDC)
  - GDC 1, "Quality Standards and Records"
  - GDC 2, "Design Basis for Protection Against Natural Phenomena"
  - GDC 4, "Environmental and Dynamic Effects Design Bases"
  - GDC 13, "Instrumentation and Control"
  - GDC 20, "Protection System Functions"
  - GDC 21, "Protection System Reliability and Testability"
  - GDC 22, "Protection System Independence"
  - GDC 23, "Protection System Failure Modes"
  - GDC 24, "Separation of Protection and Control Systems"
  - GDC 25, "Protection System Requirements for Reactivity Control Malfunctions"
  - GDC 29, "Protection Against Anticipated Operational Occurrences"

Acceptable means for meeting requirements are provided in the following Regulatory Guides (RGs):

- RG 1.53, “Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems,” which endorses IEEE Standard 379-1977, “Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems."
- RG 1.75, “Physical Independence of Electrical Systems,” which endorses IEEE Standard 384-1977, “Criteria for Independence of Class 1E Equipment and Circuits."
- RG 1.100, “Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants,” which endorses IEEE Standard 344-1987, “IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations."
- RG 1.105, “Setpoints For Safety-Related Instrumentation “ which endorses Part I of ISA-S67.04-1994, “Setpoints for Nuclear Safety-Related Instrumentation."
- RG 1.152, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants,” which endorses IEEE Standard 7-4.3.2-1993, “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.”
- RG 1.153, “Criteria for Power Instrumentation and Control Portions of Safety Systems,” which endorses IEEE Standard 603-1991, “Criteria for Safety Systems for Nuclear Power Generating Stations.”
- RG 1.168, “Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” which endorses IEEE Standard 1012-1998, “IEEE Standard for Software Verification and Validation Plans.”
- RG 1.169, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” which endorses IEEE Standard 828-1990, “IEEE Standard for Software Configuration Management Plans,” and American National Standards Institute (ANSI)/IEEE Standard 1042-1987, “IEEE Guide to Software Configuration Management.”
- RG 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” which endorses IEEE Standard 1074-1995, “IEEE Standard for Developing Software Life Cycle Processes.”
- RG 1.180, “Guidelines for Electromagnetic Interference Testing in Nuclear Power Plants,” which endorses Electric Power Research Institute (EPRI) TR- 102323, Rev. 1, “Guideline for Electromagnetic Interference Testing in Power Plants."

The following are industry standards which have been accepted by the NRC staff in meeting regulatory requirements:

- EPRI TR-102348, Rev. 1 and NRC Regulatory Issue Summary 2002-22, “Guidelines on Licensing Digital Upgrades.”
- ANSI/American Society of Mechanical Engineers (ASME) NQA-1, 1994, “Quality Assurance Program Requirements for Nuclear Facility Applications.”
- IEEE Standard 603, 1991- *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.*
- IEEE Standard 7-4.3.2, 1993 - *IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations*.
- IEEE Standard 379, 1977 - *IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems*.
- IEEE Standard 384, 1977 - *IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits*.
- IEEE Standard 344, 1987 -*IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations*.
- IEEE Standard 1012-1998, *IEEE Standard for Software Verification and Validation Plans*.
- IEEE Standard 828-1990, *IEEE Standard for Software Configuration Management Plans.*
- IEEE Standard 1074-1995, *IEEE Standard for Developing Software Life Cycle Processes.*

For TSs, the criteria for what is in the plant-specific TSs is given in 10 CFR 50.36, "Technical specifications." The criteria for limiting conditions for operation and surveillance requirements are in 50.36(c)(2) and (3), respectively. The TSs by 50.36(b) are derived from the analyses of the systems in the plant.

3.0 TECHNICAL EVALUATION

The proposed amendment would revise the Technical Specifications for PVNGS Units 1, 2, and 3 to support the replacement and upgrade of the existing CPCS, which consists of both the CPC and control element assembly calculators (CEACs). The NRC staff's review is in the areas of human factors, reactor systems, and instrumentation and controls. These are addressed below:

3.1 Proposed Technical Specification Changes

Because the replacement CPCS for each unit will be installed in refueling outages for the three units over at least a year, starting with the Unit 2 fall 2003 outage, the licensee has proposed to have the TSs contain both the current CPCS requirements and the new CPCS requirements by having the phrases "(Before CPC Upgrade)" and "(After CPC Upgrade)" on the TSs to show which requirements apply to which case. This will result with two sets of several TS sections (listed below) existing in the plant TSs with the difference being that one set is for the unit(s) before the CPCS upgrade and one set for the unit(s) after the CPCS upgrade. Unit 2 is scheduled to be the first unit to have the CPCS upgrade and the upgrade is to be completed in the Fall 2003 refueling outage. The other units will be done at a later date.

The licensee has proposed to change the following TSs:

- TS 3.2.4, "Departure From Nucleate Boiling Ration (DNBR)," by adding the note "(Before CPC Upgrade)" to the upper right hand corner of the TS 3.2.4 pages and to the applicability. There is no change to the requirements in the LCO, Actions and SRs for the units where the CPCS upgrade has not been completed.

- TS 3.2.4 by adding a new TS 3.2.4 for after the CPC upgrade by revising LCO 3.2.4 for the requirements for the core operating limit supervisory system (COLSS) for the four cases of (1) COLSS in service and either one or both CEACs are operable, (2) COLSS in service and neither CEAC is operable, (3) COLSS out of service and either one or both CEACs are operable, and COLSS out of service and neither CEAC is operable. The requirements in the LCO, Actions, and SRs that are not being changed are the requirements that are in the current TS 3.2.4. The note "(After CPC Upgrade)" has been added to the upper right hand corner of the new TS 3.2.4 pages and to the applicability.

- TS 3.3.1, "Reactor Protective System (RPS) Instrumentation - Operating," by adding the note "(Before CPC Upgrade)" to the upper right hand corner of the TS 3.3.1 pages, including TS Table 3.3.1-1, and to the applicability. There is no change to the requirements in the LCO, Actions and SRs for the units where the CPCS upgrade has not been completed.

- TS 3.3.1 by adding a new TS 3.3.1 for after the CPC upgrade by deleting Actions E and F of for LCO 3.3.1 and revising SR 3.3.1.3. The requirements in the LCO, Actions, and SRs that are not being changed are the requirements that are in the current TS 3.3.1. The note "(After CPC Upgrade)" has been added to the upper right hand corner of the new TS 3.3.1 pages and to the applicability.

- TS 3.3.3, "Control Element Assembly Calculators (CEACs)," by adding the note "(Before CPC Upgrade)" to the upper right hand corner of the TS 3.2.4 pages and to the applicability. There is no change to the requirements in the LCO, Actions and SRs for the units where the CPCS upgrade has not been completed.

- TS 3.3.3 by adding a new TS 3.3.3 for after the CPC upgrade by (1) adding the phrase "in each CPC channel" to LCO 3.3.3, (2) revising the Condition, Required Action, and Completion Time for Actions A, B, and E, (3) deleting Actions C and D, and (4) deleting SRs 3.3.3.2 and 3.3.3.6. The existing Action C would be renumbered Action C, and the word "deleted" would replace the SR for SR 3.3.3.2. The requirements in the LCO, Actions, and SRs that are not being changed are the requirements that are in the current TS 3.3.3. The note "(After CPC Upgrade)" has been added to the upper right hand corner of the new TS 3.3.3 pages and to the applicability.

- TS 5.4.1.f, "Procedures," in the section on administrative controls, by adding the note "(Before CPC Upgrade)" to the upper right hand corner of Page 5.4-1. There is no proposed change to the requirements on procedures for modification of the CPC addressable constants for the units where the CPCS upgrade has not been completed.

- TS 5.4.1.f by adding a new TS 5.4.1.f for after the CPC upgrade by changing the name of the software program manual referenced for making modifications to the CPC software including changes of algorithms and the fuel cycle specific data. The requirements not being changed are the requirements that are in the current TS 5.4.1.f. The note "(After CPC Upgrade)" has been added to the upper right hand corner of the new TS 5.4.1.f page.

3.2 Human Factors Considerations

The licensee addresses human factors considerations in its letter dated April 25, 2003. In that letter, the licensee states the following:

- “There are no CPCS related operator functions credited in the PVNGS Updated Final Safety Analysis Report (UFSAR) to prevent or mitigate an accident."
- "There are no CPCS related operator tasks that have been identified as significant contributors to plant risk and therefore none are modeled in the plant Probability Risk Assessment (PRA).”

Also, in Section 5.1 of its application, the licensee states that "The CPCS is not an initiator of any analyzed accident." From these statements and discussions with the licensee in the meeting of May 14, 2003, the NRC staff concludes from these statements that the operator actions with respect to the upgraded CPCS are not risk significant and are therefore not significant to the safe operations of the plant.

Additionally, the licensee states that, as required by the design modification process, all identified human factors impacts related to the upgraded CPCS are documented in the CPCS design modification work package. The licensee does not expect that any new tasks will need to be developed for the upgrade. Furthermore, the licensee has developed a formal site specific CPC/CEAC Replacement Human Factors Review plan to address the approach and methodology for the final acceptance of the new design, including a comprehensive checklist for the applicable NUREG-0700, “Human-System Interface Design Review Guidelines,” criteria to be properly implemented. The licensee has also committed to conducting appropriate operator training, verification and validation (V&V), and testing and monitoring throughout the process.

Based on the low risk significance of the operator actions related to the upgraded CPCS and the commitments made in the area of human factors, the NRC staff concludes that the licensee has acceptably satisfied the human performance requirements for the license amendment request.

3.3 Reactor Systems Review

The reactor systems review of this amendment evaluated the (1) impacts of the upgraded CPCS on the UFSAR Chapter 15 events, and (2) reviewed the proposed changes to the DNBR in TS 3.2.4.

3.3.1 Description of Current and Replacement CPCS Design

Both the existing and replacement CPCS consist of four independent channels of equipment (A, B, C and D) that are physically separated from each other. The CPCs generate pre-trip and trip signals on low DNBR and high LPD, as well as control element assembly (CEA) withdrawal prohibit signals to the plant protection system. A reactor trip signal from the RPS is generated when any two of the four CPCS channels generate a trip signal. Both the existing and replacement CPCs utilize CEACs to obtain CEA position and generate appropriate penalty factors when CEA position deviates by more than a specific deadband limit within each subgroup. These penalty factors are used to modify CPC calculation results in a conservative manner, which then may result in a reduction of margin to trip for low DNBR and high LPD. Each CEA position is measured by two redundant and independent Reed Switch Position Transmitters (RSPTs) associated with each CEA.

The existing CPCS design includes two redundant CEACs. CEAC 1 is mounted in CPC Channel B, and CEAC 2 is mounted in CPC Channel C. CEAC 1 monitors the position of all CEAs based upon RSPT 1 CEA position input, and CEAC 2 performs the identical function, but based on RSPT 2. CEAC penalty factor outputs in the existing system are transmitted to all four Core Protection Calculator Channels. Thus, the CPCs in all four channels receive penalty factor inputs from both CEACs. The replacement CPCS design will include a total of eight CEACs, two in each CPC channel. Each CPC channel will have a CEAC 1, using RSPT 1 inputs from all CEAs, and a CEAC 2, using RSPT 2 inputs from all CEAs. RSPT inputs to each CPC/CEAC channel will be transmitted to the other three channels. Thus, the replacement design should increase availability because the failure of one CEAC affects only one CPC channel.

3.3.2 Functionally Identical Replacement CPCS

The licensee states that the replacement CPCS is functionally identical to the existing CPCS. In its response dated July 10, 2003, to an NRC staff request for additional information (RAI), the licensee, expanding on the meaning of functionally identical, stated that functionally identical means that the algorithms in the upgraded CPCS will accomplish the same function within the same requirements for system time and accuracy. The licensee's response included a table providing a comparison between the algorithms in the existing and proposed CPCS. Changes to the algorithms are addressed in Section 3.4 below.

To demonstrate that the upgraded CPCS is functionally identical to the existing system, the licensee developed a comprehensive V&V program, which includes testing of the CPC algorithms as part of the design process to ensure that all requirements are satisfied. To perform this verification, the licensee will perform post-installation testing after startup by comparing upgraded CPCS results to those calculated under the same operating conditions (input data) using a CPC simulation program. The licensee developed this simulation program in accordance with the PVNGS quality assurance program, and the simulation program has been independently validated and verified. The final acceptance criteria will be based on statistical analysis of data collected from Units 1 and 3, and will use a 95/95 probability/confidence level criteria. The data collection and comparison to the CPC simulation program is a normal activity as part of the PVNGS initial reload power ascension testing.

The licensee also verified that the CEAC calculation of the penalty factors in the upgraded CPCS is functionally identical to the method used in the existing system, and that there are no functional changes to the CPC addressable constants.

3.3.3 Impact on UFSAR Chapter 15 Transients and Accidents

The CPCS is part of the RPS, and generates a reactor trip signal when the DNBR or the LPD approach their specified limiting safety system settings. Certain UFSAR Chapter 15 events credit these trip signals to ensure that the SAFDLs are not exceeded during AOO's. To evaluate that the upgraded CPCS will continue to perform this intended function, the NRC staff considered (1) the functionality of the upgraded system versus the existing CPCS, and (2) the CPCS response times and accuracy for the DNBR and LPD trip functions.

The licensee demonstrated the functionality of the systems, which is discussed in Section 3.2 above.

In its response dated July 10, 2003, to an NRC staff RAI, the licensee provided information which demonstrates that the response times and accuracy of the upgraded CPCS values remain bounded by the values used in the current UFSAR Chapter 15 analyses. The licensee's response included a comparison of total CPC output response times versus UFSAR Chapter 15 assumed response times, and upgraded CPCS DNBR and LPD uncertainties versus the values assumed in the UFSAR Chapter 15 analyses. Additionally, the current Chapter 15 analyses would not be impacted because there are no TS setpoint changes associated with the upgraded CPCS. The NRC staff has reviewed the information provided and finds that the upgraded CPCS will have no impact on the UFSAR Chapter 15 transients and accidents because the CPCS response times and accuracy assumed in the UFSAR Chapter 15 analyses for the DNBR and LPD trip functions remain bounding.

3.3.4 Proposed change to TS 3.2.4, Departure From Nucleate Boiling Ratio (DNBR)

The licensee is proposing to revise TS 3.2.4 to reflect the upgraded CPCS. The proposed changes will allow TS 3.2.4 to reflect the new CPCS design of eight CEACs (two per channel) instead of the existing two CEACs total, and support the upgrade of the CPCS while maintaining the same intent as that of the current CPCS related TS. There are no setpoint changes associated with the proposed amendment request. The NRC staff has reviewed the propose TS 3.2.4 changes, and finds that they reflect the upgraded CPCS configuration and maintain the intent of the current TS 3.2.4.

3.3.5 Reactor Systems Review Conclusion

For the reactor systems review, as discussed above, because the licensee has shown that the current and upgraded CPCS are functionally identical, there is no impact on the UFSAR Chapter 15 events, the proposed changes reflect the configuration of the upgraded CPCS, and the intent of TS 3.2.4 has been maintained, the NRC staff concludes that the proposed changes to TS 3.2.4 meet GDC 10 and are, therefore, acceptable

3.4 Instrumentation and Controls Review

3.4.1 Background

The licensee proposes to replace the existing CPCS (see Figure 1, page 10) with a new functionally equivalent Common Q system to be located in the existing CPC racks and cabinets. Figure 1 was drawn by the NRC staff from its review of the proposed change to the CPCS.

The existing CPCS has two CEACs physically mounted in channels B and C. There is one CEAC 1 and one CEAC 2 in the entire four-channel CPCS. Each Control Element Assembly (CEA) position is measured by two redundant and independent Reed Switch Position Transmitters (RSPTs)—RSPT 1 and 2. CEAC 1 reads RSPT 1 and CEAC 2 reads RSPT 2. Penalty factor (PF) outputs from each of these two CEAC channels are provided to all four CPC channels via one-way isolated data links.

The implementation of the proposed CPCS Common Q system is shown in Figure 2, page 11. Figure 2 was also drawn by the NRC staff from its review of the proposed change to the CPCS.

In this system, there are eight CEACs—CEAC 1 and 2 in each of the four CPC channels and the Chanel A and D isolation amplifiers are no longer needed. Nevertheless, the CEAC remains functionally the same. The new CPC and CEA instrumentation racks and the interposing relay panel will be physically located in the existing CPC cabinet. Each CEAC receives the same CEA inputs as in the present design. However, PF outputs from the CEACs are used only in the associated CPC channel. In the replacement system, the CEA position inputs will undergo analog-to-digital conversion in the channel of origin, by means of redundant CEA position processors (CPPs), CPP 1 and CPP 2, in each CPC channel. Converted CEA position is then transmitted to the associated CEAC 1 and CEAC 2 processors in each CPC channel, which perform CEA deviation PF calculations.

3.4.2 CPCS Description

The functional requirements of the proposed CPCS will be the same as those in the legacy system. Westinghouse CPCS system requirements specification (SysRS) document 00000-ICE-30158 describes the software components, design structure, information flow, processing steps and other aspects required to be implemented and includes the system physical configuration on which the CPC software will run. The SysRS also contains references to NRC regulations and industry standards that were applied to the CPCS requirements and design. The hardware description section of this safety evaluation focuses on the description of that hardware and the requirements that are application specific. This is because the Common Q system and most of its hardware components were approved in the NRC SER dated August 11, 2000.

3.4.2.1 CPCS Description - Hardware

The proposed CPCS platform is the ADVANT- based Common Q platform described in CENPD 396-P, *Common Qualified Platform Topical Report*, Rev. 01 and an appendix of that report WCAP-16097-P-A, Appendix 2, Rev. 0, *Common Qualified Platform Core Protection Calculator*

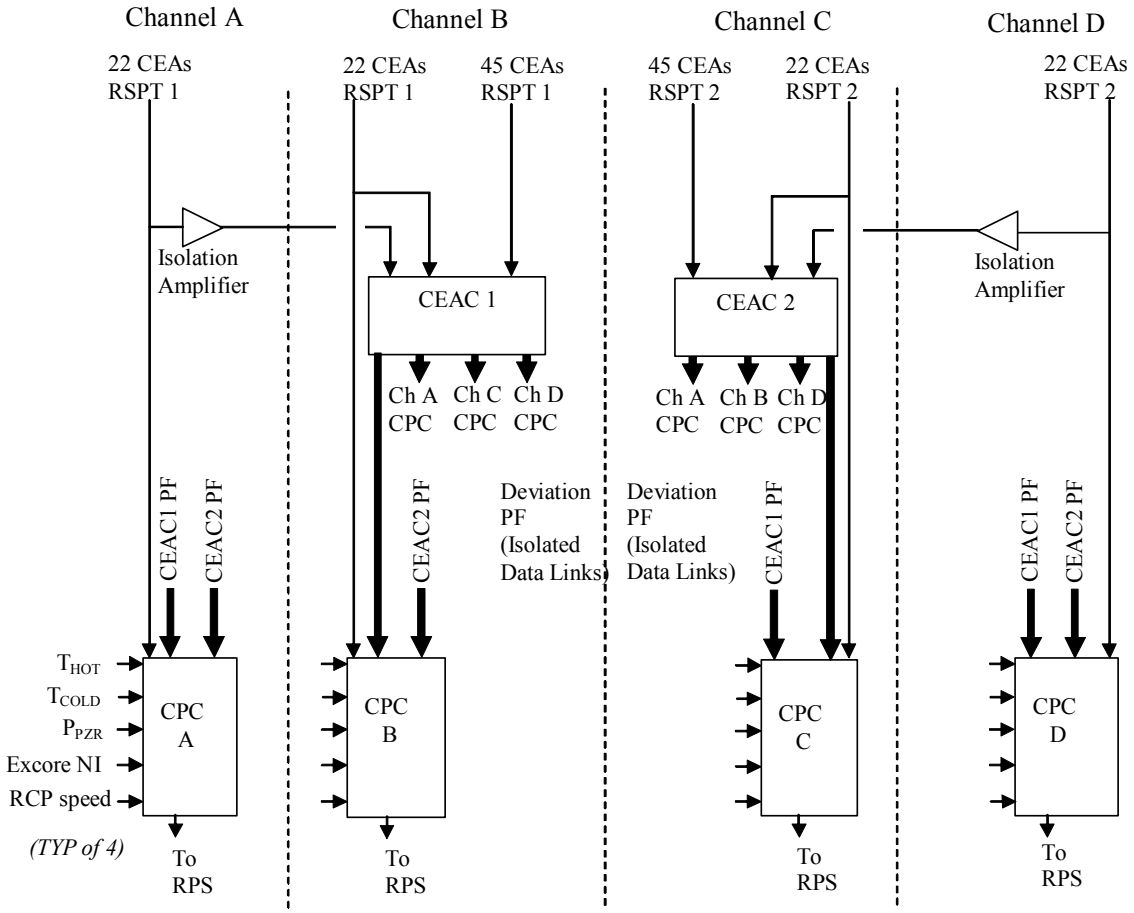

Figure 1 Existing CPCS

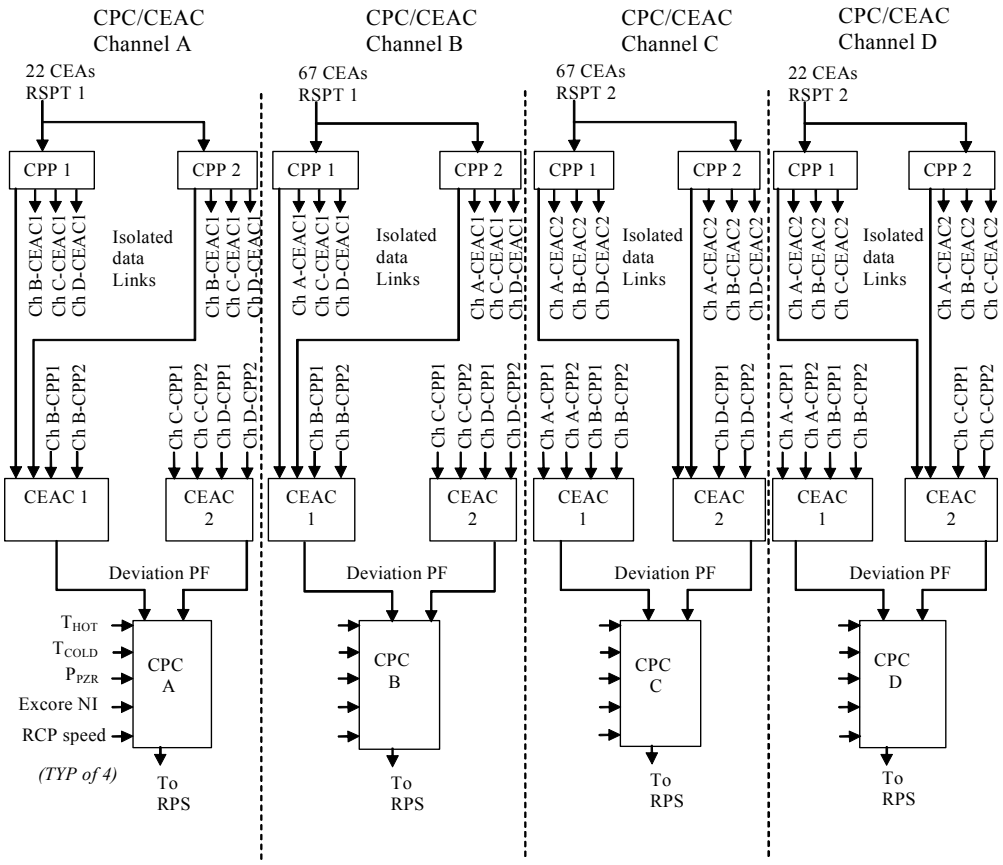

Figure 2 Proposed CPCS

System. The SysRS requirements are implemented and described in Westinghouse document 00000-ICE-30164, Rev. 01, *Hardware Design Description for the Core Protection Calculator System*. The Hardware Design Description (HDD) contains the details for the CPCS hardware design, layout, interconnections, connections with external systems, environmental requirements and connections with the RPS.

The CPC system is comprised of four redundant channels (A,B,C and D), as shown in Figure 2, that perform the necessary calculation, bistable, and maintenance functions. The system includes four redundant operator modules (OM), one per CPC/CEAC channel, located in the main control room. One CPC/CEAC channel is located in each auxiliary protective cabinet (APC)—as in the present design—where the channels are separated and electrically isolated from one another. Each channel APC also contains a maintenance and test panel (MTP) for routine testing. A CPC/CEAC channel is associated with each RPS channel and provides low DNBR and LPD trip and pretrip signals and CEA withdrawal prohibit (CWP) outputs to its associated RPS channel. The four redundant channels are designed to satisfy the single failure criteria. The CPC and CEAC processors in each channel receive process analog signals from hot leg (T_{hot}) and cold leg (T_{cold}) temperature, pressurizer pressure (P_{PZR}), ex-core neutron flux, and reactor coolant pump (RCP) speed and RSPTs. These parameters are used in the safety-related application software algorithms performed by the CPC and CEAC processors. The existing field sensors and RPS inputs will be used in the proposed design.

Figure 2 does not show the interface between each CPC channel and the RPS. Each CPC channel will interface with the RPS through an interposing relay panel (IRP) which will contain interposing relays for each digital output (DO) contact from the CPCS. The IRPs are located in the auxiliary protective cabinets. These relays, Phoenix PLC-RSC-24DC/21-21, provide the electrical interface between the CPC channel and the RPS. All contact output signals are routed through these relays on the IRP. The IRP also houses the Watchdog Timer (WDT) output interposing relay used to provide Low DNBR and High LPD trip outputs on WDT timeout. The IRPs are located in the corresponding Channels A and C.

The four CPC OMs and MTPs use a flat panel display (FPD) which consists of a liquid crystal display, and a single board computer (SBC). The SBC consists of an embedded PC, input/output (I/O) interface, Ethernet output, flash disk, hard and floppy disk drives, and a CD-ROM drive. There is one control room OM per CPC channel and it will be used by plant operations, to monitor CPCS trip status, help determine plant status, monitor CPCS status output to determine CPCS operability, change addressable constants under password control, and to initiate operating bypass of the Low DNBR and High LPD trip functions to prevent CPCS actuation during normal plant startup and shutdown.

The four MTPs are located in the APCs, one MTP per CPC channel. The MTP can replicate OM functionality, but will primarily be used as a service data link to the plant computer, allow technicians to assess CPCS status to aid in corrective maintenance, perform surveillance testing, and allow the download of software. The OMs and MTPs are designed as safety-related equipment, but are designed to conform to IEEE Standard 603 related to separation between these components and the CPC and CEAC processors. The system is designed such that loss, failure, or other abnormal events from the OMs or MTPs will not adversely affect the safety functions of the CPCS. The MTP uses a software load enable switch to permit the download of software. With the switch in normal mode, power to the hard drive and WIN NT operating system (OS) is removed, thus preventing the CPC or CEAC processor flash memory

from being changed. When this switch is enabled, hardware contacts will generate a trip for that CPCS channel. The MTP and OM have a function enable switch that will allow operators to change addressable constants. The switch can also be used to bypass the CPCS if a < 10^{-4} percent reactor power permissive is active from the RPS. This functionality is the same as in the existing system.

The CPCS also includes a non-safety related CEA Position Display System (CEAPDS), which is in the control room. The CEAPDS provides essentially the same information as the existing system, but has enhanced human machine interface (HMI) and functionality. The CEAPDS uses similar FPD technology as the OMs and MTPs and receives CEA position information from the CPCS through an Ethernet connection.

3.4.2.1.1 Isolation of Safety-Related CPCS to Non Safety-Related Systems

Figure 3 (on page 14) illustrates the CPCS connectivity with non-safety related systems including the plant computer and the CEAPDS. The figure was drawn by the NRC staff from its review of the proposed changes to the CPCS.

Connections to these systems are made using fiber optic (FO) links. The MTP and OM uses the Transmission Control Protocol/Internet Protocol; therefore, one-way communication is accomplished at the application layer of the open systems interconnection (OSI) 7-layer communication model. Communication handshaking does occur at the lower levels of the OSI model and is handled at the Ethernet interface card. The I/O interface provides a buffer circuit which separates the plant computer/CEAPDS link and the communication functions that occur between the OM/MTP, and the CPC and CEAC processors.

3.4.2.1.2 CPCS channel separation

Physical Separation:

Equipment and circuits of the CPCs require four channel separation and mechanical isolation meeting the requirements of IEEE Standard 384 which include separation distances, protection barriers and cable/signal wire separation.

Electrical Isolation:

The cabinet termination area is designed for either top or bottom field cable entry. Communications cabling between redundant CPC channels is routed via fiber optic cables. There are no copper cables between redundant CPC channels. The fiber-optic cables provide electrical isolation and independence.

Communication Isolation:

Communication cabling between channels uses fiber-optic cabling routed and connected to achieve one-way communication. This is accomplished such that FO cables are connected from the Transmit light source of the sending channel to the Receive optical sensor for the receiving channel. One-way communication implemented in this way prevents a receiving channel failure or other abnormal operation from adversely affecting the sending channel.

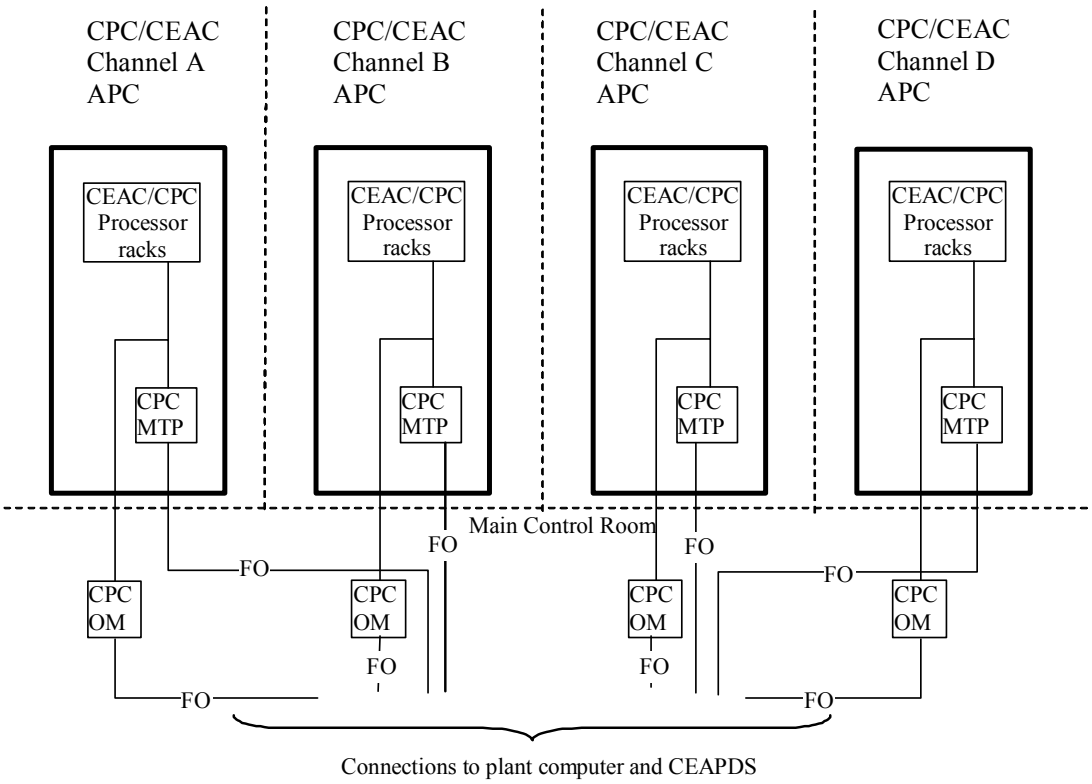

Figure 3 Connectivity to non-safety related systems

3.4.2.1.3 CPCS Single Failure

The CPCS is designed for fail safe operation under component failure or loss of electrical power as defined in the Failure Modes and Effects Analysis (FMEA) in the Westinghouse CPCS topical report.

A loss of 120 Vac power to a CPC channel will cause the channel safety outputs to assume their trip or initiation state: all DO contacts shall open, de-energizing the interposing relays. Additionally, the IRP relay power shall also be lost. A CPC processor stall or processor halt, will result in loss of its heartbeat signal output to a watch dog timer mounted within the processor modules. The CPC watchdog timer will force the CPC trip signals to their fail-safe (trip) states.

Failure of the CEAC Processor or associated CEAC to CPC HSL is transmitted to the CPC processor as a failed CEAC.

3.4.3 CPCS Description - Software

The Common Q system software consists of a real-time operating system, a task scheduler, diagnostic functions, communication interfaces, and user application programs, all of which reside on flash programmable read-only memory (PROM) in the PM646 processor module. The application program and its control modules coexist with the system software programs such as the task scheduler, diagnostic routines, and communication interfaces in the processor module. The task scheduler schedules the execution of the application programs and periodic system software tasks based on predefined priorities. The processing section of the PM646 executes the safety-related application program and the communication section handles the serial communication with other safety channels.

The executable code for the standard set of logic blocks (program control elements) is part of the base software. In addition, custom program control elements can be created as an extension to the base software.

The processing section of the PM646 module executes the safety algorithms. It has one process control program, which consists of several executable units called control modules (CONTRMs). Each CONTRM has its own cycle time and execution conditions. When this process control program is compiled into target codes, each CONTRM becomes an operating system's task. On the basis of predefined priorities, the process section schedules all the tasks using the task scheduler in the system software and executes the tasks accordingly. The basic software components of the processing section are the following:

- Task scheduler – The task scheduler schedules the application programs and periodic system tasks. It also performs diagnostic functions.

- Application programs – The application programs are created by the application engineer. The priority of the application program is set by the application tool. This is the software that the NRC staff reviewed as part of the application-specific implementation of the CPCS.

- Service data program – The service data program services all communications on the AC160 subrack backplane. Examples of such communications are I/O module

configuration and initialization, communication with the I/O modules, and communication with the AF100 bus, the communication link that connects the processor modules with the OM and MTP.

- System diagnostics – The system diagnostics perform the following:
  - Check proper operation of the window watchdog timer;
  - Validate the RAM diagnostics;
  - Monitor the status of the serial communications section.

- Background task – The background task is the last in the task sequence. It performs the following diagnostics:
  - Performs a cyclic redundancy check (CRC) of the system firmware in the flash PROMs;
  - Performs a CRC of all static domains in RAM;
  - Performs a CRC of the user programs in flash PROM;
  - Checks parameter set of I/O modules;
  - Configures I/O modules after they are replaced.

3.4.3.1 Application Software

Creation of the application program utilizes the ACC software development environment which includes a function block library of process control elements. The executable code for the standard set of logic blocks (i.e., process control elements) is part of the base software. In addition, custom process control elements can be created as an extension to the base software. The programmer references the process control element library to create the specific logic for the application.

The application program is written in the ABB Master Programming Language and consists of a process control part and a database part.

The process control part of a user application program describes the control algorithm and the control strategy. It contains the process control elements, their interconnections, and connections to the database elements. A process control program can be divided into several executable units called control modules, each consisting of process control elements. Each executable unit can be given its own cycle time and its own execution conditions. Process control elements are the smallest building blocks in a process control program. The control module is made up of function calls to the process control element library which is stored on system flash PROM.

Each processor has one process control program under which are executable control modules. When this process control program is compiled into target code, each of its control modules becomes a task to be executed under the control of the operating system.

The I/O modules continuously scan and store values independent of control module execution. When the control module executes, its first operation is to get the process input values over the backplane I/O bus from the I/O modules.

On processor initialization or restart, the application programs are reloaded from flash PROM into RAM and then started. The application software consists of the CPCS safety-related algorithms and other application specific routines that run the Common Q system as a CPC.

3.4.3.2 Safety-Related Algorithms

The SysRS describes requirements for the major software components, design structure, information flow, processing steps and other aspects required to be implemented in order to satisfy the CPCS functional requirements that must be met for software development and V&V. The safety-related algorithms are identical in functionality to the legacy system and will be implemented using the C programming language. However, there will be significant enhancements to the HMI, and error detection and handling in the proposed system. In addition, two algorithm programs shall be changed such that they are executed more frequently in order to meet response time requirements.

Implementation of the CPCS application software on the PLC-based ADVANT system entails overlaying the CPC application software on the ADVANT OS software. The OS will perform real-time operating to handle multiple events such as scheduling application programs, reading and writing files from/to the disk, and sending data across a network within fixed time constraints.

The safety-related application software for the CPCS consists of six programs which work together to accomplish CPCS functionality:

- Coolant Mass Flow Program (FLOW),
- DNBR and Power Density Update Program (UPDATE),
- Power Distribution Program (POWER),
- Static DNBR and Power Density Program (STATIC),
- Trip Sequence Program (TRIPSEQ),
- CEAC Penalty Factor Program (CEACPFP).

The first five programs are executed in the CPC Processor Subrack. The CEAC is executed in the CEAC Processor Subrack. These programs run in a time scheduled manner under a real-time OS.

The FLOW program computes (1) the primary coolant mass flow rate by calculating a normalized flow rate in each primary coolant leg and the reactor core and (2) an adjusted value of DNBR based on the number of RCPs running, the DNBR margin, the scaled core coolant mass flow rate, and the scaled DNBR margin. The DNBR margin and scaled core coolant mass flow are converted to analog form for control room meter display.

The UPDATE program performs the following major calculations:

- Calibrated neutron flux power,
- Total thermal power,
- Core average heat flux,
- Hot pin heat flux distribution,
- DNBR and quality margin at the node of minimum DNBR, updated for changes in input parameters,

- Peak LPD,
- Asymmetric Steam Generator Transient (ASGT) trip,
- Variable Overpower Trip (VOPT).

The POWER program performs the following major calculations:

- Core average axial power distribution,
- Pseudo hot pin axial power distribution,
- Three dimensional power peaking factor,
- Average of the hot channel power distribution.

The STATIC program performs the static DNBR, static hot channel quality, maximum hot leg temperature calculations, including uncertainties, the saturation temperature of water, and the average enthalpy at the core inlet and outlet.

In TRIPSEQ, minimum DNBR, quality margin, and peak local power density are compared to their respective pretrip and trip setpoints. Whenever a setpoint is violated, the appropriate contact output is actuated. In addition, trips are initiated for core conditions outside the analyzed operating space -- less than two reactor coolant pumps running, hot leg saturation, VOPT, ASGT -- or internal processor faults including:

- Failure of the RAM test self diagnostics,
- Failure of the CRC checks on the application PROM,
- Illegal machine instruction,
- Failure to meet the timing requirements

The CEAC Penalty Factor Algorithm has been designed:

- To recognize the initiation of a reactor power cutback event.
- To calculate the deviation (different in position) amongst the CEAs in each subgroup.
- To recognize excessive CEA deviation within a subgroup, and to identify each occurrence as a single CEA withdrawal, single CEA insertion, or multiple CEA deviations within a subgroup, and communicate this recognition to the CPCs.
- To calculate and/or look up a penalty factor for LPD, and a penalty factor for DNBR based on the type of deviation event, the magnitude of the deviation, the CEA subgroup with the deviation, the CEA configuration, and the elapsed time since the start of the deviation. The LPD and DNBR penalty factors shall be selected as the maximum of the LPD and DNBR penalty factors calculated for each subgroup.
- To determine the status of the CEAC sensor fail alarm and the CEA deviation alarm.
- To check some conditions under which CEAC (or upstream hardware) failure should be indicated to the CPCs.
- To provide diagnostic information on CEA sensor failures, and on the causes of a CEAC penalty factor.
- To provide an indicator to the CPCs of the scale used in determining the penalty factors transmitted.
- To support CEA cathode ray tube display software by sending appropriate parameters used for the display.

3.4.4 CPCS Evaluation

The acceptance criteria for this review is defined in NUREG-0800, the NRC Standard Review Plan (SRP), Version 6.0, May, 1997, Section 7.0, *Instrumentation and Controls - Overview of Review Process*. SRP Section 7 provides guidance for the review of the instrumentation and controls (I&C) license amendment requests, such as the licensee's application.

The subsections of 10 CFR Part 50, general industry standards, BTPs, and other guidance that were used in this safety evaluation, as well as the NRC staff's review methodology are given in Section 2.0 of this safety evaluation.

3.4.4.1 Method of Review

The material reviewed by the NRC staff is contained in the application dated November 7, 2002, and supplemental letters dated July 10 and July 30, 2003, August 13, 2003 and September 18, 2003. The NRC staff also reviewed material at the Westinghouse offices in Rockville, MD and Windsor, CT, and the licensee at the PVNGS plant site in Tonopah, AZ, and issued a trip summary report dated September 8, 2003 which provides, in part, the documentation reviewed.

The licensee had Westinghouse provide CPCS development, design and testing documentation in the Westinghouse offices in Rockville, MD, and submitted responses to RAIs that included the following documentation:

- Licensee's Procurement Specification 13-JN-1000, Rev. 2, *Engineering Specification for the Core Protection Calculator / Control Element Assembly Calculator (CPC/CEAC) System for Palo Verde Nuclear Generating Station*.
- 00000-ICE-30158, Rev. 07, *System Requirements Specification for the Common Q Core Protection Calculator System* (SysRS) - This document describes the hardware and software system purpose, design, constraints and interfaces. These requirements were taken from the legacy system functional design requirements.
- 00000-ICE-30164, Revision 02, *Hardware Design Description for the Common Q Phase 3 Core Protection Calculator System* (HDD) - This document defines the generic hardware design requirements for the CPCS.
- 14273 - ICE-36363, Revision 02, *Palo Verde Nuclear Generating System Core Protection Calculator System Input Uncertainty Calculation* - This document provides the analysis for the input processing uncertainties.
- 00000-ICE-35249, Revision 03, *Test Plan for the Common Q Core Protection Calculator System* - This document describes the overall plan for testing the CPCS including test procedures, test performance, and test reports.
- 00000-ICE-36374, Revision 01, CPC *Availability Analysis For The Common Q Core Protection Calculator System* - This document documents the worst case hardware availability of the CPCS. It is used to justify the SysRS requirement in section 3.5.3.
- 00000-ICE-36369, Revision 01, *CPC Timing Analysis for the Common Q Core Protection Calculator System* - This document present the calculation and analyses for the worst case response times of the Common Q CPCS.
- 14273-ICE-37731, Revision 00 , Software Preliminary Hazard Analysis for the Palo Verde Nuclear Generating Station Core Protection Calculator System - This document

presents the software hazard analysis for the CPC. It defines possible software hazard faults and their potential impact.

- 13-JC-RJ-0205, Revision 7, Core Operating Limit Supervisory System (COLSS) and Core Protection Calculator (CPC) Measurement Channel Uncertainties - This document provides the input uncertainties which are used as part of the overall CPC uncertainty analysis.
- 13-JC-ZZ-0204, Revision 3, Uncertainty of Analog-to-Digital Converters for Computer Input in ERFDADS, PMS, CPC, and QSPDS - This document provides the calculations for the overall uncertainty for analog-to-digital converters used to provide input to the CPC.

The NRC staff also used the following documentation previously used in conjunction with the review of the Common Q platform:

- WCAP-16097-P-A, Common Qualified Platform Topical Report, dated May 2003 (previously submitted as CENPD-396-P)
- WCAP-16097-P-A Appendix 2, Common Qualified Platform Core Protection Calculator System Revision 0, dated May 2003 (previously submitted as CENPD-P, Appendix 2)
- CE-CES-195, Rev. 1 Westinghouse Software Program Manual (SPM), Revision 01, dated May 26, 2000
- Safety Evaluation Report (SER) for Topical Report CENPD-396-P "Common Qualified Platform" dated August 11, 2000 and SER supplements dated June 22, 2001 and February 24, 2003

The NRC staff visited the Westinghouse offices in Windsor, CT to audit the CPCS application software and the software system life-cycle activities. The NRC staff used the Westinghouse Software Program Manual (SPM) CE-CES-195, approved by SER dated August 11, 2000, as the primary document for the audit. The SPM was used to evaluate the software system life-cycle activities supporting the CPC development and design, and applies to all software and firmware acquired or developed in-house for use in the Common Q system. As part of the audit of Westinghouse software system life-cycle activities, the NRC staff reviewed the requirements and design documentation, the software code, test plans and results, and Westinghouse V&V documentation.

The NRC staff also visited the PVNGS site to ascertain the scope of the licensee's involvement in the Westinghouse development and design process for the CPCS. The NRC staff used the licensee's CPCS specification 13-JN-1000, Rev. 2, "Engineering Specification for the Core Protection Calculator / Control Element Assembly Calculator (CPC/CEAC) System for Palo Verde Nuclear Generating Station," to evaluate the licensee efforts to verify conformance of the CPCS with this specification. The NRC staff reviewed the PVNGS procedures used to specify, procure, verify, validate and install the CPCS, and interviewed the licensee's personnel to confirm the appropriate use of the licensee's procedures and compliance with Specification 13-JN-1000. The NRC staff also reviewed the V&V efforts of the vendor, Westinghouse, and the licensee for the CPCS.

The NRC staff's reviewed portions of the hardware that were not reviewed in the Common Q SER dated August 11, 2000, or the SER supplements dated June 22, 2001 and February 24, 2003, as well as the application software design, qualification testing, V&V procedures, and quality control. In doing this, the NRC staff confirmed the licensee's adherence to the

plant-specific action items (PSAIs) in the August 11, 2000 SER. Additionally, the NRC staff performed CPCS functional requirement thread audits which included a detailed review of selected CPCS functions. The thread audits traced the implementation of those functions through the hardware and software, and included evaluating requirements, design, coding, testing from field devices, through the CPCS, to the outputs to the RPS.

3.4.4.2 Hardware Evaluation

A significant portion of the proposed CPCS hardware was approved by the Common Q NRC SER dated August 11, 2000 and the SER supplements dated June 22, 2001, and February 24, 2003. Therefore, the NRC staff focused on hardware application specific aspects of the Common Q system for use as a CPC, the hardware aspects discussed in the Licensee's CPCS procurement specification, and the PSAI's in the SER dated August 11, 2000. As such, the following hardware aspects were reviewed.

- Procurement Specification - Hardware
- CPC channel separation
- CPCS connection to non-safety systems
- CPCS to RPS interface - Interposing Relay Panel (IRP)
- CPCS Hardware Availability
- Use of the OM and MTP to operate the CPCS
- CPCS hardware not previously approved by the NRC
- Differences between the system to be installed and that approved in the Common Q SER dated August 11, 2000
- Channel Uncertainty

3.4.4.2.1 Procurement Specification - Hardware

The CPCS procurement Specification 13-JN-1000 is the engineering specification which provides the requirements to design, fabricate, test, deliver, and startup the new CPCS. The specification includes the applicable NRC regulations, NRC regulatory guides, and industry standards. Specification 13-JN-1000, section 1 specifies that the CPCS "shall consist of the NRC approved, safety related, microprocessor-based, 'Standard Platform' system to be installed in all three PVNGS units." In addition, Specification 13-JN-1000, Section 5.1 states in part:

> 5.1 The CPCS portion of the Palo Verde CPCS replacement described herein provides the following replacement systems:
>
> 5.1.1 Three Safety Related Core Protection Calculator Systems (one system per unit, four channels per system, including an Operators Module (OM) and Maintenance and Test Panel (MTP) per channel).
>
> 5.1.2 Safety Related Control Element Assembly Calculators (two per channel).

Since the CPCS is safety-related, the NRC staff reviewed Specification 13-JN-1000 to verify that it specified the appropriate regulatory requirements and NRC-accepted guidelines for safety-related I&C. In cases where certain regulatory requirements were not cited, the NRC

staff reviewed the specification in further detail and reviewed requirements documentation to verify that the regulations were met.

Specification 13-JN-1000, Section 5.0, "Conditions of Service and General Requirements," states in part that the "...replacement systems will replicate the functions of the existing systems." The section also contains performance requirements such as field device compatibility, instrument uncertainty, and time response. Section 6.0, "Design, Materials and Construction Overview," details such items as the system layout, hardware connections, safety channel separation and operator interfaces. Section 7.0, "Qualification Requirements," addresses the environmental, seismic, and electromagnetic and radio-frequency interference (EMI/RFI) qualification that are to be accomplished for the new CPCS. This section also requires that the contractor supply and/or procure the software in accordance with 10 CFR Part 50, Appendix B.

On the basis of its review, the NRC staff concludes that the CPCS procurement Specification 13-JN-1000 identified the correct regulatory requirements, as well as NRC regulatory guidelines and accepted industry standards for the CPCS development effort. The NRC staff further concludes that the specification contains sufficient detail with regard to hardware, interface requirements, and environmental and EMI qualification to satisfy the NRC staff that adherence to the specification will meet regulatory requirements, is consistent with the guidance in NRC regulatory guidelines and accepted industry standards. Based on this, the staff concludes that the licensee's procurement specification is acceptable.

3.4.4.2.2 CPC channel separation

The Common Q acceptance SER, Section 4.4.2.3, reviewed certain aspects of appendix 2 to the Common Q topical report. Section 4.4.2.3 states in part that “Each channel is electrically independent and capable of being physically isolated from a redundant CPCS channel as required by RG 1.75." The NRC staff reviewed applicable sections of the SysRS and the HDD to confirm that channel separation exists. The only communication that exists between channels is the one-way fiber optically connected HSL links that transmit CEA positions from the CEA Position Processors to the CEACs in the other channels. The NRC staff confirmed that this data communication will be one-way and this data communication maintains CPCS channel separation. Based on this, the NRC staff concludes that CPC channel separation is acceptable.

3.4.4.2.3 CPCS connection to non-safety systems

The IEEE-603 standard discusses the independence that should exist between safety systems and other systems. IEEE-7-4.3.2, Section 5.6 states in part that "Data communication ...between safety and nonsafety systems shall not inhibit the performance of the safety function." Communication pathways exist between the CPCS and the CEAPDS, and between the CPCS and the plant computer. As such, the NRC staff reviewed the SysRS and HDD requirements to be reasonably assured that this communication would not adversely affect the safety performance of the CPCS. In a response to an NRC staff RAI, the licensee stated that the FPDS PC node box provides a buffer circuit by providing separate interface cards. The NRC staff reviewed the hardware interfaces and confirmed their physical and electrical isolation as set out in IEEE 603 and Section 5.6 of IEEE-7-4.3.2. Based on this, the NRC staff concludes that the CPCS isolation from non-safety system is acceptable.

3.4.4.2.4 CPCS to RPS interface - Interposing Relay Panel (IRP)

The IRP was not reviewed in the Common Q August 11, 2000 SER, thus, the NRC staff reviewed it for acceptability for use in the safety-related CPCS. Section 3.3.5 of the HDD discusses the IRP use and qualification. Furthermore, the IRP was qualified with the other CPC equipment as discussed in Section 3.4.6.4 of this safety evaluation. In an RAI response regarding the IRP, the licensee stated that IRP failures have a similar effect to those of the digital output card which were analyzed in the failure modes and effects analysis which is part of the Common Q topical report. In addition, the availability analysis 00000-ICE-36374 discusses the operation and use of the IRP and its effect on the CPCS. The IRP will be tested as part of the CPCS channel functional test. The NRC staff reviewed the documentation related to its failure modes and qualification for use in safety-related applications. The NRC staff finds that the IRP is qualified for use in the safety-related CPCS and that its failure modes have been appropriately dispositioned . On this basis, the NRC staff finds that the IRP is acceptable for safety-related use in the CPCS.

3.4.4.2.5 CPCS Hardware Availability

The SysRS, Section 3.5.3, identified a channel availability goal of 5×10^{-3} failures to generate a trip on demand. The NRC staff discussed with the licensee and Westinghouse the use of this goal, particularly whether it related to software, in a phone conference call on June 5, 2003, and as part of visits to Westinghouse and the licensee. The Westinghouse availability document 00000-ICE-36374 discusses the availability goal as strictly for hardware only and contains no software availability information. The availability value comes specified in NRC-approved CEN 327-A Surveillance Test Interval Extension Topical Report which was used to justify a CPCS channel functional test surveillance interval extension from 31 to 92 days, which was approved by NRC in a November 6, 1989 SER. The availability calculation, therefore, was performed to confirm that the availability value target is met. Part of the calculation relies on the premise that CPCS on-line diagnostics render the channel failure Mean Time to Detect (MTTD) negligible for all failures except for the digital output (DO) module and the IRP. As such, the NRC staff reviewed the on-line diagnostics to be employed on the CPC as presented in the SysRS and compared them to the diagnostics for the legacy system. As a result of the legacy documentation reviewed in the Westinghouse offices, personnel interviews, documentation reviews during the Westinghouse audit, and a review of the CPCS FMEA, the NRC staff found that the diagnostics to be employed on the Common Q system are more extensive and have more coverage than in the legacy system. Therefore, the premise regarding the MTTD for those failures other than the DO and IRP is reasonable. On the basis of its review of the availability analysis document and personnel interviews during the Westinghouse audit at Windsor, CT, the NRC staff also finds that the CPCS availability analysis provides reasonable assurance that the requirements in topical report CEN 327-A have been met and are acceptable.

3.4.4.2.6 Use of the OM and MTP to operate the CPCS

The Common Q acceptance SER concluded that the OM and MTP would not adversely affect the AC 160 processing functions. Therefore, the NRC staff focused its review of the OM and MTP to verify that (1), for the OM and MTP, the possibility for addressable constants to be inadvertently changed was minimized, and (2) for the MTP, the possibility for software to be

inadvertently downloaded was minimized. The NRC staff also reviewed the MTP architecture for placing channels in test.

Operators can change addressable constants via the OM or MTP similar to the legacy system. However, unauthorized changes will be detected by the use of cyclic redundancy check (CRC) automated surveillance present in the OM and MTP. Furthermore, addressable constants can only be changed within prescribed ranges. Since the OM and MTP act as safety to non-safety system interfaces, the NRC staff also reviewed the possibility of addressable constant changes as a result of connections to the CEAPDS, local area network printer, and plant computer. This was discussed in Section 3.4.4.2.3 of this SER.

Operators can download new application software via the MTP, as in the legacy system, and thus change the safety-related algorithms present in the AC 160 firmware. However, unauthorized changes will be detected due to CRC checks that are continuously performed on the firmware that stores the safety-related algorithms.

On the basis of its review of the SysRS, HDD, and the Common Q topical report, and Appendix 2 to that report, the NRC staff concludes that the use of the OM and MTP is consistent with the Common Q topical report, Section 6.3.2.1, "Datalink to External Systems," and there is reasonable assurance that the existence of these communication interfaces will not adversely affect the CPCS from performing its safety function and is consistent with IEEE-7-4.3.2, Section 5.6.

3.4.4.2.7 Previously Not Approved Hardware Used in the CPCS

In a response to an RAI, the licensee provided a hardware list for a channel of the CPCS, The NRC staff compared this list to the list of hardware reviewed in the Common Q SER dated August 11, 2000. The following two hardware components were identified that are proposed for the PVNGS CPCS implementation that were not identified in the SER: IRIG-B time card and communication card, CI-527.

The first component is an IRIG-B time card installed in the FPDS, that is used for time stamping events for the trip buffer and failed sensor stack. The card has been qualified (Seismic, EMI, environmental) to operate in the FPDS. The staff concludes that there is reasonable assurance that failure of this card does not adversely impact the safety functions operating in the CPCs or CEACs and, therefore, finds that the IRIG-B time card is appropriately used in the FPDS application.

The other component is a communication card, CI-527, which is used in the FPDS to communicate with the CPC and CEAC processors. The card has been qualified for use in the FPDS. The staff verified that the card as used is appropriate in the FPDS and finds that there is reasonable assurance that its failure would not adversely affect the CPCS safety function. The staff concludes that the CPCS hardware not previously approved by the NRC has been qualified for use in the CPCS in accordance with the requirements of 10 CFR 50, Appendix B, and is, therefore, acceptable.

3.4.4.2.8 Differences Between the System to be Installed And That Approved by NRC

The reference to that approved by NRC is a reference to that approved in the NRC Common Q SER dated August 11, 2000. Modifications to digital systems frequently occur as enhancement are identified, hardware becomes outdated or unsupported, or software revisions are needed. As such, the NRC staff was interested in changes to the Common Q platform since the system was approved by in the Common Q SER. Items within the scope of this consideration may include the hardware used in the proposed CPCS implementation, the real time OS, the function chart builder software, compilers, and communication protocols.

The licensee provided an RAI response which included some software updates and hardware additions not presented to the NRC for review for the August 11, 2000, SER or covered in Section 3.4.4.2.7. The NRC staff reviewed this response and finds that the software changes have been appropriately analyzed and tested, and, based on this, concludes that there is reasonable assurance that the changes will not adversely impact the CPCS.

The hardware additions include a FO communication box and several non-safety related communication interfaces. The FO communication box has been qualified for use in safety-related systems and the non-safety related communication interfaces are designed not to adversely impact the CPCS safety functions. Based on this, the NRC staff finds that these hardware changes and additions are reasonable and will not adversely affect CPCS functionality or operation.

The NRC staff finds that the licensee's use of the August 11, 2000, SER and its supplements to be applicable to the PVNGS upgraded CPCS based on the NRC staff's review of the SysRS, HDD, and RAI responses.

3.4.4.2.9 Channel Uncertainty

IEEE-603, Section 6.8 discusses device setpoints stating that they "shall be determined using a documented methodology." In addressing channel uncertainty, the NRC staff reviewed the following three calculations: 14273-ICE-36363, 13-JC-RJ-0205 and 13-JC-ZZ-0204.

The licensee also responded to the NRC staff’s questions regarding uncertainty as follows:

> The CPC uncertainty calculations are divided into a "typical" hardware uncertainty calculation that covers the portion of the process while it is transmitted as an analog signal and converted to a digital signal, and the portion of the uncertainty while the information is processed as a digital value. This split is required due to the completely different approach in calculating uncertainty. The hardware uncertainty calculation determines the inaccuracies of the equipment up to and including the analog-to-digital converter. The digital uncertainty considers the inaccuracies of the algorithms and computational methods, and the machine inaccuracies inside the computer process. A summary of the results in both of the areas is provided below.
>
> Analog Uncertainty
>
> The installation of the upgraded CPCS involves only the equipment in the instrumentation cabinets. The field device and the resistance to voltage converter are unchanged. The

only change in any equipment along the signal path from the process to the point where the signal is digital is the analog-to-digital converter. The uncertainty of this equipment has been analyzed by APS and has been shown to be within the bounds already allocated for the analog-to-digital converter of the legacy CPCS. Therefore, there is no change to the analyses.

Digital/Processing Uncertainty

The processing uncertainties of the Upgrade CPC, defined as those resulting from the differences in machine precision between CPCS and the more accurate CPC/CEAC Fortran Simulation, continue to be bounded (as was the case with the legacy CPCS) by those used in the safety analysis.

The NRC staff reviewed the calculations and the licensee's response regarding channel uncertainty. The NRC staff finds that the licensee and Westinghouse have appropriately used an approved uncertainty methodology which confirms that the Common Q system processing uncertainty is within the limits of those given in the UFSAR.

3.4.4.2.10 Conclusion

On the basis of its hardware review of the CPCS, discussed above, the NRC staff finds that the plant-specific hardware implementation of the Common Q CPCS at PVNGS Units 1, 2, and 3 is acceptable.

3.4.4.3 Software Evaluation

The Common Q NRC SER also approved the generic software used by the Common Q system. This includes the OS, software used to create the CPCS algorithms, the C compiler, and the software running on the operators interfaces -- OM and MTP. For the CPC safety evaluation, the NRC staff reviewed the application specific code used to operate the Common Q system as a CPC. As such, the NRC staff reviewed the application software function chart designs and their custom C code that implement the six safety-related algorithms discussed in Section 3.4.3. Furthermore, the NRC staff reviewed the software design process used by Westinghouse, and the system specification and procurement process used by the licensee to confirm that the CPCS complies with NRC regulatory requirements. The application specific software included the following areas of review which are addressed in Sections 3.4.4.3.1 through 3.4.4.3.7:

- Procurement Specification - Software
- Software Design Life-Cycle implementation
- CPCS Application Software Quality
- Requirements to Implementation - Thread Audits
- Real-Time OS Architecture - Timing
- Software Safety Analysis
- FATs (Factory Acceptance Tests) and SAT (Site Acceptance Testing)

3.4.4.3.1 Procurement Specification - Software and Westinghouse SPM

The NRC staff reviewed in detail the licensee's Procurement Specification 13-JN-1000, which contains in part detailed CPCS software system requirement. Specification 13-JN-1000,

Section 5.0, "Conditions of Service and General Requirements," states in part that the "...replacement systems will replicate the functions of the existing systems," and also contains performance requirements such as field device compatibility, instrument uncertainty, and time response. Section 9.0, "Software Requirements," contains requirements for software specification, design, and V&V, and documents that these and other software life-cycle efforts are in accordance with applicable industry standards. This section also requires that the contractor supply and/or procure the software in accordance with 10CFR50, Appendix B. The NRC staff finds that Specification 13-JN-1000 identified the correct regulatory requirements, as well as NRC regulatory guidelines and accepted industry standards for the CPCS development effort. The NRC staff also finds that the specification contains sufficient detail with regard to software, and its interface requirements that adherence to the specification will meet regulatory requirements, and is consistent with the guidance in NRC regulatory guidelines and accepted industry standards. The NRC staff used this document as a guide to ensure that software requirements were met by the vendor, Westinghouse, and that the licensee was sufficiently engaged in the V&V of Westinghouse work with respect to the requirements in the specification.

The NRC staff also reviewed the Westinghouse SPM CE-CES-195, Revision 1, approved by Common Q NRC SER dated August 11, 2000. The SPM applies to all software and firmware acquired or developed within Westinghouse for use in the Common Q system. The NRC staff used the SPM as the primary document for the software portion of the review. It was used to evaluate the software system life-cycle activities supporting the CPC development and design.

3.4.4.3.2 Software Design Life-cycle Implementation

The Common Q SER PSAI 6.5 discusses the need for the NRC staff to review, on a plant-specific basis, the implementation of the life-cycle process and its design outputs. As such, the NRC staff audited the Westinghouse software system life-cycle activities applicable to the CPCS at the Westinghouse, Windsor, CT, offices. The NRC staff interviewed the personnel responsible for specifying the software and system requirements, developing the software, testing the system, and providing V&V. As part of reviewing the software life-cycle, the NRC staff reviewed the following 26 documents at the Westinghouse offices in Rockville, MD, and Windsor, CT, to confirm that Westinghouse appropriately applied the SPM to the CPCS development:

- 00000-ICE-3208, Revision 08, *Functional Design Requirements for a Core Protection Calculator* - The function design requirements (FDR) document provides a description of the legacy—or currently installed—CPCS functional design.
- 00000-ICE-3234, Revision 06, *Functional Design Requirements for a Control Element Assembly Calculator* - This document provides a description of the legacy Control Element Assembly (CEA) Calculator (CEAC) algorithm functional design to be implemented in the CPCS. (Note that the Common Q CPCS requirements were developed from 00000-ICE-3208 and 00000-ICE-3234, and designed to be functionally identical to the legacy requirements.)
- 14273-ICE-37731, Revision 00, *Software Preliminary Hazard Analysis for the Palo Verde Nuclear Generating Station Core Protection Calculator System* - This document identifies possible software failures in the CPCS design and any potential hazardous impacts that could result from those failures.

- 00000-ICE-30158, Revision 07, *System Requirements Specification for the Common Q Core Protection Calculator System* - This document describes the hardware and software system purpose, design, constraints and interfaces. These requirements were taken from the legacy system functional design requirements (FDR).
- 00000-ICE-3233, Revision 04, *Software Requirements Specification* [SRS] *for the Common Q Core Protection Calculator System* - This document describes the software requirements for the six processors that will be present in each CPCS channel: the CPC and auxiliary processors, two CEAC 1 processors, and two CEAC 2 processors.
- 00000-ICE-30155, Revision 04, *System Requirements Specification for the Common Q Generic Flat Panel Display* - This document describes the system requirements, capabilities, and interfaces for the flat panel display user interface.
- 00000-ICE-3239, Revision 03, *Software Requirements Specification for the Common Q Generic Flat-Panel Display Software* - This document provides a description of the software, the software to hardware interfaces, the external interfaces, and error and operational displays.
- 00000-ICE-1278, Revision 00, *System Requirements Specification for the Common Q CEA Position Display* [(CEAPDS)] - This document defines the hardware and functional requirements for a CEAPDS, which interfaces with the Common Q safety related components. This system is classified as non-safety related and NRC staff review was limited to human factors and the effect of the CEAPDS on the safety-related CPCS.
- 00000-ICE-1279, Revision 00, *Software Requirements Specification for the Common Q CEA position Display System (CEAPDS)* - This document provides the software requirements for the CEAPDS.
- 00000-ICE-30165, Revision 02, *Software Design Description for the Common Q Core Protection Calculator System STATIC DNBR and Power Density Program* - This document describes the software design of the custom PC elements that constitute the STATIC program. Custom PC elements are software units that are specifically written for an application, in this case the CPCS. They are written in the C programming language and become part of the function blocks that are later connected in the application software to form the application specific portion of the Common Q platform.
- 00000-ICE-30107, Revision 02, *Common Q Core Protection Calculator System Software Design Description DNBR and Power Density UPDATE Program Decomposition* - This document describes the software design description of the custom PC elements that constitute the UPDATE program.
- 00000-ICE-30108, Revision 02, *Coolant Mass Flow Program Decomposition, Failed Sensor Stack Program Decomposition, Trip Sequence Program Decomposition, [and] Trip Buffer Selection Program Decomposition for the Common Q Core Protection Calculator System Software Design Description* - This document describes the software design description of the custom PC elements for the FLOW, FAILSENS, TRIPSEQ, and TRIPBUFF 1, 2, 3 and 4 programs. The NRC staff focused on FLOW and TRIPSEQ as these are the two of the six safety-related algorithms discussed in the CPC system requirements document and the CPC licensing topical report, WCAP-16097, *Common Qualified Platform Core Protection Calculator System*.
- 00000-ICE-30106, Revision 02, *Common Q Core Protection Calculator System Software Design Description, POWER Distribution Program Decomposition* - This document describes the software design description of the custom PC elements for the POWER program.
- 00000-ICE-30129, Revision 02, *Software Design Description for the Common Q Core Protection Calculator System Core Element Assembly Calculator* - This document

describes the software design description of the PC elements for the CEAC penalty factor program.

- 00000 - ICE - 37756, Revision 02, *Code Review Report for the Common Q Core Protection Calculator DNBR and Power Density Update Program* - This report documents Westinghouse personnel review of the program source code. This document describes the software modules that were reviewed, and provides a tracking history for software problems that were found and their resolution.
- 00000-ICE-37781, Revision 00 draft, *Requirements Traceability Matrix* [RTM] *for the Arizona Public Service Core Protection Calculator System Project* - This document tracks the CPCS requirements throughout the CPCS development life-cycle. The RTM is also used by the developers for cross referencing software requirements, and assists the reviewer in tracking the propagation of the CPCS requirements through each phase of the system life-cycle. The RTM is a living document that continues to be changed as the CPCS is developed. Consequently, the RTM is a draft document that cannot be finalized until after the CPCS development effort is completed and the system is installed in the plant.
- 00000-ICE-35249, Revision 03, *Test Plan for the Common Q Core Protection Calculator System* - This document describes the overall plan for testing the CPCS including test procedures, test performance, and test reports.
- 00000-ICE-35293, Revision 00, *Module Test Procedure for the Common Q Core Protection Calculator System* - This document describes the test plan for the custom PC elements that were designed using the function chart builder.
- 00000-ICE-35399, Revision 01, *Unit Test Procedure for the Common Q Core Protection Calculator System*, Revision 01 - This document describes the unit testing procedure, which discusses three tests: the dynamic test, the input sweep test, and the live input test. A unit consists of an integrated set of software modules.
- 00000-ICE-35483, Revision 02, *Unit Test Procedure for the One Channel Common Q Core Protection Calculator System* - This document defines the one-channel system test (OCST) test procedure, which is used to validate the functionality of one channel of the CPCS. This test procedure does not test the interactions between multiple CPCS channels.
- 00000-ICE-37367, Revision 00, *Dynamic Test Report for the Common Q Core Protection Calculator* - This document reports the results of the CPCS dynamic testing. The test cases exercised dynamic portions of the CPC algorithms by modeling design basis events. An I/O simulator was used to provide inputs and read/store output results. The test bed was the single channel facility at Windsor, CT.
- 00000-ICE-37373, Revision 00, *Input Sweep Test Report for the Common Q Core Protection Calculator* - This document reports the results of the input sweep tests. The input sweep test was designed to verify that the CPCS algorithms will initialize to a steady state condition for each of a number of input combinations within the CPCS operating space.
- 00000-ICE-37765, Revision 00, *Live Input Test Report for the Common Q CPCS* - This document reports the results of live input testing. Live input tests validate that the dynamic response of the CPC software is consistent with that predicted by design analysis. Live input testing is used to evaluate the integrated hardware/software system performance in the CPCS operational modes.
- 00000-ICE-35488, Revision 00, *Four Channel Factory Acceptance Procedure for the Core Protection Calculator System* - This document describes the procedure for the four channel system test (FCST) of the CPCS. The FCST tests those functions not tested in

the unit testing or OCST, and is also used to test the integrated system. Test exception reports are generated as necessary and fed back for correction via software change requests.

- 14373-ICE-37777, Revision 00, *Hardware Acceptance Test Report for the Palo Verde Nuclear Generating Station Unit 2 Core Protection Calculator System* - This document reports the results of the hardware factory acceptance tests performed in the Westinghouse Nuclear Automation facility in Monroeville, PA.
- CEN-327, dated January, 1989, *RPS/ESFAS Extended Test Interval Evaluation* - This report provides a basis for requesting changes to the Technical Specification surveillance testing requirement for selected components in the Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS). This topical report was approved in an NRC SER dated November 6, 1989.

The NRC staff reviewed this documentation in varying levels of detail using Specification 13-JN-1000 and the SPM, and compared the software life-cycle documentation listed above to the specification and the SPM. The NRC staff finds that, with only a few minor exceptions, Westinghouse has followed and appropriately applied the SPM to the CPCS development effort. Those exceptions that were taken were deemed to be of little impact or were addressed by means other than those explicitly set out in the SPM. One example of this was the specification of safety requirements. The SPM requires that software safety requirements be identified in the software requirements specification. The NRC staff found that these software safety requirements were not present in the SRS. However, Westinghouse pointed out that the requirements for the legacy system were being directly and completely translated to the Common Q platform, and hence the SRS did not need a section outlining software safety requirements in this case. The NRC staff finds this justification acceptable.

To reduce the risk of new software/hardware hazards being designed into the new system, the NRC staff reviewed Westinghouse's adherence to their coding standard for the C programming language and interviewed Westinghouse on their approach to identifying new software hazards as a result of the use of the C programming language and the software system architecture changes from the legacy system. The NRC staff also reviewed the preliminary software safety documentation and determined that the exception taken to the SPM requirement is reasonable.

The NRC staff also visited the PVNGS site to ascertain the scope of the licensee's involvement in the development and design process for the CPCS project. The licensee provided the following documentation for NRC staff review:

- Specification 13-JN-1000, Rev. 2, *Engineering Specification for the Core Protection Calculator / Control Element Assembly Calculator (CPC/CEAC) System for Palo Verde Nuclear Generating Station* - The engineering specification provides the requirements to design, fabricate, test, deliver, and startup the new CPCS and includes applicable regulations, NRC regulatory guides, and industry standards.
- 80DP-0CC01, *Control of Software and Data for Digital Process Control and Monitoring Systems* - This document describes the life-cycle process, standards compliance, design reviews and audits, and documentation requirements for digital process control and monitoring software, data, firmware, and associated software development systems.
- 87DP-0CC08, *Control of Vendor Documentation* - This document discusses the preparation, configuration management, and use of vendor engineering, quality and

shipping documents. The scope of this document includes many of the documents that the NRC reviewed as part of the software system audit in Windsor, CT.

- Critical Design Review Minutes: April 2003, August 2002, March 2002, and October 2001. These notes documented the discussion items between the licensee and Westinghouse, and resolution of various aspects of the CPCS design and installation.
- Notes and results of the licensee's visits to Westinghouse in Pittsburgh, February 2003. These notes describe the results of the licensee's visit to Westinghouse, and discusses system anomalies, test cases and status, and human factors.

In an RAI response, the licensee responded to the NRC staff's question regarding the licensee's justification for concluding that software requirements per Specification 13-JN-1000 were complete and correct. The licensee responded in part as follows:

1. Westinghouse has provided to APS the required types of software documentation, such as System Requirement Specifications, Software Requirements Specifications, Software Design Descriptions (SDD), V&V documentation and Software Testing/Analysis documentation.

2. The format and generic content of each of the documents is consistent with the expectations within APS. It was not the intent of the Specification to require Westinghouse to follow exactly any of the sample document formats described in any of the IEEE documents.

3. APS reviews of the individual documents and an APS lead SQA surveillance audit conducted at Westinghouse has provided APS with confidence that the specific content of individual documents and Westinghouse compliance with SQA requirements has been met. Reviews were typically conducted by the responsible engineering group within APS. This included OCS Engineering, Nuclear Fuels Management (NFM), Equipment Qualification (EQ), and EMI/RFI experts. The NFM department was primarily responsible to ensure that the new CPCS algorithms were functionally identical to the legacy system algorithms. The OCS engineering group was primarily responsible to ensure the hardware and its interfaces would be compatible. When there were discrepancies, comments would be submitted to Westinghouse. Typically, responses to the comments would be provided by Westinghouse to development an agreement, and then the document would be revised to reflect the final understanding. The personnel most knowledgeable in the area, plus others conducted these reviews. For example, NFM personnel would review all SDDs, since they were knowledgeable of the CPC algorithms. OCS Engineering and Maintenance would review the Hardware Design Descriptions (HDDs). EQ and EMI/RFI personnel would review qualification reports.

4. APS also conducted four Critical Design Reviews (CDRs) with Westinghouse. These CDRs looked at the overall hardware and software design of the system, helped guide the design, and provided action items to both APS and Westinghouse to ensure the system to be provided was the system that was both specified and desired.

5. APS also observed three factory acceptance tests (FATs). The first two were primarily APS personnel observing the conduct of the formal FAT procedures. The third FAT was time set aside for APS to send a cross-functional team to insert different failures, and

conduct tests outside of the scope of the formal FAT procedures. Knowledgeable APS personnel created a set of potential failures or off normal conditional that were then placed in the four channel hardware. The response was documented and compared against expected behavior where requirements existed.

During the visit to PVNGS, the NRC staff reviewed the results of these licensee meetings and reviews, and concludes that the licensee has been satisfactorily involved in the design and verification process and has provided reasonable assurance that the requirements in Specification 13-JN-1000 have been met.

3.4.4.3.3 CPCS Application - Software Quality

HICB-14, "Software Reviews," states in part that Implementation of an acceptable software life cycle provides the necessary software quality and further that software quality is an important element in preventing the propagation of common-mode failures. The August 11, 2000, Common Q SER states in part that "The quality of the plant-specific Common Q system is dependent on the licensee's proper implementation of the CENP software program manual." This manual refers to the SPM, which was addressed in the previous section. Because the SPM was appropriately used, the NRC staff concludes that the CPCS application-specific software is of reasonable quality to be employed in the CPCS safety-related application at PVNGS.

3.4.4.3.4 Requirements to Implementation - Thread Audits

PSAI 6.8 of the Common Q SER states that the licensee must verify that the new system—the Common Q platform—provides the same functionality as the system that is being replaced—the legacy system. In order to confirm this, the NRC staff performed two thread audits of CPCS functions which included a detailed review of the implementation of those functions. These requirements were traced through the software system life-cycle phases including the following: requirements development/translation, design description and coding, function chart generation, V&V activities, software test phases, hardware and software integration, and FATs. This review included evaluating actual sections of the code and following the signal path through the hardware circuitry.

One thread audit reviewed the LPD function. The LPD control algorithm uses the hot leg temperature (Thot), the cold leg temperature (Tcold), the pressurizer pressure (Ppzr), the RCP speed, excore nuclear instrumentation readings, and CEAC positions to calculate a static and dynamic reactor core LPD. This value is compared against an allowable value to determine whether or not to generate a RPS trip. The NRC staff performed a thread audit of this function by tracing the detailed operation field sensor input and digital conversion, LPD algorithm calculation and setpoint comparison, and output of the system results to the RPS interface. The NRC staff also compared the timing requirements of the PVNGS UFSAR for the LPD function to ensure the timing requirements of the existing plant protection systems were achieved by the new system. This included a detailed evaluation of the Westinghouse documentation to ensure requirements were correctly translated from the legacy system documentation to the proposed Common Q system. The NRC staff performed another thread audit which included the RCP speed sensing system to determine if the RCP speed was correctly converted to flow, which is used in several of the functions of the CPCS.

In both thread audits, the NRC staff used the RTM to aid in tracing requirements for the chosen thread audits. In these audits, the NRC staff was able to adequately trace through the requirements from the legacy system to the proposed CPCS through the entire life-cycle. Based on this, the NRC staff concludes that there is reasonable assurance that the legacy system requirements have been appropriately translated to the new CPCS system.

3.4.4.3.5 Real-Time OS Architecture - Timing

PSAI 6.6 of the Common Q SER states that licensees must review the timing and validation for application specific implementation of the Common Q system in order to verify timing requirements are met. The CPC timing analysis is described in document 00000-ICE-36369, *CPC Timing Analysis for the Common Q Core Protection Calculator System*. HICB-21, "Real Time Performance," provides guidance to the NRC staff regarding digital system timing analysis.

The NRC staff reviewed the CPCS software to confirm that the algorithms meet or exceed (1) the legacy system timing and (2) the timing requirements specified in the PVNGS UFSAR. The NRC staff also reviewed the timing analysis document 00000-ICE-36369 and considered the timing delays that exist in a 2 out of 4 (2/4) system. These aspects included the timing variation (worse case) that may exist due to process scheduling and the worse case processor clock timing that may exist due to processor drift. This also included the worse case time delay that may exist in data transfer of penalty factor from the CEAC processor to the CPC processor. The NRC staff also reviewed the system testing used to validate the FSAR timing requirements.

The NRC staff noted several changes to the CONTRM cycle times from those in the legacy system, particularly the UPDATE and POWER CONTRMS. These changes were needed as a result of analyses which considered worst case timing aspects found in a 2/4 digital acquisition system. The new cycle times for these processes improved the timing performance and, according to the licensee in an RAI response, all UFSAR time requirements associated with the CPCS have been met.

The NRC staff reviewed the CPCS test plan, document 00000-ICE-35249, and confirmed acceptance criteria for time response and accuracy. During the software system audit in Windsor, CT, the NRC staff reviewed the testing documentation to confirm that the timing requirements were met. Furthermore, the NRC staff performed a critical timing analysis of the real time architecture to determine if errant interrupt handling or CONTRM scheduling could cause UFSAR timing limits to be exceeded, safety-algorithms to be bypassed, or CONTRMs to stall program flow. In these postulated cases, the NRC staff determined that safety-related algorithms will run and the WDT will time out causing a channel trip if the CONTRMs stall program flow. Therefore, the NRC staff finds that the timing analysis has correctly identified worst case timing for the CPCS and the validation tests verify that the Common Q CPCS will satisfy the plant-specific requirements for accuracy and response time.

3.4.4.3.6 Software Safety Analysis

HICB-14 discusses the use of software safety plan (SSP) in the software life-cycle. The Westinghouse SPM, which contains the SSP in section 3, was prepared using the guidance in HICB-14. The NRC staff reviewed Westinghouse's implementation of Section 3 of the SPM and also reviewed the software preliminary hazard analysis document 14273-ICE-37731.

During the software system audit, that NRC staff interviewed Westinghouse personnel regarding use of the C programming language to implement the safety-related algorithms. This discussion included considerations of the C programming language and potential system hazards due to its use. To aid in this discussion, the NRC staff considered the guidance of NUREG/CR-6463, Revision 1, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems," Section 4 - C and C++. This report provides guidance to the NRC on auditing of programs for safety systems written in ten programming languages including C.

Document 14273-ICE-37731 references and uses the guidance present in NUREG/CR 6430, Revision 2, "Software Safety Hazard Analysis," which provides guidance on considering hazards attributed to software. The NRC staff used NUREG/CR 6430 as guidance in reviewing 14273-ICE-37731 and in its interviews with Westinghouse software engineering personnel.

To reduce the risk of new software/hardware hazards being designed into the new system, the NRC staff reviewed Westinghouse's adherence to their coding standard for the C programming language and interviewed Westinghouse personnel on their approach to identifying new software hazards as a result of the use of the C programming language and the software system architecture changes from the legacy system. As part of the effort to identify errors, the NRC staff interviewed the licensee's personnel to ascertain their involvement in the software safety analysis process. The licensee performed two notable tasks in this area. Operation personnel familiar with the operation of the legacy CPCS postulated scenarios to challenge the operation of the Common Q CPCS. These abnormal operational scenarios were sent to Westinghouse in the form of test cases. As a result of these test cases, several improvements were made to the CPCS software. The licensee also provided an RAI response identifying events or errors that had occurred on the legacy system during its operation and how these were corrected. The RAI response identified four reportable events and discussed the Common Q response to each. In some cases, the lessons learned from these events resulted in software improvements. Based on this, the NRC staff finds that the licensee was sufficiently engaged in the effort to identify software hazards in the Common Q system and that those identified have been corrected.

3.4.4.3.7 FATs and SAT

The licensee discussed the FATs and SAT in its application. The submittal outlines the purpose and content of both tests. The FATs contain a comprehensive suite of tests that cover the SysRS functional requirements and all test anomalies and failures have been dispositioned and corrected. Based on its review of the FATs documentation, the NRC staff finds that the FATs have appropriately identified the requirements to be tested and provides reasonable V&V that the Common Q CPCS will operate as specified.

The NRC staff requested additional information concerning the SAT in an RAI. In the response, the licensee reported that the SAT procedure is not complete. The SAT will be conducted after the CPCS is installed in each unit during the refueling outage in which it is installed. However, the licensee did outline the procedural items and the time response, calibration and functional tests to be performed. Based on its review, the staff also finds that the SAT items identified in the RAI response provides assurance that the plant-specific operational aspects such as field devices, RPS interfacing and PVNGS environs will be adequately tested to confirm the operability of the CPCS.

Because this new CPCS is first being installed in Palo Verde, the NRC staff intends to visit the PVNGS Unit 2 to observe the performance of portions of the SAT in the upcoming Fall 2003 refueling outage. The NRC staff is not planning to observe the SATs for Units 1 and 3 in their refueling outages, and it has not required that this testing be performed at Unit 2 before issuance of the license amendment. By the definition of "operable" in the TSs, if the SAT is not passed, the new CPCS can not be declared operable by the licensee for the restart of the units from the refueling outages in which the Common Q CPCS is installed.

3.4.4.3.8 Conclusion

On the basis of its software review, which is discussed above, the NRC staff finds that the application-specific software used in the Common Q CPCS at PVNGS Units 1, 2, and 3 is acceptable.

3.4.5 Regulatory Compliance

The following subsections discuss the degree of regulatory compliance of the Common Q CPCS. The GDCs listed in Appendix A to 10 CFR Part 50 establish the minimum requirements for the design of nuclear power plants; 10 CFR 50.55a(h) incorporates IEEE Standard 603-1991. The regulatory guides and endorsed industry codes and standards listed in SRP Table 7-1 are the guidelines used as the basis for this evaluation.

Section 50.55a(a)(1) is addressed by conformance with the codes and standards listed in the SRP. In the specification, design and testing development phases, the vendor used codes and standards that are the same as or equivalent to the standards identified in the SRP. Based on this, the NRC staff concludes that the Common Q CPCS conforms with this requirement.

Section 50.55a(h) endorses IEEE Standard 603-1991, which addresses both system-level design issues and criteria for qualifying safety-related devices. Procurement specification 13-JN-1000 requires the compliance with IEEE-603, 1991. The NRC staff reviewed the Common Q CPCS against IEEE-603 design-basis requirements of Sections 4.1 through 4.12; the safety system requirements of Sections 5.1 through 5.15; the function and design requirements of Sections 6.1 through 6.8; the function requirements of Sections 7.1 through 7.5; and the power source requirements of Sections 8.1 through 8.3. The NRC staff reviewed the application, documentation submitted August 13 and September 18, 2003, and document at the Westinghouse offices and PNVGS. Based on these reviews, the NRC staff concludes that the CPCS using the Common Q platform satisfy the requirements of 10 CFR 50.55a(h) with regard to IEEE Standard 603-1991.

As stated in Section 2.0 of this safety evaluation, the NRC staff determined that the following GDCs specified in Appendix A to 10 CFR Part 50 were the applicable design criteria for this review:

- GDC 1, on quality standards and records
- GDC 2, on design basis for protection against natural phenomena
- GDC 4, on environmental and dynamic effects design bases
- GDC 13, on instrumentation and control
- GDC 20, on protection system functions
- GDC 21, on protection system reliability and testability

- GDC 22, on protection system independence
- GDC 23, on protection system failure modes
- GDC 24, on separation of protection and control systems
- GDC 25, on protection system requirements for reactivity control malfunctions
- GDC 29, on protection against anticipated operational occurrences

GDC 1 requires that structures, systems, and components (SSCs) important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. The NRC staff reviewed the equipment description for conformance to the guidelines in the regulatory guides and industry codes and standards that apply to this equipment. Based on its review of the APS procurement specification requirements that specify conformance to these quality standards, the NRC staff concludes that there is reasonable assurance that the CPCS Common Q system conforms to the applicable guidelines and regulatory criteria of GDC 1.

GDC 2 requires that SSCs important to safety shall be designed to withstand the effects of natural phenomena and GDC 4 requires that SSCs important to safety be designed to accommodate the effects of, and to be compatible with, the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including LOCAs. Based on the licensee's procurement specification requirements and the requirements specified in the SysRS and HDD, the NRC staff concludes that the licensee and the vendor have specified, designed and tested CPCS Common Q system consistent with the design bases for the intended safety-related application, and, therefore, these system designs are in accordance with the requirements of GDC 2 and 4.

GDC 13 requires that instrumentation shall be provided to monitor variables over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. GDC 13 requires that appropriate controls shall be provided to maintain these variables and systems within their prescribed operating ranges. The NRC staff reviewed the derivation of the uncertainty as presented in the three submitted calculations, and found it to be consistent with the recommendations of Regulatory Guide 1.105. This was discussed in Section 3.4.4.2.9, "Channel Uncertainty," of this safety evaluation. The vendor qualified the CPCS Common Q system for the environment in which the systems are to operate and this was verified by the licensee. This is discussed in Sections 3.4.6.1 and 3.4.6.4 on PSAIs 6.1 and 6.4, respectively. On the basis of these activities, the NRC staff concludes that the CPCS Common Q designs were in accordance with GDC 13.

GDC 20 requires that protection systems be designed to sense accident conditions and to initiate the operation of systems and components important to safety. On the basis of its review of the translation of the legacy CPCS system requirements to the Common Q CPCS and the satisfactory conclusions on the suitability of the Common Q CPCS hardware and software in Sections 3.4.4.2.10 and 3.4.4.3.8 of this safety evaluation, the NRC staff concluded that the CPCS Common Q system is designed to sense accidents and to initiate the operation of equipment to respond to the accidents, and, therefore, the system is in accordance with the requirements of GDC 20.

GDC 21 requires that the protection systems be designed for high functional reliability and in service testability commensurate with the safety functions to be performed, and that no single failure results in loss of the protection function. These systems must be designed to permit periodic testing of their functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred. On the basis of the NRC staff's review of the Common Q CPCS system in Sections 3.4.6.7 and 3.4.2.1 of this safety evaluation, the NRC staff concludes that the system conforms to the guidelines for periodic testing in RG 1.22 and RG 1.118, which meet GDC 21. The CPCS Common Q upgrade also conforms to the guidelines regarding the application of the single-failure criterion in IEEE Standard 379, as supplemented by RG 1.53. This is based on the requirements given in the licensee's procurement specification which was verified by the NRC staff to contain the appropriate regulatory requirements, including the single failure criteria. The NRC staff further concluded that the Common Q system is consistent with the guidance of IEEE Standard 603 with regard to system reliability and testability. Therefore, the NRC staff finds that the CPCS design is in accordance with the requirements of GDC 21.

GDC 22 requires that protection systems be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or the systems shall be demonstrated to be acceptable on some other defined basis. On the basis of its review addressed in the Common Q SER and in Section 3.4.6.11 of this safety evaluation, the NRC staff finds that the CPCS Common Q design is in accordance with the requirements of GDC 22.

GDC 23 requires that protection systems be designed to fail into a safe state. On the basis of its review addressed in Sections 3.4.4.2.6 and 3.4.6.10 of this safety evaluation, the NRC staff concludes that the CPCS implementation was designed to fail into a safe mode and, therefore, the CPCS Common Q design is in accordance with the requirements of GDC 23.

GDC 24 requires that protection systems be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. IEEE Standard 603 is an acceptable method to meet GDC 24. On the basis of its review of the interfaces between the CPCS and other plant systems addressed in Section 3.4.6.4 of this safety evaluation, the NRC staff concludes that the CPCS Common Q system design satisfies the guidance of IEEE Standard 603 with regard to control and protection system interactions and, therefore, is in accordance with the requirements of GDC 24.

GDC 25 requires that protection systems be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems such as accidental withdrawal of control rods. The CPCS design basis requirements cover reactivity control system accidents such as the accident withdrawal of controls rods. On the basis of its review that the Common Q CPCS was designed to the same system and functionality requirements as that approved by the NRC staff for the legacy system, and the NRC staff concluded that the legacy system met GDC 25 in NUREG-0857 dated November 1981, and its supplements, which licensed PVNGS, the NRC staff concludes that the CPCS Common Q system design is designed in accordance with GDC 25.

GDC 29 requires that protection and reactivity control systems be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences. The NRC staff discussed the defense against common mode failure for the CPCS in its discussion of PSAI 6.11, in Section 3.4.6.11 of this safety evaluation, in that PSAI 6.11 requires defense against common-mode failure in digital instrumentation and control systems. In Section 3.4.6.11, the NRC staff concludes that licensee has appropriately addressed PSAI 6.11. In Section 3.4.4.3.4 of this safety evaluation, the NRC staff further finds that legacy functionality has been translated to the Common Q system with reasonable assurance. On this basis and the basis of its review of the software system life-cycle documentation as discussed in Section 3.4.4.3 of this safety evaluation, the NRC staff concludes that the CPCS Common Q system design is designed in accordance with GDC 29.

On the basis of the above conclusions, the NRC staff determines that the CPCS Common Q system's design is in accordance with the relevant requirements of GDCs 1, 2, 4, 13, 20, 21, 22, 23, 24, 25, and 29. Based on this, the NRC staff concludes that the CPCS Common Q system has been designed to function in accordance with the requirements of 10 CFR 50.55a(a)(1) and 55a(h), and GDCs 1, 2, 4,13, 20, 21, 22, 23, 24, 25 and 29. On this basis and because of the affirmative conclusions in Sections 3.2 on human factors considerations and Section 3.3 on reactor systems, the NRC staff concludes that the Common Q system is acceptable for use in safety-related applications as a CPCS at PVNGS Units 1, 2 and 3.

3.4.6 Licensee's Disposition of Common Q SER PSAIs

The Common Q SER date August 11, 2000, lists fourteen PSAIs that must be performed by a licensee when requesting NRC approval for installation of a Common Q system. In the following subsections, the NRC staff discusses each PSAI, the licensee's disposition, and the NRC staff's conclusion regarding the disposition.

3.4.6.1 PSAI 6.1

PSAI 6.1 states that "Each licensee implementing a specific application based upon the Common Q platform must assess the suitability of the S600 I/O modules to be used in the design against its plant-specific input/output requirements."

The licensee responded as follows:

> The suitability of all new components are assessed to meet applicable requirements in accordance with the PVNGS Quality Assurance Program. Performance requirements for these components are assured, for example, by specifying them in purchase contracts, observing vendor testing and analysis, reviewing vendor documentation, performing design reviews by the engineering department, and by performing validation tests after installation. All these activities are controlled by PVNGS administrative procedures. The Input/Output Subsystem incorporated as part of the design specification for the Common Q CPCS replacement has been designed to fully meet the functional requirements set forth in the System Requirements Specification (SysRS) for the Common Q Core Protection Calculator System. These requirements meet or exceed the equipment qualification requirements for PVNGS. The Input/Output subsystem will be deemed capable of performing its design function by successful completion of testing, culminating in a Factory Acceptance Test (FAT) to be performed by the vendor at the

> Westinghouse manufacturing/engineering facility. Acceptance criteria will be based on the SysRS. Environmental and seismic testing have already been successfully completed per Westinghouse test plans.

In a response to an NRC staff RAI, the licensee confirmed that "The FATs performed at Westinghouse have demonstrated that all appropriate performance requirements (e.g., time response, accuracy, etc.) were met, and therefore APS [the licensee] considers the individual modules having met their performance requirements for PVNGS." The NRC staff reviewed the FAT procedures and the results relating to the I/O modules. The NRC staff also interviewed Westinghouse personnel regarding I/O compatibility with existing field devices. Since Westinghouse was involved in the engineering of the legacy system, they had retained the knowledge needed to specify the interface requirements for field devices including impedance matching and scaling. The SAT to be performed before plant startup will serve to verify this interfacing. Therefore, based on the FATs and the SAT to be completed after installation, the NRC staff considers that the licensee has appropriately addressed PSAI 6.1.

3.4.6.2 PSAI 6.2

PSAI 6.2 states that "A hardware user interface that replicates existing plant capabilities for an application may be chosen by a licensee as an alternative to the FPDS. The review of the implementation of such a hardware user interface would be a plant-specific action item."

The licensee's responded as follows:

> APS intends to use the Flat Panel Display System (FPDS) as developed by Westinghouse for the CPCS. An alternative hardware interface will not be used. Therefore, this action item is not applicable.

The NRC staff confirmed that the licensee intends to use the FPDS. Based on this, the NRC staff considers that the licensee has appropriately addressed PSAI 6.2.

3.4.6.3 PSAI 6.3

PSAI 6.3 states that "If a licensee installs a Common Q application that encompasses the implementation of FPDS, the licensee must verify that the FPDS is limited to performing display and maintenance functions only, and it is not to be used such that it is required to be operational when the Common Q system is called upon to initiate automatic safety functions. The use of the FPDS must be treated in the plant specific FMEAs."

The licensee's responded as follows:

> The FPDS to be purchased by APS will be limited to performing display and maintenance functions only. The plant specific Failure Mode Effects Analysis (FMEA) prepared in accordance with PSAI 6.10 will address the loss of the FPDS. Additionally, the NRC in their Safety Evaluation for the Closeout of Several of the Common Qualified Platform Category 1 Open Items Related to Reports CENPD-396-P, Revision 1 and CE-CES-195 Revision 1, dated June 22, 2001, (Ref. 3 [in the RAI letter]) has stated that this action item has been resolved and is considered closed. Therefore, [the licensee concludes that] no further evaluation is required.

The Staff reviewed its June 22, 2001 SER (supplement 1 of the SER dated August 11, 2000) and confirmed that this action has been resolved and no further evaluation is required of a licensee. Based on this, the NRC staff considers that the licensee has appropriately addressed PSAI 6.3.

3.4.6.4 PSAI 6.4

PSAI 6.4 states that "Each licensee implementing a Common Q application must verify that its plant environmental data (i.e., temperature, humidity, seismic, and electromagnetic compatibility) for the location(s) in which the Common Q equipment is to be installed are enveloped by the environment considered for the Common Q qualification testing, and that the specific equipment configuration to be installed is similar to that of the Common Q equipment used for the tests. CENP configured the Common Q test specimen for seismic testing using dummy modules to fill all the used rack slots. As part of the verification of its plant-specific equipment configuration the licensee must check that it does not have any unfilled rack slots."

The licensee's responded as follows:

> The environmental conditions occurring in PVNGS control buildings consist of temperature, pressure and humidity conditions. CPCS equipment will be located in a mild (non-harsh) environment. Therefore, age related degradation is expected to be insignificant for temperature and humidity. The CPCS equipment (elevation 140' of control building) will be exposed to the following environmental conditions during the life of the plant.

Parameter	**Normal**		**Duration**	**Abnormal**		**Duration**
	Min	**Max**		**Min**	**Max**	
Temperature	65F	104F	Continuous	55F	122F	8 Hours
Humidity	40% RH	60% RH	Continuous	20% RH	90% RH	8 Hours
Pressure	Atmosph	Atmosph	Continuous	Atmosph	Atmosph	Continuous
Radiation	Negligible	Negligible	Continuous	Negligible	Negligible	Continuous

> The Common Q CPCS has been environmentally qualified by Westinghouse for the environmental conditions described in the table below (on page 41) that result from abnormal conditions for which it must operate. No condensation formed on the test item during any phase of the testing.

Parameter	Abnormal		Duration
	Min	Max	
Temperature	40F	140F	12 Hours
Humidity	20%	95% RH	12 Hours
Pressure	Atmospheric	Atmospheric	Continuous

During anticipated abnormal transients/conditions, the essential HVAC system maintains the essential areas (control room, computer room and associated rooms at elevation 140') within normal design ambient temperature, pressure and humidity conditions. Therefore, the environmental conditions do not increase above normal design conditions as a result of anticipated abnormal transients/conditions. Based on the above, the environment considered for the Common Q qualification testing envelopes the specific PVNGS temperature and humidity conditions.

The licensee's response to PSAI 6.4 (Seismic Testing)

The seismic qualification of the Common Q Equipment for PVNGS has been completed by Westinghouse. APS has evaluated the Required Response Spectra (RRS) cited in the Westinghouse Seismic Test Plan for OBE, SSE, and Table Limits, and has determined that they are significantly higher than the PVNGS floor response spectra curves documented in the Palo Verde Equipment Qualification Program Manual for the area where the CPC/CEAC system will be installed (140 ft control building), and therefore, envelopes the seismic criteria for PVNGS.

The dummy modules populating the unused chassis slots during seismic testing are essentially the outer cases and front faces of modules similar in size and appearance to the active modules, but lacking the internal electronics and associated hardware.

Installation of the Common Q CPCS hardware at PVNGS will include dummy modules in unused chassis slots. Plant modification documents used for implementing the Common Q CPCS at PVNGS will specify this requirement. PVNGS administrative procedures, which ensure equipment qualifications (e.g., seismic, etc) are maintained in the design change process, will control all future changes to the CPCS.

The licensee's response to PSAI 6.4 (EMI/RFI)

Westinghouse is performing specific EMI/RFI tests on the CPCS equipment in accordance with EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," Revision 1. The test data collected by Westinghouse will be compared to NUREG/CR-6431 and Palo Verde's EMI/RFI Engineering study by Palo Verde Engineering. These comparisons will verify that the new CPCS will not be affected by the existing EMI/RFI environment. These comparisons will also verify that the new CPCS will not introduce EMI/RFI at levels that would affect surrounding equipment.

The NRC staff reviewed the licensee's temperature and humidity environment of the control room and those that the Common Q system was tested to, and finds that for temperature and humidity the plant environment is bounded for that which the Common Q has been tested.

For seismic, the licensee has confirmed that the required response spectra for the Common Q equipment is enveloped by the spectra the Common Q was tested for.

For EMI/RFI, the NRC staff reviewed the RAI response regarding the operational anomaly related to the RE102 radiated emissions test, which was discussed in the SER supplement dated February 24, 2003. In its August 13, 2003, response, the licensee stated that, through the use of an EMI consultant, CHAR Services Inc., it has evaluated these radiated emissions at higher than the specified limits and has determined that the radiated emissions do not affect equipment within the surrounding area. Furthermore, an in-situ EMI/RFI test will be performed by Wyle Labs to test the CPC in an open rack to verify that the CPCS meets RE101, RE102, RS101, and RS103 specifications. Wyle labs will make recommendations if the CPC fails any of the tests regarding what type of shielding should be used on the CPC cabinet or rack to meet those standards. The tests must be completed satisfactorily so that the CPCS is considered operable.

The EMI/RFI test to be performed is part of the licensee's regulatory commitment discussed in Section 3.6 of this safety evaluation.

Based on the (1) discussion above, (2) licensee's efforts to verify environmental requirements are met, and (3) interviews with licensee personnel during the PVNGS visit, the NRC staff concludes that the licensee has appropriately addressed PSAI 6.4.

3.4.6.5 PSAI 6.5

PSAI 6.5 states that "On the basis of its review of the CENP's software development process for application software, the [NRC] staff concludes that the SPM specifies plans that will provide a quality software life cycle process, and that these plans commit to documentation of life cycle activities that will permit the [NRC] staff or others to evaluate the quality of design features upon which the safety determination will be based. The [NRC] staff will review the implementation of the life cycle process and the software life cycle process design outputs for specific applications on a plant specific basis."

The licensee responded as follows:

> In accordance with the PVNGS Quality Assurance Program, APS uses administrative control procedures to establish software quality assurance and configuration management for process computer software, firmware and associated software development computer systems, and associated documentation. They ensure that the integrity of a process software product is known and preserved throughout its life cycle (from development to retirement). These controls also apply to the development tools and systems used to develop and test process software.
>
> As is already required by administrative control procedures, APS will maintain documentation of the Common Q CPC Software Life Cycle Process provided by Westinghouse for both the Implementation Activities and the required Design Outputs.

> This documentation is for internal use and to allow for the NRC staff review. This documentation will include life-cycle process documentation provided by Westinghouse (i.e. Safety Analysis Activities, V&V plans, V&V results, Testing Results) as well as installation test activities performed and documented by APS in accordance with Plant Modification Processes. ... Per procedural requirements, APS also maintains the requirements documents provided by Westinghouse (i.e. Functional Design Requirements, System Specifications, Software Requirements Specifications), design output documents (i.e. Software Design Descriptions, system build, configuration documents and code listings associated with the system) as well as Training and Maintenance Manuals.

PSAI 6.5 is addressed in Section 3.4.4.3, "Software Evaluation," and, based on that section, the NRC staff concludes that the licensee has appropriately addressed PSAI 6.5.

3.4.6.6 PSAI 6.6

PSAI 6.6 states that "When implementing a Common Q safety system (i.e. PAMS, CPCS, or DPPS), the licensee must review CENP's timing analysis and validation tests for that Common Q system in order to verify that it satisfies its plant specific requirements for accuracy and response time presented in the accident analysis in Chapter 15 of the [plant] safety analysis report."

The licensee responded as follows:

> The acceptable response times for the [PVNGS] CPCS are those given in the Updated Final Safety Analysis Report (UFSAR), Table 7.2-4AA (Reactor Protective Instrumentation Response Times), for the Local Power Density – High (I.A.8) and DNBR – Low (I.A.9). These are the response times used in the accident analyses in Chapter 15 of the UFSAR. Westinghouse (CENP) will perform a plant-specific analysis of the program timing (CPCS Timing Analysis). In addition, response time testing will be performed as part of the CPCS Factory Acceptance Test (FAT) on each system to be installed at Palo Verde. APS will review Westinghouse test results to ensure plant specific requirements for accuracy and response time as presented in the accident analysis in Chapter 15 of the PVNGS safety analysis report have been met.

PSAI 6.6 is addressed in Section 3.4.4.3, "Software Evaluation," and based on that section, the NRC staff concludes that the licensee has appropriately addressed PSAI 6.6.

3.4.6.7 PSAI 6.7

PSAI 6.7 states that, "The OM and the MTP provide the human machine interface for the Common Q platform. Both the OM and MTP will include display and diagnostic capabilities unavailable in the existing analog safety systems. The Common Q design provides means for access control to software and hardware such as key switch control, control to software media, and door key locks. The human factors considerations for specific applications of the Common Q platform will be evaluated on a plant-specific basis.

The NRC staff reviewed the method to access and control the CPCS software, safety-related algorithms and addressable constants. Software can be downloaded only through accessible

auxiliary protective cabinets that can be locked. The MTP uses a key to energize the hardware used to download new software. The OM or MTP can be used to change addressable constants, but has keylock controls. Furthermore, the licensee has established procedures to maintain the configuration of the CPCS software. The NRC staff reviewed this during its visit to the PVNGS. The NRC staff finds that the Common Q system maintains access control of the CPCS software media and hardware. Additionally, the licensee will institute configuration management similar to the legacy system. One notable change involves using the Westinghouse, NRC-approved SPM to make software changes, which is discussed in Section 3.4.7, "Evaluation of Proposed Technical Specification Changes." Human factors issues are addressed in Section 3.2, "Human Factors Considerations," and the NRC staff concludes that the licensee has acceptably addressed the human factors aspects of the CPCS. Based on this, the NRC staff considers that the licensee has appropriately addressed PSAI 6.7.

3.4.6.8 PSAI 6.8

PSAI 6.8 states that "If the licensee installs a Common Q PAMS, CPCS or DPPS, the licensee must verify on a plant-specific basis that the new system provides the same functionality as the system that is being replaced, and meets the functionality requirement applicable to those systems."

The licensee responded as follows:

> As part of the normal design change process at Palo Verde the suitability of all new systems is assessed. This review covers the overall function of the system, as well as the design and licensing basis of the system. The Purchase Specifications for the CPC/CEAC System Replacement details the conditions of service and general requirements that must be met in the Common Q CPCS. These specifications detail the necessary performance requirements to assure functionality is maintained with the new system. Enhancements to the CPCS are occurring as part of the Common Q design evaluation process for Palo Verde. In every case, performance requirement factors are being taken into account to ensure that the new CPCS will provide the same functionality as the CPCS being replaced.

The NRC staff conducted a software audit to ensure that the functionality requirements of the old legacy system were the same as the Common Q system to be installed. This is addressed in Section 3.4.4.3, "Software Evaluation," and, based on that section, the NRC staff confirmed that the licensee has appropriately addressed PSAI 6.8, in that the new CPCS has the functionality requirements of the legacy system.

3.4.6.9 PSAI 6.9

PSAI 6.9 states that "Modifications to plant procedures and/or TS due to the installation of a Common Q safety system will be reviewed by the NRC staff on a plant-specific basis. Each licensee installing a Common Q safety system shall submit its plant-specific request for license amendment with attendant justification."

The licensee responded as follows:

> As part of the normal design change process at Palo Verde, the impact to plant procedures and TS is evaluated for all design changes. Plant procedures have been preliminarily reviewed and changes identified. All procedure changes will be evaluated in accordance with 10 CFR 50.59 requirements prior to implementation. This license amendment request outlines the impact to the PVNGS TS and Bases that support implementation of the Common Q digital CPCS provided by Westinghouse. Justification for changes to the TS are included in this amendment request.

The licensee submitted TS changes and attendant justification as part of its application which is covered in Sections 3.1, "Proposed Technical Specification Changes," and 3.4.7, "Evaluation of Proposed Technical Specification Changes."

The NRC staff requested addition information regarding modifications to plant procedures as a result of installing the Common Q CPCS. In its RAI response, the licensee provided a table of the procedures that will change as a result of the CPCS upgrade. This table included the procedure number, the title and a brief description of the procedure change. The procedures that will change include maintenance and normal operating procedures. No emergency operating procedures will change as a result of the CPCS upgrade.

The licensee also stated that many of these procedures were still being revised and that this would continue into the shutdown of Unit 2 for the upcoming refueling outage and installation of the new CPCS. The NRC staff interviewed licensee personnel to discuss the procedures that will be changing, especially the changes to the functional test procedure. The functional test procedure is required by the TSs to be performed under certain conditions. This procedure will change as a result of the new Common Q system. As such, the NRC staff requested additional information regarding the change to the functional test procedure. In an RAI response, the licensee outlined the changes that will occur. The NRC staff reviewed this response and finds that the changes to the functional test procedure are reasonable, and reflect the new Common Q CPCS. While the plant procedure modifications have not been completed, the NRC staff did review the licensee's governing procedures and interviewed personnel regarding these modifications. Based on these reviews, the NRC staff finds that the licensee has an established methodology for the identification and modification of the plant procedures that are affected by the Common Q system.

Based on the above, the NRC staff considers that the licensee has appropriately addressed PSAI 6.9.

3.4.6.10 PSAI 6.10

PSAI 6.10 states that "A licensee implementing any Common Q applications (i.e., PAMS, CPCS, or DPPS) must prepare its plant specific model for the design to be implemented and perform the FMEA for that application."

The licensee responded as follows:

> A plant specific FMEA for the Palo Verde CPCS, similar to one in the Westinghouse Common Q CPC topical report, has been prepared. The results will be summarized in the Failure Modes and Effects Analysis, Table 7.2-4A, of the Palo Verde UFSAR in accordance with the requirements of 10 CFR 50.71(e). In general there have been no

changes in the way that the CPC and CEAC respond to input failures. This FMEA confirms that no single failure associated with the replacement CPCS will defeat more than one of the four protective channels, assuring proper protective action at the system level.

The NRC staff reviewed the plant-specific FMEA for the Common Q design and found that it focused on component and field device failures, but did not address software failures. However, Westinghouse performed a software safety analysis which was reviewed by the NRC staff. This is covered in Section 3.4.4.2.6, "Software Safety Analysis." Based on its review, the NRC staff agrees that no single failure associated with the replacement CPCS will defeat more than one of the four protective channels, and that the upgraded CPC and CEAC will respond similarly to input failures in a manner similar to the legacy system. Furthermore, the review of the CPCS FMEA confirms that a component single failure of the Common Q system not prevent the CPCS from performing its safety function. Based on this, the NRC staff considers that the licensee has appropriately addressed PSAI 6.10.

3.4.6.11 PSAI 6.11

PSAI 6.11 states that "If a licensee installs Common Q PAMS, CPCS, DPPS or Integrated Solution, the licensee shall demonstrate that the plant-specific Common Q application complies with the criteria for defense against common-mode failure in digital instrumentation and control system and meets the requirements of HICB-19."

The licensee's response to PSAI 6.11 (defense-in-depth and diversity):

The replacement CPCS is the first application of Common Q hardware at Palo Verde. There are no plans at this time to replace any of the non-safety plant control systems with Asea Brown Boveri (ABB) computer technology. Therefore, there is no potential to reduce the diversity or defense in depth of the Palo Verde systems related to Common Q. In Supplement 1 to the Safety Evaluation Report issued to ANO-2 (NUREG 0308), the first plant with digital CPCs, the diversity of the Core Protection Calculators was evaluated, and found to be acceptable. ANO-2 SER Appendix D, Supplement 1, “Design Basis” states the following:

"Because the core protection calculator system (CPCS) is a first of a kind design, the [NRC] staff considered failure of the CPCS to perform its normal function. Backup trips and normal shutdown mechanisms were reviewed to assess the depth of protection provided. The extent of this review is beyond that normally performed for reactor protection systems. The CPCS provides the initial, but not the only trip, for the steam line break accidents, reactor coolant pump shaft seizure and steam generator tube rupture. Increased fuel damage could occur for the above accidents with concurrent failure of the CPCS. However, analog backup trips on system pressure…are available to provide reactor shutdown and mitigate the consequences of accidents. Failure of the CPCS, concurrent with any of the above incidents, is an extremely unlikely event. Backup trips are available to limit the consequences of each of the above events, even with failure of the CPCS, except the CEA misoperation event." The CPCS provides a reactor trip for CEA deviation events where DNBR or peak linear heat rate limits are approached. Automatic reactor trips have not been provided in previous Combustion Engineering protection system designs for this event. In the unlikely event that a CEA deviation event

which required a reactor trip occurred without a CPC initiated trip, the operator would get alarms from the core operating limit supervisory system (COLSS) on CEA position and flux tilt similar to that in non-CPCS plants. Manual trip could then be initiated. The [NRC] staff has considered failure of the digital trip system to perform its design function. Backup analog trips and/or inherent shutdown mechanisms limit the consequences of this type of failure for all but the CEA misoperation events. For CEA misoperation, a manual trip, similar to previous plants, is required but numerous alarms and indications are available to inform the operator of the event. We find the backup to the CPCS to be acceptable.

Diversity issues associated with replacement of the CPC channels with a common qualified platform-based system are acceptable based upon the following:

- Palo Verde possesses an almost identical backup set of hardware implemented RPS trip functions as ANO-2.

- Palo Verde RPS trips are identical with the exception that Palo Verde also has Low Flow RPS trip based on Steam Generator primary side differential pressure. This trip is used to provide sheared [RCP] shaft event protection, but would serve as a backup for any loss of flow event, including a seized RCP shaft.

- Replacement of the [existing] four CPC channel hardware with a common qualified platform presents a digital to digital upgrade of the Palo Verde CPC system. Licensing of this system addressed diversity issues by assuming a common cause failure of all four CPC channels. As noted in the Safety Evaluation Report issued to ANO-2 on the CPC channels, the NRC found the backup analog trips, inherent shutdown mechanisms, and provisions for manual operator action acceptable.

The licensee's response to PSAI 6.11 (CPCS evaluation):

The replacement CPCS is the first application of Common Q hardware at Palo Verde. The original ESFAS system has not been upgraded from its original equipment (it has some 1970’s vintage digital components that are limited to discrete logic gates and related elements, but it is not a Common Q based system). The ESFAS does not employ digital computers or software. Therefore, the failure case involving a common mode failure of all CPCS channels is not changed. The Palo Verde specific FMEA will be very similar to the generic FMEA proposed by Westinghouse for this area.

The NRC staff reviewed these responses, the UFSAR ,and the SER (NUREG-0308, dated November 1977, that licensed Arkansas Nuclear One, Unit 2, and Supplement 1 to the NUREG dated March 1978) that the licensee references in its application. The NRC staff noted that there are CPCS backup trips that are safety-related. Hence the licensee's response that “There are no plans at this time to replace any of the non-safety plant control systems with Asea Brown Boveri (ABB) computer technology” is not sufficient. In an RAI response, the licensee clarified the previous statement by stating that “There are no plans at this time to replace any other 'safety' or non-safety plant control systems with similar computer technology."

The NRC staff interviewed Licensee personnel and reviewed the procedures for a CEA misoperation event. In an RAI response, the licensee states that "The response time for operator action during a CEA misoperation event (Single Full-Length CEA Drop Event) is 900 seconds (15 minutes) as stated in Section 15.4.3 of the PVNGS UFSAR. Only the CEA insertion event is considered for CEA misoperation since a CEA withdrawal event is backed up by a high pressurizer pressure trip whereas a CEA insertion event has no backup automatic trip." The NRC staff noted that NUREG-0308 postulated only a failure of the CPCS to perform its function and concluded that backup trips were available for all reactor trips the CPCS is designed to initiate, except for the CEA misoperation. However, the SER found the alarms available for this event and the subsequent manual action to be acceptable. In an RAI, the licensee stated that, "The backup alarm and indications to warn operators of a CEA misoperation event (CEA insertion) are still available and will not be changed upon implementation of the Common Q CPCS." Based on the statements made by the licensee, the NRC stall concludes that the defense in depth and diversity analysis that the legacy system was designed under, and has previously been found to be acceptable, will not change due to the use of the Common Q system. Therefore, the NRC staff finds that the licensee has appropriately addressed PSAI 6.11.

3.4.6.12 PSAI 6.12

PSAI 6.12 states that "A licensee implementing a Common Q DPPS shall define a formal methodology for overall response time testing."

The licensee responded as follows:

> This plant specific action item is not applicable since Palo Verde is not proposing implementing a Common Q Digital Plant Protection System (DPPS) at this time.

Because the licensee is not proposing to implement a Common Q DPPS, the NRC staff agrees that this PSAI is not applicable to the proposed installation of the Common Q CPCS in the licensee's application. Based on this, the NRC staff finds that the licensee has appropriately addressed PSAI 6.12.

3.4.6.13 PSAI 6.13

PSAI 6.13 states that an applicant shall perform an "analysis of the capacity of the shared resources to accommodate the load increase due to sharing."

The licensee has responded as follows:

> The shared resource issue relates to multiple Common Q based systems (e.g., both CPC and PAMS) using the same resources (such as the AF100 bus or an Operator Module). The replacement CPCS is the first application of Common Q hardware at Palo Verde. Therefore this issue is not applicable at this time. Any future plant changes involving Common Q (such as PPS, ESFAS, RPS or PAMS) will require this analysis for the resources that would actually be shared.

Because the licensee, in its application, is only proposing use of the Common Q CPCS and has no current plans to upgrade other safety systems at PVNGS to the Common Q platform, the NRC staff finds that the licensee has appropriately addressed PSAI 6.13.

3.4.6.14 PSAI 6.14

PSAI 6.14 states that "The licensee must ascertain that the implementation of the Common Q does not render invalid any of the previously accomplished TMI action items."

The licensee has responded as follows:

> TMI action items from 50.34(f)(2) that are relevant to the PVNGS implementation of a new CPCS are as follows:
>
> - 50.34(f)(2)(i) - Provide simulator capability that correctly models the control room and includes the capability to simulate small-break LOCA's.
>
> - 50.34(f)(2)(iii) - Provide, for Commission review, a control room design that reflects state-of-the-art human factor principles prior to committing to fabrication or revision of fabricated control room panels and layouts. In regards to the Simulators used to train PVNGS Licensed Operators, each simulator is designed to correctly model the Unit Control Rooms (with some minor differences to accommodate unit differences) including the capability to simulate small-break LOCAs. As required by plant procedure, APS will be purchasing CPC systems for each of the two simulators that will correctly model the CPC version being placed in each of the Unit control rooms.
>
> In regards to the Simulators used to train PVNGS Licensed Operators, each simulator is designed to correctly model the Unit Control Rooms (with some minor differences to accommodate unit differences) including the capability to simulate small-break LOCAs. As required by plant procedure, APS will be purchasing CPC systems for each of the two simulators that will correctly model the CPC version being placed in each of the Unit control rooms.
>
> In regards to Human Factors, and as stated before, the CPC Replacement Project, as required by plant procedures, will receive a Human Factors (HF) Review in accordance with applicable NUREG 0700, Human-System Interface Design Review Guideline, criteria prior to the system being placed in service and made operable. The HF Review will focus on design features and characteristics of the new CPC system to ensure that the system incorporates acceptable human factors engineering principles and that the system provides the necessary system information, control capabilities, feedback, and analytical aids necessary for control room operators to accomplish their functions effectively.
>
> Therefore, the CPCS implementation at PVNGS does not render invalid any of the previously accomplished TMI action items.
>
> Likewise, the new CPCS will not render invalid any other of the plant's previously accomplished protection or safety functions. The CPCS design function will remain the same as the one existing. The Common Q CPCS will continue to provide Reactor

Protection System (RPS) trips on Low Departure from Nucleate Boiling Ratio (DNBR) and High Local Power Density (LPD) in response to calculations involving several input variables. It will also continue to provide a Control Element Assembly Withdrawal Prohibit (CWP) signal to the Plant Protection System (PPS). The CPCS does not directly interface with any other protection or safety function.

The NRC staff noted that the licensee did not mention TMI Action item 10 CFR 50.34(f)(2)(v) that states "Provide for automatic indication of the bypassed and operable status of safety systems." This item is applicable by the SRP in reviewing reactor protection systems, and the CPCS is part of these systems. The NRC staff reviewed and found that the legacy system to Common Q system requirements and functionality contained essentially no differences, as stated in Section 3.4.4.3.4 of this safety evaluation. The NRC staff also reviewed in detail the method of bypassing CPCS channels and its effect on RPS and finds that CPCS channel bypasses are clearly indicated to plant personnel and only permitted by the RPS when reactor power is less than 10^{-4} percent power. Furthermore, only one channel can be placed in test at a time. Based on these conclusions, the NRC staff finds that the Common Q CPCS implementation meets 10 CFR 50.34(f)(2)(v).

Based on the above statements by the licensee regarding the plant simulators for the Common Q CPCS, the staff finds that the implementation of the Common Q CPCS meets 10 CFR 50.34(f)(2)(i).

The NRC staff reviewed 50.34(f)(2)(iii). This is addressed in the human factors review of the proposed CPC upgrade in Section 3.2 on human factors considerations. Because the NRC staff concludes in Section 3.2 that the licensee has acceptably satisfied the human performance requirements, the NRC staff also concludes that 50.34(f)(2)(iii) has been appropriately addressed.

Therefore, based on the above, the NRC staff finds that the licensee has appropriately addressed PSAI 6.14.

3.4.6.15 Conclusion

Based on the discussion above on the 14 PSAIs from the August 11, 2000, SER, the NRC staff concludes that the licensee has appropriately addressed all of the PSAIs in the Common Q NRC SER issued August 11, 2000.

3.5 Evaluation of Proposed Technical Specification Changes

The NRC staff reviewed the submittals which addressed the licensee's proposed changes to the TSs, which are described in Section 3.1 of this safety evaluation. The proposed changes are to TSs 3.2.4 on the DNBR, 3.3.1 on RPS instrumentation, 3.3.3 on the CEACs, and 5.4.1.f on procedures. The proposed changes were proposed in the licensee's letters of November 7, 2002, and July 30, 2003. The licensee committed to relocate the requirements in TS LCO 3.3.1 Condition E and LCO 3.3.3 Condition C from the TSs to the PVNGS Technical Requirements Manual (TRM) in its letter of August 13, 2003.

The licensee proposed to have two sets of TSs 3.2.4, 3.3.1, 3.3.3, and 5.4.1.f in the PVNGS TSs. One set would be labeled "Before CPC Upgrade" and one set, "After CPC Upgrade." This is because not all the units will have the new Common Q CPCS installed at the same time. The replacement CPCS for each unit will be installed in refueling outages for the three units over at least a year, starting with the Unit 2 fall 2003 outage, and continuing into 2004 for Units 1 and 3. The TSs labeled "Before CPC Upgrade" have no further changes because the current TSs are the approved TSs for the current CPCS. The staff has considered the licensee's proposal to have the two sets of TSs and agrees that until the new Common Q CPCS is installed in all three units, there must be two sets of CPCS TSs. One set for the old legacy CPCS and one for the new Common Q CPCS. Because the licensee has proposed a set of TSs for the old CPCS that contains the current approved requirements for the old system and a new set of TSs for the requirements on the new Common Q system, the NRC staff concludes that the proposed current TSs for the old CPCS with the phrase "Before CPCS Upgrade" to account for the old system in Units 1 and 3, before the new system is installed, is acceptable.

The proposed TS changes for "After CPC Upgrade" are addressed below:

3.5.1 Changes to TS 3.2.4

As discussed in Section 3.4.2.1 of this safety evaluation, there are now eight CEACs (two for each of the four CPC channels) in the new Common Q CPCS instead of only two CEACs in the existing legacy system. Because of this, the licensee has proposed changes to TS 3.2.4 to maintain the same intent of TS 3.2.4 for the new system. In the existing CPCS, one inoperable CEAC would result in all four CPC channels receiving input from the only one operable CEAC. Now, for one inoperable CEAC, each of three CPC channels would be receiving input from two operable CEACs and the one CPC channel with the inoperable CEAC would still be receiving from the one operable CEAC of the two CEACs for that CPC channel. This difference must be accounted for in TS 3.2.4.

LCO Requirements

LCO 3.2.4 provides four methods for maintaining the DNBR, and the licensee has not proposed to change the statement that "The DNBR shall be maintained by one of the following methods." Of the four methods in the LCO 3.2.4, two were for the COLSS in service and two were for the COLSS out of service. The proposed changes have nothing to do with the DNBR limits or the design of the COLSS.

The licensee is not revising the requirements in each method of either (1) maintaining the COLSS calculated core power less than or equal to COLSS calculated core power operating limit based on DNBR, (2) maintaining the COLSS calculated core power less than or equal to COLSS calculated core power operating limit based on DNBR decreased by the allowance specified in the core operating limit report (COLR), or (3) operating within the region of acceptable operation specified in the COLR using any operable CPC channel. The licensee, however, has proposed to revise the parenthetical statement for each of the four methods that specifies whether the COLSS is in or out of service and how many of the two CEACs in a CPC channel are operable. Because there will be eight CEACs (2 CEACs for each of the four CPC channels) in the new Common Q CPCS compared to only two CEACs in the existing CPCS, the parenthetical statement on CEACs being operable for each method has to be revised.

The licensee has first proposed to reformat the methods to list them under one of the following two headings: (a) COLSS in service or (b) COLSS out of service. Therefore, the reference to COLSS being either in service or out of service would be placed in the headings instead of the parenthetical statement in the current TSs. Because this change has no effect on the requirements specified in the four existing approved methods and is merely administrative, the NRC staff concludes that this proposed change is acceptable.

When the COLSS is in service and one or both CEACs are operable, the parenthetical statement on the CEACs, for the first method in the current LCO 3.2.4, is being changed from "when ... either one or both Control Element Assembly Calculators (CEACs) are OPERABLE" to "when at least one Control Element Assembly Calculator (CEAC) is OPERABLE in each OPERABLE Core Protection Calculator (CPC) channel." Because the change is consistent with the change in the CPCS from only two CEACs in the legacy system to two CEACs for each of the four CPC channels in the Common Q system, the NRC staff concludes that the proposed change is acceptable.

When the COLSS is in service and neither CEAC is operable, the parenthetical statement on the CEACs, for the second method in the current LCO 3.2.4, is being changed from "when ... neither CEAC is operable" to "when the CEAC requirements of LCO 3.2.4.a.1 are not met." The proposed change means that when the COLSS is in service and the previous method (i.e., the proposed method LCO 3.2.4.a.1) can not be used, this method shall be used. Therefore, for the COLSS in service, only the new methods LCO 3.2.4.a.1 or LCO 3.2.4.a.2 may be used to maintain the DNBR within acceptable limits. Because the change is consistent with the change in the CPCS from only two CEACs to two CEACs for each of four CPC channels, is consistent with the current LCO 3.2.4 where for the COLSS in service that only existing method LCO 3.2.4.a or 3.2.4.b may be used, and the two methods are not being changed, the NRC staff concludes that the proposed change is acceptable.

When the COLSS is out of service and either one or both CEACs are operable, the parenthetical statement on the CEACs, for the third method in the current LCO 3.2.4, is being changed from "when ... either one or both CEACs are OPERABLE" to "when at least one [CEAC] is OPERABLE in each OPERABLE CPC channel." Because the change is consistent with the change in the CPCS from only two CEACs to two CEACs for each of the four CPC channels, the NRC staff concludes that the proposed change is acceptable.

When the COLSS is out of service and neither CEAC is operable, the parenthetical statement on the CEACs, for the fourth method in the current LCO 3.2.4, is being changed from "when ... neither CEAC is operable" to "(with both CEACs inoperable) when the CEAC requirements of LCO 3.2.4.b.1 are not met." The proposed change means that when the COLSS is out of service and the previous method (i.e, the proposed method LCO 3.2.4.b.1) can not be used, this method shall be used and the operable CPC channel that would be chosen would have both CEACs inoperable.

The restriction in proposed LCO 3.2.4.b.2 that both CEACs are inoperable is necessary because the proposed LCO 3.3.3 (addressed below in Section 3.5.3 of this safety evaluation) has actions that do not require a CPC channel to be declared inoperable for an inoperable CEAC. Specifying that the operable channel must have both CEACs inoperable is having the licensee choose the most conservative operable CPC channel for determining the DNBR. If no operable CPC channel has both CEACs inoperable, then proposed method LCO 3.2.4.b.1 must

be chosen because that method states that "at least one CEAC is operable in each OPERABLE CPC channel." If there is not at least one operable CEAC in each operable CPC channel, then at least one operable channel has both CEACs inoperable.

Therefore, for the COLSS out of service, the licensee has proposed that the methods LCO 3.2.4.b.1 or 3.2.4.b.2 will be used to maintain the DNBR within acceptable limits. Because (1) the proposed change is consistent with the new CPCS having two CEACs for each of four CPC channels and (2) the proposed methods LCOs 3.2.4.b.1 and 3.2.4.b.2 are not being changed from the current methods LCOs 3.2.4.c and 3.2.4.d (for COLSS out of service), the NRC staff concludes that the proposed change is acceptable.

Based on the above evaluation, the NRC staff concludes that the proposed changes to LCO 3.2.4 are acceptable. The NRC staff also reviewed the remaining requirements in LCOs, Actions, and SRs in TS 3.2.4. Based on its review of the CPCS in Section 3.4.2 of this safety evaluation, it concludes that there were no other requirements in TS 3.2.4 that needed to be revised or added for the new Common Q CPCS.

3.5.2 Changes to TS 3.3.1

3.5.2.1 TS 3.3.1 Changes - LCO Actions

Condition E

The licensee proposed to delete Condition E from LCO 3.3.1. This includes the Required Action E.1 and the completion time. Condition E is the required action for one or more CPC channels with a high cabinet temperature alarm. The licensee provided the following justification for removing Condition E:

> In the presently installed CPCS, each CPC channel is equipped with two cabinet temperature switches that provide remote annunciation on high cabinet temperature conditions. In the replacement CPCS there are two cabinet temperature sensing RTDs per channel, each providing an analog temperature input measurement to different analog input modules. The cabinet temperature input allows for display of existing cabinet temperature on the Operator's Module (OM) and Maintenance Test Panel (MTP). The CPC processor monitors the RTDs and compares the temperature against a high temperature alarm setpoint and provides a digital output to the cabinet temperature high annunciator and a channel trouble alarm indication on the OM and MTP. The cabinet temperature alarm setpoint of 122 degrees F is well below the 140 degree F temperature to which the CPCS was subjected to during environmental testing.
>
> The replacement CPCS possesses extensive online diagnostics to continuously monitor and assess channel functionality. These diagnostics address numerous failure conditions from many causes, temperature stress being only one such cause. Failures will be flagged by pertinent error messages and a channel trouble alarm on the OM and MTP. The design also has provisions for remote annunciation on channel trouble. The nature of the failure can be diagnosed from these locations. Therefore, since channel functionality is continuously self-diagnosed, Condition E [One or more core protection calculator (CPC) channels with a cabinet high temperature alarm] and the Required

> Action [Perform CHANNEL FUNCTIONAL TEST on the affected CPC] are no longer required.

The NRC staff reviewed the channel functional test procedure currently used as a Required Action for Condition E and noted that part of the procedure tests components external to the CPCS, specifically the remaining part of the RPS. Furthermore, the NRC staff noted that the "extensive online diagnostics" will not test this portion of the RPS. Therefore the claim concerning the diagnosing of channel functionality is questionable and the NRC staff found the justification put forth in the licensee's application to be incomplete. However, the licensee provided an RAI response to the NRC staff's concern regarding removing condition E. In the visit to PVNGS, the NRC staff also discussed in detail the removal of Condition E from TS 3.3.1.

In its application, the licensee proposed to delete the LCOs 3.3.1 Condition E and 3.3.3 Condition C requirements from the TSs. In the RAI response dated August 13, 2003, for NRC Request A.10, the licensee provided the following justification for this change:

> These two LCO conditions do not meet all of the requirements of 10 CFR 50.36. APS acknowledges that the CPCS does in fact meet the four criteria of 10 CFR 50.36(c)(2)(ii) and should continue to have LCO requirements (as reflected in LCO 3.3.1 Conditions A, B, C, D and G[,] and LCO 3.3.3 Conditions A, B, and E).
>
> However, 10 CFR 50.36(c)(2)(i) states that LCOs are "*the lowest functional capability or performance levels of equipment required for safe operation of the facility*." APS believes that the requirements to perform a functional test on a CPC cabinet high temperature alarm, as stated in LCO 3.3.1 Condition E and LCO 3.3.3 Condition C, do not meet the definition for an LCO in 10 CFR 50.36(c)(2)(i). The following is [the] basis for this conclusion:
>
> a. A high CPC cabinet temperature alarm does not indicate the lowest functional capability or performance level of a CPC or CEAC. These alarms (122 deg F) are actuated well below the qualification temperature of the CPCs and CEACs (140 deg F) and merely inform the Operations staff of a potential challenge to CPC/CEAC operability. Typically only one of four channels is affected on high cabinet temperature since each cabinet has its own independent cooling system.
>
> b. These LCO requirements have no follow up requirements for continuous monitoring after the initial test to determine if functionality may be affected in the future with an existing high temperature condition. In contrast, the improved Common Q CPCS provides more extensive online diagnostics than the [old] legacy CPCS and will continuously monitor and assess CPC/CEAC module functionality. These diagnostics address numerous failure conditions from many causes, temperature stress being only one such cause. Failures are flagged by pertinent error messages and a channel trouble alarm on the Operators Module (OM), Maintenance Test Panel (MTP) and remote annunciation. The improved CPCS design provides greater confidence in identifying and alarming an actual loss of CPC/CEAC functionality.

The licensee also justified removing Condition E by stating that “A CPC high cabinet temperature alarm does not meet any of the four criteria of 10 CFR 50.36(c)(2)(ii)."

The basis for existing LCO 3.3.1, Condition E, is given on Page 3.3.1-29 of the TS Bases. The TS basis for Condition E agrees with what was stated above by the licensee. The NRC staff also reviewed the hardware temperature qualification of the Common Q shown in Section 3.4.6.4, "PSAI 6.4," which shows the temperature to which the Common Q was tested. The NRC staff also reviewed the criteria of 10 CFR 50.36(c)(2)(ii). Because the high CPC cabinet temperature alarm of Condition E does not relate to when the CPCS becomes inoperable, the NRC staff finds that Condition E does not meet the criteria of 50.36(c)(2)(ii) to be in the TSs and, thus, the licensee has provided sufficient justification for removing LCO 3.3.1 Condition E from the TSs and moving it to the TRM. Therefore, the NRC staff concludes that the proposed change is acceptable.

Condition F

The licensee proposed to delete Condition F from LCO 3.3.1. This includes the Required Action F.1 and the completion time. Condition F is the required action for one or more CPC channels with three or more auto restarts during a 12-hour period. The licensee provided the following justification for removing Condition F:

> In the presently installed CPCS, numerous failures result in an “auto restart” in which the CPC processor attempts to reinitialize and return to operation following a failure condition (e.g., floating point arithmetic fault, divided by zero, etc.). If the restart is successful due to a spurious failure condition, the CPC will resume normal (untripped) operation. The cause of the failure is logged at the CPC OM. It is possible for a marginally performing CPC channel processor to recover from repetitive failures. This Condition forces performance of a channel functional test if three or more such failure and restart conditions occur in a 12 hour period to assure the CPC is reliable.
>
> The replacement CPCS has no such auto restart capability. A processor failure will result in a HALT condition, in which the CPC processor remains in a tripped state, the watchdog timer times out, and maintenance personnel must perform a restart or repair of the affected module. Therefore, a marginally performing CPC processor cannot continue to remain in operation without deliberate action by the maintenance staff. Any repair will result in appropriate diagnostics being performed on the module to assure operability. Therefore, Condition F and the associated Required Action are no longer required.

The basis for existing LCO 3.3.1, Condition F, is given on Page 3.3.1-29 of the TS Bases. The TS basis for Condition F agrees with what was stated above by the licensee. The NRC staff reviewed this response and agrees with the licensee that the Common Q CPCS has no restart capability, and, therefore, Condition F is no longer applicable for the new CPCS. Based on this, the NRC staff concludes that Condition F may be deleted and the proposed change is acceptable.

3.5.2.2 TS 3.3.1 changes - Surveillance Requirements (SRs)

SR 3.3.1.3

The licensee proposed to revise SR 3.3.1.3 by replacing "autostart count" with "System Event Log." The proposed SR 3.3.1.3 would state the following: "Check the CPC System Event Log." The licensee provided the following justification for revising SR 3.3.1.3. The system event log allows operators to assess CPC channel status. The licensee provided the following justification for this change:

> Because of the numerous redundant features in a CPC channel, including redundant input modules and data links, most of these failures will not in themselves cause CPC channel inoperability. Failures which render the channel inoperable, such as loss of both redundant CPC analog input modules, will additionally cause a CPC fail lamp on the OM and MTP, and annunciation, accompanied by channel low DNBR and high LPD trip outputs. Failure rendering a CEAC inoperable, such as loss of both redundant CEA position inputs on four or more CEAs, will similarly result in a CEAC fail lamp on the OM and MTP, and CEAC fail annunciation, as well as a CEAC fail flag to the associated CPC processor. The CPC will respond to a CEAC failure in the same manner as the CPC in the existing system.
>
> This surveillance requirement forces personnel to periodically review the failure [or system event] log in order to ascertain channel performance, even if the individual failures do not render a channel inoperable. Failure to repair a faulty module could make the individual CPC susceptible to a single failure in the redundant module, in those cases when a redundant module exists. However, there is no requirement that all failures be addressed within a set time interval, unless they result in one of the other conditions (Fail/Sensor Fail) delineated above. The frequency of 12 hours reflects the nature of the surveillance, in which those failures that result in channel inoperability will independently cause a CPC fail condition, and CPC processor failure will result in a CPC HALT. Therefore, this surveillance requirement is of primary use in detecting failure of redundant features that may not be required for the CPC to perform its safety-related function.

Because the Common Q CPCS does not have an auto restart feature, but does have a system event log, which allows operators to assess channel status, the NRC staff finds that the proposed SR 3.3.1.3 change is acceptable. However, the NRC staff would point out that the SRs for CPC channel operability are the channel check in SR 3.3.1.1 and the channel functional test in SR 3.3.1.7.

3.5.2.3 Remaining Requirements in TS 3.3.1

The NRC staff reviewed the remaining requirements in LCOs, Actions, and SRs in TS 3.3.1. Based on its review of the CPCS in Section 3.4.2 of this safety evaluation, it concludes that there were no other requirements in TS 3.3.1 that needed to be revised or added for the new Common Q CPCS.

3.5.3 Changes to TS 3.3.3

3.5.3.1 TS 3.3.3 Changes - LCO Requirements

TS 3.3.3 are on the CEACs for which, as explained in Section 3.4.1 of this safety evaluation, there are two CEACs in each CPC channel. Because of this, the licensee has proposed to add the phrase "in each CPC channel" such that LCO 3.3.3 would read "Two CEACs shall be operable in each CPC channel." Because there are two CEACs in each CPC channel, the proposed LCO 3.3.3 for the new Common Q CPCS accurately requires that all CEACs must be operable, which is the basis for the existing LCO 3.3.3 in the TS Bases for LCO 3.3.3. Based on this, the NRC staff concludes that the proposed revised LCO 3.3.3 for the new Common Q CPCS is acceptable.

3.5.3.2 TS 3.3.3 Changes - LCO Actions

Conditions A and B

The licensee proposed to (1) add the phrase "in one or more CPC channels" to Conditions A and B, and (2) add a new required action to Conditions A and B to "Declare the affected CPC channel(s) inoperable." If either Condition A or B were not met, the licensee would perform the new required action immediately or perform the existing required actions. The existing required actions would be renumbered to account for the proposed new Required Action A.1 and B.1. There are no changes to the wording of the existing renumbered required actions and no changes to the completion times.

For the current CPCS, Condition A is the action for one CEAC being inoperable and Condition B is, for the required action and associated completion time of Condition A not being met or both CEACs being inoperable. The licensee provided the following justification for changing Conditions A and B, and adding the new required actions:

> TS changes are required to reflect the incorporation of two CEACs in all four CPC channels, rather than the two CEACs shared among the four CPCs of the existing CPCS design. In the replacement design, it will be possible to have CEACs inoperable in one or two CPC channels but still have an operable CEAC function in the remaining channels. There will be no change to the cabling of CEA position inputs to the CPCS. That is, RSPT 1 field inputs for approximately one quarter of the CEAs (the channel A target CEAs) are cabled in to CPC channel A. The remaining three-quarters of the RSPT 1 based CEA position inputs are cabled to CPC channel B. Similarly, approximately three quarters of the RSPT 2 CEA positions are cabled to CPC channel C, and the remaining one quarter of the RSPT 2 based CEA position inputs are cabled to CPC channel D.
>
> In the existing CPCS, CEAC 1 is mounted in CPC channel B, and CEAC 2 is mounted in CPC channel C. Thus, CEAC 1 directly receives three quarters of its CEA position inputs from RSPT 1 directly from channel B, and the remaining one quarter of the RSPT 1 inputs from the channel A CEA Position Isolation Amplifier (CPIA) via an analog isolator. Similarly, CEAC 2 is located in channel C, where it receives three quarters of the RSPT 2 based inputs directly, and the remaining one quarter of the RSPT 2 based position inputs from channel D via a CPIA mounted in channel D. CEAC 1 monitors the position of all CEAs based upon RSPT 1 CEA position input, and CEAC 2 performs an identical

function based upon RSPT 2. CEAC penalty factor outputs in the existing system are transmitted to all four CPC channels over one-way isolated data links. Thus, the CPCs in all four channels receive penalty factor inputs from both CEACs.

In the replacement system, the CEA position inputs will undergo analog to digital conversion in the channel of origin, by means of redundant CEA position processors (CPPs 1 and 2) in each CPC channel. Converted CEA position is then transmitted to all four channels, where a CEAC 1 and CEAC 2 processor reside. Since CPPs are redundant in each channel, a single CPP failure will not result in a loss of the CEA position transmission to the associated CEAC in the four CPC channels. However, it will still be possible for individual RSPT failures, which provide input to the both CPPs within a channel, to cause loss of a CEAC in multiple CPC channels.

Functionally, each CPC continues to receive penalty factors from two CEACs. However, failures in a single CEAC processor will only affect the CPC in the channel in which it resides. The proposed TS reflects this design. CEAC failures in one or two CPC channels may be treated as any other CPC channel failure as defined in existing LCO 3.3.1. Required Actions A.1 and B.1 of LCO 3.3.3 provide the option of declaring the affected CPC channel inoperable immediately. In the event of a single channel CEAC failure, this may be the preferred action, since the existing required actions for single channel inoperability in LCO 3.3.3 are based upon loss of the CEAC functions in all channels, which, in the new implementation, would not be the case.

As discussed in Sections 3.4.4.2 of this safety evaluation, the NRC staff reviewed in detail the hardware configuration of the CPCS including the functionality and location of the CEAC processors. The NRC staff also reviewed the communication between RSPTs and CEACs, and the method that CEA positions are sent to each of the other channels. To reflect the design change that there are two CEACs in each CPC channel, as discussed above, Conditions A and B need to be changed. Based on the justification provided by the licensee and the NRC staff review of the new Common Q CPCS, the NRC staff concludes that the proposed changes to Conditions A and B, including the new required actions and completion time, reflect the new CPCS. Based on this, the NRC staff concludes that the proposed changes are acceptable. The completion time of immediately (as defined in the TSs) to declare the affected CPC channel(s) inoperable is consistent with similar required actions in the TSs. The operators will have the option to declare the CEAC inoperable which would result in the CPC channel being inoperable, which is covered in TS 3.3.1.

Conditions C and D

The licensee has proposed to delete Conditions C and D, including the required actions and completion times, from the TSs. Condition C is for receipt of a CPC channel B or C cabinet high temperature alarm and Condition D is for three or more auto restarts during a 12 hour period.

For Condition C, the deletion of the action for a CPC cabinet high temperature alarm is addressed in Section 3.5.2.1 of this safety evaluation for the proposed deletion of Condition E of TS 3.3.1. For the same basis, the NRC staff concludes that the proposed deletion of Condition C, and its required action and completion time, is acceptable.

For Condition D, the deletion of the action for three or more auto restarts during a 12-hour period is addressed in Section 3.5.2.1 of this safety evaluation for the proposed deletion of Condition F of TS 3.3.1. For the same basis, the NRC staff concludes that the proposed deletion of Condition D, and its required action and completion time, is acceptable.

The licensee has also proposed to renumber Condition E to Condition C. This includes the required action for Condition E. Because, with the deletion of Conditions C and D, the remaining conditions for LCO 3.3.3 have to be renumbered, the NRC staff concludes that the proposed change is acceptable.

Therefore, based on the above discussion, the NRC staff finds that the proposed changes to LCO 3.3.3 Conditions A through D are acceptable. The NRC staff also notes that, similarly as for LCO 3.3.1 Condition E, the licensee has provided sufficient justification for moving TS LCO 3.3.3 Condition C to the TRM.

3.5.3.3 TS 3.3.3 Changes - SRs

The licensee has proposed to revise SR 3.3.3.2 to state "Deleted" and to delete SR 3.3.3.6. The effect of stating "deleted" in SR 3.3.3.2 is to delete the requirement to "Check the CEAC auto restart count" without having to renumber existing SRs 3.3.3.3 through 3.3.3.5. The deletion of SR 3.3.3.6 is to delete the requirement to "Verify the isolation characteristics of each CEAC isolation amplifier" and to delete the reference to SR 3.3.3.6 being removed from the TSs.

The proposed deletion of SR 3.3.3.2 is addressed in Section 3.5.2.2 of this safety evaluation. Because the Common Q CPCS does not have the auto restart count, the NRC concludes that a SR to check the CEAC auto restart count is unnecessary. Based on this, the NRC staff concludes that the proposed revision of SR 3.3.3.2 to state "Deleted" is acceptable. By stating "Deleted," SRs 3.3.3.3 through 3.3.3.5 do not have to renumbered. The reference to SR 3.3.3.2 will remain in the TSs, but there will be no surveillance requirement to perform.

The licensee also proposed to delete SR 3.3.3.6. Because the Common Q CPCS, as described in Section 3.4.1 of this safety evaluation, does not have these isolation amplifiers, the NRC staff concludes that SR 3.3.3.6 is unnecessary. Based on this, the NRC staff finds that removing this requirement is acceptable.

3.5.3.4 Remaining Requirements in TS 3.3.3

The NRC staff reviewed the remaining requirements in LCOs, Actions, and SRs in TS 3.3.3. Based on its review of the CPCS in Section 3.4.2 of this safety evaluation, it concluded that there were no other requirements in TS 3.3.3 that needed to be revised or added for the new Common Q CPCS.

3.5.4 Changes to TS 5.4.1(f), Administrative Controls

The licensee proposes to change TS 5.4.1(f) by replacing the reference to CEN-39(A)-P, "CPC Protection Algorithm Software Change Procedure," with a reference to CE-CES-195, "Software Program Manual for Common Q Systems." The change is to the paragraph that states that "Modifications to the CPC software ... shall be performed in accordance with the most recent

version of the [referenced document] which has been determined to be applicable to the facility." TS 5.4.1(f) is requiring that the licensee make modifications to the CPC software using an approved document.

The licensee's proposed change to TS 5.4.1(f) would change the procedure used to make modifications to CPC software. The licensee proposes that the SPM be used for the Common Q CPCS instead of CEN-39(A)-P which is the document for the existing legacy CPCS. The SPM (CE-CES-195) was developed by Westinghouse for modifying the Common Q CPCS software, as discussed in Sections 3.4.4.1 and 3.4.4.3.1 of this safety evaluation, and should be the required document listed in TS 5.4.1(f) for such modifications. Because the SPM is the document to control modifications of the Common Q CPCS software, the NRC staff concludes that the proposed change to 5.4.1(f) is acceptable.

3.5.5 Conclusion

Based on the human factors, reactor systems, and electrical and instrumentation and controls reviews, which are discussed in the NRC staff's evaluation of the individual proposed changes to the TSs, the NRC staff concludes that the proposed amendments to revise TSs 3.2.4, 3.3.1, 3.3.3, and 5.4.1(f) to account for the new Common Q CPCS are acceptable.

3.6 Regulatory Commitments

The licensee made two commitments to the NRC in its application and supplemental letters listed in Section 1.0 of this safety evaluation.

In Attachment 3 of the application, the licensee provided the following regulatory commitment:

> APS will ensure that all plant specific action items described in section 6.0 of NRC Safety Evaluation (SE), Acceptance for Referencing of Topical Report CENPD-396-P, Rev. 01, “Common Qualified Platform” and Appendices 1, 2, 3 and 4, Rev. 01 (TAC No. MA1677), dated August 11, 2000, are completed.

As stated in Attachment 3, the completion date is "prior to implementation of the Common Q CPCS at PVNGS." This would be prior to the licencee's acceptance of the Common Q CPCS as an functional and operable system as described in its application and supplemental letters.

In its August 13, 2003, letter, the licensee also made the following commitment:

> APS will relocate the requirements of TS LCO 3.3.1 Condition E and LCO 3.3.3 Condition C from the TS to the PVNGS Technical Requirements Manual (TRM) prior to declaring the Common Q Core Protection Calculator System operable.

These commitments will be part of the licensee's Commitment Management System. Changes to these commitments would be reported to the NRC in accordance with Nuclear Energy Institute, "Guideline for Managing NRC Commitments," dated June 9, 1995, endorsed by the Commission, in which the NRC would be notified in writing of safety significant changes in these commitments before the change is made. Based on this, the NRC staff concludes that the commitments are acceptable and do not have to be made part of the license.

4.0 STATE CONSULTATION

In accordance with the Commission's regulations, the Arizona State official was notified of the proposed issuance of the amendment. The State official had no comments.

5.0 ENVIRONMENTAL CONSIDERATION

The amendments change a requirement with respect to installation or use of a facility component located within the restricted area as defined in 10 CFR Part 20, and change surveillance requirements. The NRC staff has determined that the amendments involve no significant increase in the amounts, and no significant change in the types, of any effluents that may be released offsite, and that there is no significant increase in individual or cumulative occupational radiation exposure. The Commission has previously issued a proposed finding that the amendments involve no significant hazards consideration, and there has been no public comment on such finding (68 FR 49527, published August 18, 2003). Accordingly, the amendments meet the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(9). Pursuant to 10 CFR 51.22(b) no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendments.

6.0 CONCLUSION

The Commission has concluded, based on the considerations discussed above, that: (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, (2) such activities will be conducted in compliance with the Commission's regulations, and (3) the issuance of the amendments will not be inimical to the common defense and security or to the health and safety of the public.

Principal Contributor: Richard Eckenrode
Mark Kowal
Chris Graham
Michael Waterman

Date: October 24, 2003

cc:

Mr. Steve Olea
Arizona Corporation Commission
1200 W. Washington Street
Phoenix, AZ 85007

Douglas Kent Porter
Senior Counsel
Southern California Edison Company
Law Department, Generation Resources
P.O. Box 800
Rosemead, CA 91770

Senior Resident Inspector
U.S. Nuclear Regulatory Commission
P. O. Box 40
Buckeye, AZ 85326

Regional Administrator, Region IV
U.S. Nuclear Regulatory Commission
Harris Tower & Pavillion
611 Ryan Plaza Drive, Suite 400
Arlington, TX 76011-8064

Chairman
Maricopa County Board of Supervisors
301 W. Jefferson, 10th Floor
Phoenix, AZ 85003

Mr. Aubrey V. Godwin, Director
Arizona Radiation Regulatory Agency
4814 South 40 Street
Phoenix, AZ 85040

Mr. Craig K. Seaman, Director
Regulatory Affairs/Nuclear Assurance
Palo Verde Nuclear Generating Station
P.O. Box 52034
Phoenix, AZ 85072-2034

Mr. Hector R. Puente
Vice President, Power Generation
El Paso Electric Company
2702 N. Third Street, Suite 3040
Phoenix, AZ 85004

Mr. John Taylor
Public Service Company of New Mexico
2401 Aztec NE, MS Z110
Albuquerque, NM 87107-4224

Ms. Cheryl Adams
Southern California Edison Company
5000 Pacific Coast Hwy Bldg DIN
San Clemente, CA 92672

Mr. Robert Henry
Salt River Project
6504 East Thomas Road
Scottsdale, AZ 85251

Terry Bassham, Esq.
General Counsel
El Paso Electric Company
123 W. Mills
El Paso, TX 79901

Mr. John Schumann
Los Angeles Department of Water & Power
Southern California Public Power Authority
P.O. Box 51111, Room 1255-C
Los Angeles, CA 90051-0100

Brian Almon
Public Utility Commission
William B. Travis Building
P. O. Box 13326
1701 North Congress Avenue
Austin, TX 78701-3326