September 8, 2003

LICENSEE: Arizona Public Service Company (APS)

FACILITIES: Palo Verde Nuclear Generating Station

SUBJECT: MEETINGS WITH REPRESENTATIVES OF ARIZONA PUBLIC SERVICE COMPANY FOR PALO VERDE NUCLEAR GENERATING STATION (TAC NOS. MB6726, MB6727, AND MB6728)

The Nuclear Regulatory Commission (NRC) staff conducted visits to (1) the licensee's contractor offices in Windsor, Connecticut, during the week of June 16-20, 2003, and (2) the licensee's plant site during the week of July 14-17, 2003. The visits were held as part of the NRC staff's review of a proposed license amendment request (LAR) for Palo Verde Nuclear Generating Station, Units 1, 2, and 3 (PVNGS).

Enclosure 1 is the list of attendees. Enclosures 2 and 3 are handouts from the NRC staff for the visit to Windsor, Connecticut and the PVNGS plant site, respectively.

BACKGROUND

The licensee submitted an application dated November 7, 2002, as supplemented by the letters dated April 25 and July 10, 2003, to change the Technical Specifications (TSs) to support an upgrade to the core protection calculator system (CPCS) to replace the current system due to parts obsolescence. The request was part of a LAR for PVNGS. The licensee stated that all CPC and control element assembly calculator (CEAC) systems are to be replaced with a functionally equivalent, digital Common Qualified (or Common-Q) CPC System provided by Westinghouse. The Westinghouse Common-Q CPC System design concept was approved by NRC in its Safety Evaluation (SE), "Acceptance for Referencing of Topical Report CENPD-386-P, Revision 01, 'Common Qualified Platform" and Appendices 1, 2, 3, and 4, Revision 01'," dated August 11, 2000, and the two SE supplements dated June 22, 2001 and February 24, 2003 (ADAMS ML003740165, ML011690170, and ML030550776, respectively).

The SE identifies 14 plant-specific action items that a licensee must address as part of a plant-specific request to use the platform in a safety-related application such as the CPC. Plant-specific action item (PSAI) 6.5 states in part that "The 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." Additionally, PSAI 6.8 states in part that, " ...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 staff's review of the APS application includes the review of these plant-specific bases.

A meeting was held to discuss the CPCS upgrade LAR application with the licensee on May 14, 2003. The meeting summary was issued on June 24, 2003.

As part of its review, the staff decided that it would visit the Westinghouse offices in Windsor, Connecticut (CT), and the plant site in Maricopa County, Arizona. Westinghouse is the CPCS application software developer and APS's contractor for the CPCS upgrade.

The following is a summary of the two trips.

WINDSOR, CT, TRIP SUMMARY

The staff audited the Westinghouse software system life-cycle activities applicable to the CPCS at the Windsor, CT, offices. The staff used the Westinghouse Software Program Manual (SPM) CE-CES-195, Revision 1 (ADAMS ML003721618) approved by NRC SE in August 11, 2000, as the primary document for the audit and was used to evaluate the software system life-cycle activities supporting the CPC development and design. The SPM applies to all software and firmware acquired or developed in-house for use in the Common Q system.

The staff reviewed the CPCS software to confirm the algorithms meet or exceed the legacy system timing and the timing requirements specified in the PVNGS Updated Final Safety Analysis Report (UFSAR). The staff interviewed the personnel responsible for specifying the software and system requirements, developing the software, testing the system, and providing verification and validation. The staff reviewed the following documents at the Westinghouse offices in Rockville, MD, and Windsor, CT, to confirm that Westinghouse appropriately applied the SPM to the CPCS development and that the timing requirements were met:

- 00000-ICE-3208, Rev. 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, Rev. 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.

  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, Rev. 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, Rev. 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 FDR.

- 00000-ICE-3233, Rev. 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, Rev. 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, Rev. 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, Rev. 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 nonsafety-related and staff review was limited to human factors and the effect of the CEAPDS on the safety-related CPCS.

- 00000-ICE-1279, Rev. 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, Rev. 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. The STATIC program computes static values of departure from nucleate boiling ratio (DNBR), hot channel quality, primary thermal power, and maximum hot leg temperature. This program also establishes the static values of the process variables that constitute the baseline conditions for the DNBR UPDATE program. STATIC is a safety-related program algorithm.

- 00000-ICE-30107, Rev. 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. The UPDATE program computes the updated values of DNBR, quality margin, and local power density based on temperature, pressure, core power, flow, and power distribution. UPDATE also computes neutron flux power, thermal power, hot pin axial shape index, hot pin heat flux, the one-pin integrated radial peaking factor, the asymmetric steam generator transient (ASGT) trip, and the variable overpower trip (VOPT). UPDATE is a safety-related algorithm.

- 00000-ICE-30108, Rev. 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 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*. The FLOW program computes a normalized flow rate in each leg of the primary coolant system and in the reactor core, and also calculates an adjusted value of DNBR based on the number of reactor coolant pumps (RCPs) running. The TRIPSEQ program will output trip signals when computed variables within the other safety related algorithms compute values that violate predetermined setpoints. TRIPSEQ will also output a trip if certain core conditions are outside the analyzed operating space or certain CPC malfunctions are detected. Such core conditions include less than two RCPs running, an ASGT, or a rapid rise in power.

- 00000-ICE-30106, Rev. 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. The POWER program computes average axial power distribution, pseudo hot pin axial power distribution, three dimensional power peaking factor, and an average of the hot channel power distribution.

- 00000-ICE-30129, Rev. 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. The CEAC penalty factor program calculates CEA deviation (difference in position) amongst the CEAs in each CEA subgroup, recognizes a single CEA withdrawal or insertion or multiple CEA deviations, calculates maximum local power density (LPD) and DNBR penalty factors based on the type, magnitude, subgroup, CEA configuration, and elapsed time, and recognizes the initiation of a reactor power cutback event. The CEAC penalty program sends values and status to the CPC processor algorithms as appropriate.

- 00000 - ICE - 37756, Rev. 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, Rev. 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

lifecycle. 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 lifecycle. 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, Rev. 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, Rev. 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, Rev. 01, *Unit Test Procedure for the Common Q Core Protection Calculator System*, Rev. 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, Rev. 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, Rev. 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 input/output (I/O) simulator was used to provide inputs and read/store output results. The test bed was the single channel facility (SCF) at Windsor, CT.

- 00000-ICE-37373, Rev. 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, Rev. 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, Rev. 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, Rev. 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 (HFAT) 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 staff performed several thread audits of the CPCS requirements given in the legacy documentation, 00000-ICE-3208 and 00000-ICE-3234. These requirements were traced through the software system life-cycle phases including, requirements development/translation, design description and coding, function chart generation, verification and validation (V&V) activities, software test phases, hardware and software integration, and factory acceptance testing.

One thread audit addressed the LPD function. The LPD control algorithm uses the hot leg temperature, the cold leg temperature, the pressurizer pressure, 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 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 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. The requirements were traced from the legacy documents using the RTM as a guide for tracing requirements. 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 platform. The staff also 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.

The staff also reviewed the general life-cycle activities that Westinghouse used in the specification and design of the CPCS using the SPM. The staff interviewed design and V&V personnel as part of these thread audits.

The staff provided clarifications and participated in several discussions regarding requests for additional information (RAI) questions, including CPCS channel availability and CPCS timing analysis.

Audit Findings and Conclusions

The 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 covered 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 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. To reduce the risk of new software/hardware hazards being designed into the new system, the 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 staff also reviewed the preliminary software safety documentation and determined that the exception taken to the SPM requirement is reasonable.

The staff used the RTM to aid in tracing requirements for the chosen thread audits. The staff observed several errors in the RTM. Westinghouse stated that the RTM was a draft document and that final review for corrections of the RTM had not taken place. While the RTM is indeed a draft and is not a controlling document in the life-cycle process, the staff pointed out that the RTM is the primary resource used by V&V and maintenance personnel to verify that software requirements are correctly translated. Furthermore, given the maturity of the CPCS project, the staff expected a more complete and correct RTM. Westinghouse stated that the RTM would be reviewed and corrected. The staff noted in the subsequent audit at PVNGS that the RTM had been reviewed by Westinghouse, but several inconsistencies identified during the Windsor, CT, audit had not been corrected. A more detailed discussion is provided in the discussion regarding the audit at PVNGS.

The staff noted a reliability value associated with a CPCS channel during a review of the CPCS SysRS. In a review of the reliability calculation, the staff noted the mixing of availability and reliability terminology. In discussions with Westinghouse personnel, it was determined that this value is an availability value, not a reliability one, and is taken from previously approved CEN-327. The staff reviewed the availability analysis and pointed out that additional information was needed to support the claim regarding diagnostics coverage to detect all but the CPCS digital output card failures and interposing relay failures. Furthermore, the staff will review the calculation regarding system diagnostics and their effect on the CPCS channel availability.

The staff finds that plant specific action item (PSAI) 6.5 and PSAI 6.8 in the SER approving the Common Q platform have been addressed acceptably for the PVNGS CPCS. The staff will provide further information regarding the conclusions derived from this audit in the SE for APS' application dated November 7, 2002, to change the TSs to support an upgrade to the core protection calculator system.

PVNGS SITE TRIP SUMMARY

The staff 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 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 APS and Westinghouse and resolution of various aspects of the CPCS design and installation.

- Notes and results of APS visits to Westinghouse in Pittsburgh, February 2003 - These notes describe the results of the APS visit to Westinghouse, and discusses system anomalies, test cases and status and human factors.

- 77ST-9SB07, CPC Channel A Functional Test, Revision 8, and 77ST-9SB12, CEAC 1, Revision 7. This is the technical specification channel functional test procedure for the existing CPCS.

The staff interviewed personnel involved in specifying the CPCS as well as those who performed engineering support and V&V evaluations. The staff reviewed the licensee's Specification 13-JN-1000 to evaluate the licensee efforts to verify conformance of the CPCS with the licensee's specifications. The staff also reviewed the licensee's V&V of the vendor design process. The reviews included evaluating the licensee's confirmatory efforts with respect to 13-JN-1000, Sections 5.0, 6.0, 7.0, and 9.0.

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 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,* discusses the environmental, seismic and EMI qualification that will be or has been accomplished for the new CPCS. 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 Appendix B of Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50. The staff reviewed licensee compliance with the licensee procedures used in the CPCS upgrade, particularly 80DP-0CC01 and 87DP-0CC08. The staff also observed the existing CPCS in the control room and in the licensee's test facility at PVNGS.

The staff finalized the list of RAIs and discussed all questions and outstanding items. The staff obtained the requested information, or obtained commitments from the licensee to provide the requested information as it became available during the CPCS development effort.

Audit Findings and Conclusions

The staff finds that APS has appropriately applied its plant standards, particularly 80DP-0CC01 and 87DP-0CC08, to the CPCS project. 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. Procurement specification 13-JN-1000 contains sufficient detail with regard to hardware, software, and interface requirements, environmental and electromagnetic interference qualification, and instrument uncertainty to satisfy the staff that adherence to the specification will meet regulatory requirements, and is consistent with the guidance in NRC regulatory guidelines and accepted industry standards. Furthermore, based on its review of the licensee's critical design reviews, V&V efforts, specification of additional test requirements, correction of legacy CPCS failures, design review visits to Westinghouse, and adherence to Specification13-JN-1000, the staff concludes that APS has been acceptably engaged in the CPCS design and development process.

The staff identified an issue with regard to the original APS license submittal concerning TS changes. APS proposes to remove a TS requirement to perform a functional test upon receipt of a CPCS high temperature alarm. APS provided justification in its submittal as follows:

> 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 [operators module] and MTP [Maintenance and Test Panel]. 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 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 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 staff finds the justification to be incomplete. APS stated that it will review alternative options with regard to this TS change including withdrawing the TS change request or submitting a modified TS change request.

The staff reviewed the RTM provided to APS by Westinghouse and found that some errors that the staff identified during its audit at Windsor, CT, had not been corrected. For example, in the column for the software implementation phase for several of the system requirements, the OCST continued to be referenced as the source document for the coding instead of the applicable code listing document. The performance of corrective, perfective, or adaptive maintenance on a software system requires that the personnel performing the maintenance be able to identify the specific coding modules requiring the maintenance. By not providing a reference to the software coding documents, Westinghouse or the licensee may not be able to reliably maintain the software if changes are required or desired in the future. Consequently, the staff recommended to the licensee that the RTM be corrected to provide the required traceability.

The staff finds that PSAI 6.1 and PSAI 6.4 in the SER approving the Common Q platform have been addressed acceptably for the PVNGS CPCS. The staff will provide further information regarding the conclusions derived from this audit and conclusions regarding all SER PSAIs and the licensee's CPCS license amendment in a forthcoming SER, with an expected delivery in September 2003.

The NRC staff did not accept any information for its review of the CPC upgrade LAR from the licensee because it did not want the two trips to be the means by which the additional information needed by the staff to complete its review of the LAR is submitted on the PVNGS docket. As part of the trip to the PVNGS site, the NRC staff did discuss what additional information and documentation needed to be submitted by APS.

The NRC staff completed its presentations and the site visits were adjourned.

/RA/

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

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

Enclosures:
1. List of Meeting Attendees
2. NRC Staff Handout for Week of June 16-20, 2003, Visit
3. NRC Staff Handout for Week of July 14-17, 2003, Visit
4. List of Acronyms

cc w/encls: See next page

online diagnostics" will not test this portion of the RPS. Therefore, the claim concerning the diagnosing of channel functionality is questionable and the staff finds the justification to be incomplete. APS stated that it will review alternative options with regard to this TS change including withdrawing the TS change request or submitting a modified TS change request.

The staff reviewed the RTM provided to APS by Westinghouse and found that some errors that the staff identified during its audit at Windsor, CT, had not been corrected. For example, in the column for the software implementation phase for several of the system requirements, the OCST continued to be referenced as the source document for the coding instead of the applicable code listing document. The performance of corrective, perfective, or adaptive maintenance on a software system requires that the personnel performing the maintenance be able to identify the specific coding modules requiring the maintenance. By not providing a reference to the software coding documents, Westinghouse or the licensee may not be able to reliably maintain the software if changes are required or desired in the future. Consequently, the staff recommended to the licensee that the RTM be corrected to provide the required traceability.

The staff finds that PSAI 6.1 and PSAI 6.4 in the SER approving the Common Q platform have been addressed acceptably for the PVNGS CPCS. The staff will provide further information regarding the conclusions derived from this audit and conclusions regarding all SER PSAIs and the licensee's CPCS license amendment in a forthcoming SER, with an expected delivery in September 2003.

The NRC staff did not accept any information for its review of the CPC upgrade LAR from the licensee because it did not want the two trips to be the means by which the additional information needed by the staff to complete its review of the LAR is submitted on the PVNGS docket. As part of the trip to the PVNGS site, the NRC staff did discuss what additional information and documentation needed to be submitted by APS.

The NRC staff completed its presentations and the site visits were adjourned.

/RA/

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

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

Enclosures:
1. List of Meeting Attendees
2. NRC Staff Handout for Week of June 16-20, 2003, Visit
3. NRC Staff Handout for Week of July 14-17, 2003, Visit
4. List of Acronyms

cc w/encls: See next page

DISTRIBUTION:

PUBLIC	PDIV-2 Reading	TMensah
RidsNrrDlpm (TMarsh/ELeeds)	RidsNrrDlpmLpdiv (HBerkow)	JClark, EDO
RidsNrrDlpmLpdiv-2 (SDembek)	RidsNrrPMJDonohew	RidsRgn4MailCenter (LSmith)
RidsNrrLAMMcAllister	RidsOgcRp	
CGraham (NRR/DE/EEIB)	MWaterman (NRR/DE/EEIB)	
EMarinos (NRR/DE/EEIB)	RidsAcrsAcnwMailCenter	***See Previous Concurrence**

ADAMS Accession No.: ML032521518 **NRC-001**

OFFICE	PDIV-2/PM	PDIV-1/LA	EEIB/SC	PDIV-S/SC
NAME	JDonohew	MMcAllister	EMarinos*	SDembek
DATE	9/3/2003	9/2/03	8/28/03	9/4/03

DOCUMENT NAME: C:\ORPCheckout\FileNET\ML032521518.wpd

OFFICIAL RECORD COPY

LIST OF ATTENDEES DURING TRIP OF JUNE 16-20, 2003

VISIT TO WINDSOR, CONNECTICUT

CPC UPGRADE LICENSE AMENDMENT REQUEST REVIEW

NAME	AFFILIATION
C. Graham	NRC/NRR/EEIB
M. Waterman	NRC/NRR/EEIB
T. Weber	APS
D. Gregoire	APS
A.F. Swirburl	APS
R. Pickwoad	APS
W. Odess Gilette	Westinghouse
B. Hudnoll	Westinghouse
B. Denyer	Westinghouse
W. Gardner	Westinghouse

Where:
APS = Arizona Public Service Company
NRC = Nuclear Regulatory Commission
NRR = Office of Nuclear Reactor Regulation
EEIB = Electrical and Instrumentation and Controls Branch

ENCLOSURE 1

LIST OF ATTENDEES DURING TRIP OF JULY 14-17, 2003

VISIT TO PALO VERDE PLANT SITE

CPC UPGRADE LICENSE AMENDMENT REQUEST REVIEW

NAME	AFFILIATION
C. Graham	NRC/NRR/EEIB
M. Waterman	NRC/NRR/EEIB
D. Gregoire	APS
A.F. Swirburl	APS
R. Pickwoad	APS
A.M. Taufig	APS
T.S. Shiu	APS
B. Hudnoll	Westinghouse (by phone)
W. Gardner	Westinghouse (by phone)

Where:
APS = Arizona Public Service Company
NRC = Nuclear Regulatory Commission
NRR = Office of Nuclear Reactor Regulation
EEIB = Electrical and Instrumentation and Controls Branch

NRC STAFF HANDOUT FOR WEEK OF JUNE 16-20, 2003, VISIT

1. Talking Points for Palo Verde Conference Call 06/05/2003

2. NRC SW System Audit in Windsor, CT for CPC application

ENCLOSURE 2

TALKING POINTS FOR PALO VERDE CONFERENCE CALL 06/05/2003

The conference call was held with the licensee on June 5, 2003, to discuss the visits by the NRC staff to Windsor, CT and the Palo Verde site. These talking points and the outline of the trip to Windsor, CT were sent to the licensee prior to the conference call.

Schedule

Discuss Visits

Windsor, Connecticut for Software Audit (week of June 16- Monday through Friday)

PVNGS for review of Arizona Public Service Company (APS) core protection calculator system (CPCS) implementation (week of July 14 , Monday through Friday)

APS Documentation

Have received: procurement specification, request for additional information (RAI) draft responses in meeting of May 14, 2003, APS Document 80DP-0CC01 and several engineering drawings

Westinghouse office document review - Questions

Requirements Traceability Matrix - discussion to clarify its use

Describe the connections that exist between the CPCS channels in the CEAC processors. How is channel independence maintained?

The system event log holds up to a certain number of events, is there a limiting condition for operation for types of events that may be present in the system event log.

What events or errors have occurred on the legacy system during its operation and how were these corrected?

The drawing given in the FMEA shows transmission control protocol/Internet protocol connections from the OMs (in addition to the connection from the MTP discussed previously) to what appears to be a LAN and LAN printer. Discuss how the existence of this connection does not permit inadvertent changes to addressable constants. What addressable constants can be changed from the OM?

Has an FMEA been performed for the interposing relay panel?

The RCPSSS (reactor coolant pump shaft speed sensor) converts signals from the RCP shaft speed for use by the DP acquisition cards in each CPCS channel. Is the RCPSSS new? If not has it been approved by the staff? Why are there not two DP cards (for RCP) as there are two AI cards for other analog inputs such as Th, Tc and Pressure?

WDT's can be implemented in different ways in the Common Q, describe their configuration for CPC. How will the WDTs be tested?

The SPM, Section 3.4 discuss SW safety. Under the section, *Sequences of actions that can cause the system to enter a hazardous state*, it states that "...hazards are identified in the Software Requirements Specification." Please identify where in the SRS for the CPCS these are located?

FDR for a CPC discusses interlocks and permissives in section 3.7. A $<10^{-4}$ % reactor power trip and pretrip bypass (with the ability to change the setpoint) is discussed. Please discuss for the Common Q, how the failure of this bypass or the failure of the bypass to be automatically removed if reactor power is greater than the setpoint, does not present a single or common mode failure to the CPCS.

In the SysRS, a reliability goal of $5x10^{-3}$ failures / channel is mentioned. Is this for the hardware only? Is there a reliability block diagram, fault tree or other analysis methodology identified to support this value?

Comments

NRC SW SYSTEM AUDIT IN WINDSOR, CT FOR CPC APPLICATION

The NRC will visit the offices of Westinghouse in Windsor, Connecticut (CT), to conduct an audit of the CPC application running on the Common Q platform. NRC August 11, 2000, Common Q SER (ADAMS Accession # ml003740165) Section 4.3.2 *Summary of the Evaluation of the Life Cycle Planning Process* and PSAI 6.5 are the bases for this audit. The staff will use the Westinghouse Software Program Manual for Common Q Systems as a guide to review the life-cycle process and the software life-cycle process for the CPC application. Additional references are provided below:

IEEE standard for software reviews and audits
FDR for a CPC
FDR for a CEAC
SysRS (System requirements specification)
SRS (Software requirements specification)
RTM
Testing documents

Note: Function thread audits will be informal table top discussions looking in detail at SRS, SDD's (including function charts and code), testing docs and feedback process to correct/update SysRS and SRS. NRC wishes to work undisturbed during certain times with Westinghouse personnel available for questions or doc requests, if needed. One function will be provided before arrival, the remaining 3 will be provided upon arrival on site.

Facilities requested: Closed room in relatively quiet area with large table.

Schedule for June 16 to 20, 2003, Visit to Windsor, CT

June 16 (Monday)

1:00 PM Opening Remarks : NRC, APS and Westinghouse

2:00 - 5:00 PM Document review - NRC to review docs in informal session.

June 17 Tuesday

8:00 Westinghouse discuss life-cycle activities for the CPC to include the following:

SPM application
Translation of requirements from Legacy CPC to Common Q
Generation of SysRS and SRS
V&V effort
RTM
Use of Liverpool Data Research Associates for testing
Testing strategy and results

12:00 Lunch break

1:00 Continuation of morning discussion

Begin with function 1 thread audit (function 1 will be the calculation of **local power density**)

4:30 - 5:00 NRC to provide feedback on days activities.

5:00 close

June 18 Wednesday

8:00 Continuation of function 1 thread audit

Begin 2 thread audit

12:00 Lunch break

1:00 Continuation of function 2 thread audit, commence function 3 thread audit

4:30 - 5:00 NRC to provide feedback on days activities.

5:00 close

June 19 Thursday

8:00 Continue function 3 thread audit, commence function 4 thread audit

12:00 Lunch

1:00 Questions from submittal, RAI's, Rockville office review and phone cons

4:30 - 5:00 NRC to provide feedback on days activities.

5:00 close

June 20 Friday

8:00 Continuation of Thursday discussion

10:00 NRC Caucus in closed session

11:00 Closing remarks by NRC, APS, and Westinghouse

12:00 End of visit

NRC STAFF HANDOUT FOR WEEK OF JULY 14-17, 2003, VISIT

1. AGENDA, NRC Visit to APS – Core Protection Calculator

2. Question for Visit to Palo Verde

ENCLOSURE 3

AGENDA

NRC Visit to APS – Core Protection Calculator

The Staff will visit the PVNGS to evaluate and review the APS efforts with regard to the upgrade of the core protection calculator system (CPCS) for units 1,2 and 3. The staff will use the APS engineering procedures and the procurement spec as part of the review and will also evaluate APS involvement in the procurement, implementation, changeout, installation and pre and in-situ acceptance testing of the Common Q core protection calculator.

Monday

1:00–5:00 PM

Staff arrival

Staff will perform document review and orientation activities in closed session, with APS available for document orientation and requests. Please provide also in electronic format on CD.

> Procurement Specification (Paper only, staff has electronic copy)
> *Control of SW and Data for PCMS* 80DP-0CC01 (Paper only, staff has electronic copy)
> Related Implementing Procedures as listed in APS draft response #5 under "Additional Information." Any additional APS procedures used.

Tuesday

8:00 – 12:00

Opening remarks by NRC and APS

APS will please provide discussion in the following areas: *(APS may modify agenda flow to suit its needs and presentation flow.)*

CPCS specification generation and procedures used in the CPCS upgrade.

Include in discussion:

- Specification of requirements
- Procurement
- Installation and testing schedule
- Process to ensure requirements were correctly translated
- Process to ensure added requirements did not adversely affect CPC functions
- Extent of involvement of CPCS users-engineers, control room operators and maintenance techs

12:00 – 1:00

Lunch

1:00 – 5:00

Tour of existing CPCS (simulator can be used)

APS efforts in reviewing the Common Q system as suitable for use in PVNGS

- Visits to Westinghouse and results
- APS design reviews and comments of major system components, design documents and schedules (as described in APS specification 13-JN-1000 revision 2, section 2.2)
- Performance of setpoint engineering and analysis work. (as described in APS specification 13-JN-1000 revision 2, section 2.14)
- V&V efforts
- Field device and reactor protection system compatibility
- Differences between CPCSs of unit 1,2 and 3
- Resolution of procurement spec items from section 9 and results of design reviews with APS at PVNGS site (as described in section 12.4)

Wednesday

8:00 – 12:00

EMI acceptance

Site acceptance test (SAT):

- Plan
- Verification of requirements
- Acceptance criteria
- Time response
- Power ascension and power operation

12:00 - 1:00

Lunch

1:00 – 5:00

Continuation of morning discussion

Thursday

8:00 – 12:00

RAI questions and resolution

12:00 - 1:00

Lunch

1:00 – 5:00

Continuation of morning discussion
NRC caucus in closed session (3:00 PM)
Closeout and depart (3:30 closeout)

June 26, 2003

QUESTIONS FOR VISIT TO PALO VERDE

The following questions were provided by NRC to Arizona Public Service Company (APS) in support of the core protection calculator system (CPCS) license amendment request (LAR) review visit on July 14 - July 17, 2003 at the PVNGS site. The NRC will be addressing these types of questions during the visit in order to evaluate APS review involvement activities as they relate to the CPCS upgrade request. These questions are not all inclusive and the NRC staff does not intend to ask all of the questions given below. The questions relate mostly to APS' Verification and Validation (V&V) activities, and the level of involvement therein.

QUESTIONS

1.0 Commercial Dedication Review

Activity: Planning

Product: Configuration Management Plan

Property: Correctness

Has the licensee ensure that revisions to the code are correct, have the correct revision number, have the proper installed values, are properly installed in the hardware, and are properly controlled?

Property: Organization

Has the licensee's configuration control board been identified, and do they understand their duties?

Product: Concept/Management Plan

Property: Quality

Is the commercial dedication process to be performed under 10 CFR 50 Appendix B? Is the new system compatible with the installation environment such that system performance will not be degraded compared to the system being replaced?

Will the modified system meet the required plant environmental and seismic envelopes? If revisions to tech specs are contemplated, are they correctly specified? Does the system perform adequately under heavy duty cycle loading, e.g., during accident conditions? Is there any difference in system performance between normal and accident conditions?

If the upgraded system has a response to restoration of power different from the system being replaced, are the consequences bounded by what was evaluated previously in the SAR?

If the upgraded system has a failure mode on loss of power different from the system being replaced, are the consequences within the limits previously documented in the SAR?

Are the methods that the licensee will use to determine if the system is operable known, and is it known if any revisions to tech specs are contemplated?

Are there means available to alert the operators to failure conditions, including new kinds of failures peculiar to the new design or different from the replaced equipment?

Product: Design Basis Requirements Allocated to Hardware

Property: Accuracy

Is there a quantitative accuracy requirement for each analog or digital input variable?

Property: Completeness

Are security measures specified to prevent the intrusion of viruses or other unauthorized activities?

Is there a requirement that the system perform self-diagnostics and report detected failures?

Is there a numerical specification for reliability or availability, e.g. MTBF, MTTR, and is this number adequate for the application?

Product: System Design

Property: Completeness

Does the timing fill the requirements of an analysis of sampling rate for digital control, and will the execution time of the software meet these requirements?

Are the electrical loads associated with the upgraded system addressed in the design? Is each output signal fully specified?

Is each output channel protected against short circuit?

Is each input signal fully specified?

If self-test features exist, do these features contain a return-to-normal in the event of an accident?

Does the upgraded system have adequate cabinet cooling?

Is the handling of all "out of range" inputs, including open and shorted circuits, specified?

Property: Consistency

Are the bypassed and inoperable detection means and indication consistent with the plant design basis?

Property: Functionality

Do the calibration and surveillance procedures provide complete loop testing, or is there adequate overlap of the separate sections to insure complete testing?

Activity: Procurement

Product: Analysis of Experience Data

Property: Critical Characteristics

Are the records of performance adequate for the determination of the characteristic?

Activity: Integration

Product: System Build and Configuration Documents

Property: Unambiguity

Do the plant drawings reflect all of the changes required by this modification, and have the plant safety analyses been updated to reflect the new equipment?

Property: Correctness

Did the licensee review the documented V&V system in place which includes a final validation phase to assure that the software meets all of its requirements?

Did the licensee review the documented V&V system in place which examines each phase of the software production process for correctness of input and output from each phase of software lifecycle?

Did the licensee review this V&V activity and was adequate documentation provided for this review?

Can the software configuration management system identify versions of software that are subject to defects that are discovered in the field?

Property: Unambiguity

Does the vendor have a configuration management system which documents a baseline design and which controls all changes made to the design?

Activity: Validation

Product: Special Test Report

Property: Completeness

Were all test anomalies resolved?

Were all critical characteristics of the software demonstrated?

Property: Critical Characteristics

If some of the critical characteristics are not adequately controlled by the vendor's quality assurance/quality control (QA/QC) program, what special tests and inspections were performed to verify the necessary characteristics?

Is it clear that if the tests and inspections are passed that the characteristic that is being controlled is present?

Are the special tests and inspections completely documented together with procedures for performing them?

Were special tests and inspections required for the electromagnetic interference/radiofrequency inference (EMI/RFI) requirements or was EPRI Report TR-102323 referenced?

Product: System Acceptance Tests

Property: Correctness

Does the post-modification testing performed by the licensee adequately demonstrate that the installed system's configuration meets the design basis?

Was system timing tested to verify that the actual system response times meet the requirements of the accident analysis?

Were the local and remote alarms indicating degraded conditions tested during the post installation testing?

Does the site acceptance test (SAT) adequately address the software/hardware requirements?

Does the SAT have acceptance criteria and procedure to perform if criteria is not met?

Activity: Installation

Product: CM Configuration Audit and Installation Report

Property: Correctness

If the software has been updated since the system was originally installed, was the update handled in accordance with the licensee's configuration management plan and any other QA/QC documents which may apply?

If the system's software is loaded from magnetic media, are the original and backup media properly labeled and controlled, and stored correctly?

Has the auditor verified that the system setpoints and coefficients are consistent with the system's documentation?

Product: Setpoint Analysis

Property: Accuracy

Have all set points been properly modified for this change?

Property: Consistency

Do the calibration procedures for the new equipment meet the Technical Specifications, applicable licensee standards, and vendor recommendations?

Property: Safety

Do the plant drawings reflect all of the changes required by this modification, and have the plant safety analyses been updated to reflect the new equipment?

Product: Plant Procedures

Property: Completeness

Are electrostatic discharge and EMI/RFI procedures and precautions properly documented and incorporated into relevant procedures?

Has the auditor verified that plant procedures have been updated to reflect the new system?

Have emergency operating procedures changed as a result of this system upgrade and what are those procedures.

Property: Correctness

Is there a method in place to assure that the software loaded is the correct software and that any corruption can be detected by documented surveillance methods?

Product: Technical Specifications

Property: Accuracy

Have all surveillance intervals been changed to reflect this change?

Property: Safety

Do the plant drawings reflect all of the changes required by this modification, and have the plant safety analyses been updated to reflect the new equipment?

Activity: Operation

Product: Operational Change Management Report

Property: Completeness

Does the licensee have arrangements to be notified of defects or problems with the dedicated product?

Does the licensee have a plan to ensure maintenance of commercial dedication?

Activity: Procurement

Product: Procurement Document

Property: Completeness

Is the environment in which the equipment will operate completely specified, and is this specification consistent with the plant licensing basis?

Is the grounding system specified and are there any special grounding requirements?

Have the specs and requirements in the procurement document been verified to have been completed satisfactorily?

Property: Consistency

Do the procurement documents specify the items to be purchased unambiguously by part number, model number, and revision numbers and are these consistent with the vendor and product(s) selected?

Activity: Validation

Product: Burn-In, Conflict Test and Software Compatibility

Property: Consistency

Did the licensee confirm that the hardware selected was compatible with the software selected?

Product: Critical Characteristic Test Report

Property: Correctness

Does the post-modification testing performed by the licensee adequately demonstrate that the installed system's configuration meets the design basis?

Do the system outputs fail-safe (or as-is if required by the design basis) on loss of power for those systems that provide inputs to safety related functions or which perform safety functions?

Activity: Installation

Product: Setpoint Analysis

Property: Accuracy

Have all set points been properly modified for this change?

Property: Consistency

Do the calibration procedures for the new equipment meet the Tech. Specs., applicable licensee standards, and vendor recommendations?

Property: Safety

Do the plant drawings reflect all of the changes required by this modification, and have the plant safety analyses been updated to reflect the new equipment?

Product: Installation and Checkout Report

Property: Completeness

Were all critical characteristics of the hardware demonstrated?

Are any test units or data loggers connected to the system properly used and properly isolated?

Is proper indication and/or annunciation provided for system bypass and failure?

Property: Consistency

Property: Reliability

Has the auditor verified that signs have been posted prohibiting nearby radio transmissions and that ship and mobile radio traffic is sufficiently far away so that the system is unaffected?

Product: Plant Procedures

Property: Completeness

Are electrostatic discharge and EMI/RFI procedures and precautions properly documented and incorporated into relevant procedures?

Product: Technical Specifications

Property: Accuracy

Have all surveillance intervals been changed to reflect this change?

Property: Safety

Do the plant drawings reflect all of the changes required by this modification, and have the plant safety analyses been updated to reflect the new equipment?

Product: Training Records

Property: Completeness

Do the training records reflect the training given to operators, technicians, and system engineers for the new system?

Are all operating modes identified?

Product: Plant Safety Analyses

Property: Completeness

Has the licensee analyzed the effect of the system replacement on related issues such as Regulatory Guide 1.97, Station Blackout (10 CFR 50.63), ATWS (10 CFR 50.62), 10 CFR 50 Appendix R, and the SPDS to ensure consistency with the plant licensing basis?

Property: Safety

Do the plant drawings reflect all of the changes required by this modification, and have the plant safety analyses been updated to reflect the new equipment?

Activity: Operation

Product: Maintenance Plan

Property: Security

If PCs, portable configurators, or other computer based interface test equipment is used, are adequate controls for physical protection, virus protection, password controls, and personnel access, etc. used to insure the integrity of such equipment?

2.0 Inspection Module Review

Activity: Inspection

Did the licensee or the vendor perform verification and validation (V&V) on the software?

Has the software quality control, configuration management, and general software quality documentation been reviewed for proper demonstration of compliance with the requirements of 10 CFR Part 50 Appendix B?

If the vendor performed the V&V, did the licensee review this V&V?

3.0 Software Review

Activity: Planning

Product: Software Management Plan

Property: Management - Responsibilities

Are the responsibilities of each member of the project's management and technical team defined?

Does the Plan explicitly require that the Software Project Management Plan & Software Development Plan be revised when there are major changes to either the software scope of work or to the organizational structure?

Is there a formal procedure for review and approval of the Plan?

Does the Plan provide a means of updating the Plan?

Are the people that provided the initial review or approval of the Software Management Plan and the Software Development Plan identified by name?

Is there a formal mechanism for dealing with externally and internally generated changes of scope?

Does the Plan include a policy statement that the personnel who product each output required by the Development Plan have primary responsibility for the quality of that output?

Property: Management - Security

Is the security level of each phase defined?

Is the security organization, including lines of communication, lines of responsibility and lines of authority, depicted?

Is there a documented security plan?

Property: Resources - Methods / Tools

Does the Plan describe the methods, techniques and tools required to carry out the project management?

Property: Resources - Personnel

Does the Plan specify the numbers and types of personnel required to conduct the project?

Are the personnel resources required for each project phase identified?

Has each phase of the software life cycle been divided into elementary tasks with a well-defined activity for each task?

Property: Implementation - Schedule

Does the Plan identify key work packages?

Does the schedule justify the time anticipated to complete each task?

Is there a formal documented delivery schedule?

Is time for reviews and audits included in the schedule as project milestones?

Does the schedule include time for the integration of new software with existing software, purchased software, hardware and documentation?

Are the inputs to and outputs of each phase identified and shown on the master schedule?

Does the Plan identify key milestones and hold points?

Does the Plan include a project schedule?

Have sufficient intermediate milestones been identified?

Property: Management - Organization

Has a project life cycle been defined?

Does the life cycle include uniquely identifiable development, verification and support processes with well-defined inputs and outputs?

Is the life cycle model appropriate to the project?

Has the life cycle model been documented in the Plan?

Property: Management - Oversight

Does a method exist to identify any deviations from the software development plan in time to take corrective action?

Does the Plan require that progress be documented at regular intervals?

Does a method exist for monitoring progress against the software development plan?

Are required software quality factors identified and ordered by importance?

Are project priorities listed?

Is a strategy for managing the technical development effort specified?

Property: Management - Purpose

Is there a clear, concise, documented description of the objectives of each life cycle phase and its context in the overall project?

Are all required software quality factors identified in the Plan?

Does the Plan identify key design and implementation issues, and preliminary studies, simulation modeling and / or the prototyping required to resolve them?

Property: Resources - Methods / Tools

Does the Plan describe the approach to be followed for reusing software?
Are tools developed with the same rigor and level of detail as the deliverable software?

Have tools been developed or acquired to improve the quality and reliability of the software?

Does the Plan describe the software development environment?

Does the Plan identify suitable facilities, tools and aids to facilitate the production, management and publication of appropriate and consistent documentation?

Does the Plan describe the software development methods to be used?

Property: Resources - Standards

Does the Plan identify software requirements standards?

Does the Plan mandate the project-specific standards and guidelines to be followed?

Does the Plan identify software design standards?

Does the Plan identify software code standards?

Product: Software Quality Assurance Plan

Property: Implementation - Measurement

Does the Plan require that data associated with the methodologies used in the life cycle and the software products be systematically collected and analyzed?

Does the Plan require QA data to be systematically collected and analyzed to determine software quality?

Property: Implementation - Procedures

Does the Plan describe the Software Quality Assurance procedures from start of project to finish?

Are all required software quality factors identified in the Plan?

Does the Plan require Software Quality Assurance participation in formal reviews and audits?

Does the Plan include procedures to identify and correct conditions adverse to quality?

Does the Plan require that Software Quality Assurance personnel attend all project software progress meetings?

Does the Plan describe the methods, procedures and controls for ensuring that technical, quality and other requirements are accurately stated in the project documentation?

Does the Plan provide for quality assurance participation in the assessment and review of project-specific standards, methods and tools?

Does the Plan describe quality-related reports?

Does the Plan assure that traceability is maintained through all phases of the software life cycle?

Does the Plan provide a schedule of software quality assurance activities?

Property: Implementation - Record Keeping

Does the Plan specify record keeping requirements?

Does the Plan describe storage, handling and shipping procedures?

Does the Plan include a list of documents subject to software QA oversight?

Is the document control mechanism specified?

Does the Plan describe record management procedures?

Property: Management - Organization

Does the Plan describe the software quality assurance organization?

Does the Plan describe QA reporting channels?

Does the Plan describe the boundaries between the software QA organization and other company organizations?

Property: Management - Purpose

Does the Plan list specific objectives for the software QA effort?

Does the QA Plan list the general functions the software QA organization will be expected to perform?

Property: Management - Responsibilities

Does the Plan require the software quality assurance organization to assess and evaluate system safety, reliability and maintainability characteristics of the software?

Does the Plan state the responsibility and authority of the Software Quality Assurance organization?

Property: Resources - Methods / Tools

Does the Plan describe the resources required to support the Software Quality Assurance program?

Does the Plan describe the tools that will be used to accomplish the quality assurance function?

Does the Plan describe the methods and techniques that will be used to accomplish the quality assurance function?

Property: Resources - Standards

Does the Plan describe standards and procedures to be used?

Does the Plan provide methods to assure that the approved standards, methodologies and tools are applied throughout the software lifecycle?

Does the Plan establish and maintain the standards and methodologies for software quality assurance, V&V and configuration management?

Product: Installation Plan

Property: Implementation - Measurement

Are a set of indicators required to determine the success or failure of the installation effort?

Does the Plan require that the error rate found during installation be measured, recorded, analyzed and reported?
Does the Plan require that data associated with the installation be collected and analyzed?

Property: Implementation - Procedures

Is adequate testing required to provide confidence that the installed system will perform its safety functions?

Does the Plan require that all affected functions be declared inoperable according to the plant's technical specifications before proceeding with installation?

Does the Plan list the tasks required for system installation?

Does the Plan provide step-by-step procedures required to accomplish the installation?

Does the Plan provide an inventory of the software required to support the installation?

Does the Plan describe the methods, procedures and controls used to ensure that the success or failure of the installation effort can be readily determined?

Are checks required to ensure that the computer system is functional?

Is a check required to ensure that the correct software versions are installed on the correct computers?

Are installation reports defined?

Does the Plan require that anomalies discovered during installation be reported to the developer and resolved prior to placing the software into operation?

Does the Plan require that appropriate return-to-service testing be conducted prior to declaring the modified function operable?

Property: Management - Organization

Are reporting channels described?

Does the Plan describe the installation organization?

Does the Plan describe the boundaries between the installation organization and other safety system installation organizations?

Property: Management - Purpose

Does the Plan provide a general description of the installation process?

Does the Plan include a general description of the environment within which the computer system and software system is qualified to operate?

Property: Management - Responsibilities

Does the Plan define the responsibilities and authority of the software installation organization?

Is the delineation of responsibility between the development organization and the customer defined in such a way that misunderstandings in communication between the two organizations are kept to a minimum?

Property: Resources - Methods / Tools

Does the Plan require that installation tools be qualified with a degree of rigor and level of detail appropriate to the safety significance of the software which is to be installed using the tools?

Does the Plan describe the physical facilities and accommodations required during installation?

Does the Plan describe the methods, techniques and tools that will be used to accomplish the installation function?

Product: Operations Plan

Property: Implementation - Measurement

Does the Plan require that the operator error rate found during operation activities be measured, recorded, analyzed and reported?

Does the Plan provide a set of indicators required to determine the success or failure of the operating procedures?

Property: Implementation - Procedures

Does the Plan describe the procedures necessary to start, operate and stop the software system?

Does the Plan describe actions to be taken if the computer system starts to behave abnormally?

Does the Plan describe procedures for executing the software in all operating modes?

Is the user documentation defined?

Does the Plan describe procedures for ensuring that the software state is consistent with the plant operating mode at all times?

Does the Plan describe backup procedures for data and code, and the intervals at which backup should occur?

Does the Plan require a list of error messages?

Property: Management - Organization

Is the organizational structure appropriate for the control of the software operation described?

Does the Plan specify operator interface stations and actions required to support operation?

Property: Management - Purpose

Does the Plan include a general description of the operation of the software?

Does the Plan include a general description of the functions that the software is to perform, and a general discussion of the means of carrying out those functions?

Property: Management - Responsibilities

Are the responsibilities and authority of the plant operators to manage the computer systems defined?

Property: Management - Security

Does the Plan describe the monitoring activities needed to detect penetration or attempted penetration of the software system?

Does the Plan describe controls needed over operation activities to prevent unauthorized changes to hardware, software and system parameters?

Does the Plan include a description of security requirements for operating the software system?

Does the Plan provide contingency plans needed to ensure appropriate response to penetration?

Property: Resources - Methods / Tools

Does the Plan describe the facilities required to operate the delivered software?

Does the Plan describe the methods, techniques and tools that will be used to operate the software system?

Does the Plan describe the documentation required to support the delivered software?

Product: Software V&V Plan

Property: Implementation - Measurement

Does the Plan require a set of indicators that can be used to determine the success or failure of the V&V effort?

Does the Software V&V Plan specify the criteria to be used to identify the completion of each V&V task?

Does the Software V&V Plan establish evaluation criteria for the review plans, review specifications and review procedures?

Does the Plan require that data be systematically collected and analyzed to determine the effectiveness of the V&V effort?

Does the Plan require that the error rate found during software reviews and software testing be measured, collected, analyzed and reported?

Does the Software V&V Plan establish evaluation criteria for the test plans, test specifications, test procedures and test cases?

Did the licensee review software errors found by the V&V process?

Has the licensee ensured that revised code is correct?

If software was revised and updated since the system installation, was the update handled in accordance with the configuration management plan and any other QA documents that may govern? If there is any inactive code in the system (i.e., code still found in memory but not used for the plant-specific application), did the licensee verify that it cannot or will not be reactivated erroneously or through subsequent revisions?

Did the licensee verify that "generic" values used in the software code are applicable to this plant?

Did the licensee demonstrate that the software V&V meets the ANSI/IEEE Std. 7-4.3.2 (1993) guidance?

Did the software used in the test equipment undergo a V&V process?

Does the Software V&V Plan specify procedures for technical software review activities?

Does the Software V&V Plan specify a method for resolving discrepancies identified during the verification of each V&V task?

Does the Software V&V Plan require that formal communication between the verification and design groups be documented?

Does the Software V&V Plan require the generation and dissemination of anomaly reports?

Does the Software V&V Plan specify a procedure for evaluating the effect of proposed software changes on planned V&V tasks?

Does the Software V&V Plan identify all items which will be subject to V&V activities?

Does the Software V&V Plan specify the planning assumptions for each V&V task?

Does the Software V&V Plan require approved test plans, specifications and procedures to be in place before the start of the testing activity?

Does the Software V&V Plan specify procedures for test case selection?

Does the Software V&V Plan require that the test case documentation specify expected results?

Does the Software V&V Plan require that review and software V&V reports summarize the positive practices and findings?

Does the Software V&V Plan specify review inputs, entry criteria, exit criteria and outputs?

Does the Software V&V Plan require approved review plans, specifications and procedures to be in place before the start of the review activity?

Does the Software V&V Plan describe the activities to be performed to evaluate each software item and each development activity to demonstrate that the requirements have been met?

Does the Software V&V Plan require that review and software V&V reports summarize the actions performed and the methods and tools used?

Does the Software V&V Plan specify procedures for evaluating the risks associated with each project development activity?

Does the Software V&V Plan specify procedures to ensure that systems in which errors are detected are properly analyzed, reported, corrected, re-verified, re-validated and re-tested?

Does the Software V&V Plan specify the pass/fail criteria for each V&V task?

Does the Software V&V Plan specify the method by which each V&V task is to be carried out?

Does the Software V&V Plan establish procedures which will be used by the verification team?

Does the Software V&V Plan specify a procedure for coordinating proposed software changes with the Configuration Management organization?

Does the Software V&V Plan specify the V&V tasks which will be carried out?

Does the Plan describe V&V reporting requirements?

Does the Software V&V Plan describe procedures for carrying out each V&V task during each life cycle phase of the software development effort?

Property: Management - Organization

Are reporting channels defined?

Does the Plan describe the boundaries and interfaces between the software V&V organization and other company organizations?

Does the Software V&V Plan specify the relationships among the different V&V tasks?

Property: Management - Purpose

Does the Plan define the purpose and scope of the software V&V activities?

Does the Plan include a general description of the software V&V process?

Property: Management - Responsibilities

Does the Software V&V Plan identify a specific person to carry out the verification of each task?

Is it clear from the Plan that the V&V authority has adequate independence?

Does the Software V&V Plan identify the person with authority to approve the successful completion of the testing tasks?

Does the Software V&V Plan identify the person with authority to approve the successful completion of the V&V tasks?

Does the Software V&V Plan define the responsibilities for carrying out each V&V task?

Does the Software V&V Plan identify how the required resources will be made available when needed?

Property: Management - Risks

Does the Software V&V Plan specify procedures for evaluating the development risk associated with each software item?

Does the Software V&V Plan include a contingency plan to identify risk factors that may cause the V&V task to fail to perform its functions?

Does the Software V&V Plan specify a method for identifying the risk associated with each V&V task?

Does the Software V&V Plan specify a method for evaluating the criticality (risk to safety) of each software item?

Property: Resources - Methods / Tools

For those tools yet to be developed, is there an estimate in the Software V&V Plan of the time and resources needed to develop and qualify the tools?

Does the Software V&V Plan specify the method, materials and schedule for carrying out each V&V task?

Does the Software V&V Plan specify the tools, techniques and methods to be used in the V&V tasks?

Does the Software V&V Plan specify the method for carrying out testing at the unit, integration, system and acceptance test levels?

Does the Software V&V Plan specify the resources required for acquisition, training, support and qualification of each tool, technique and method?

Property: Resources - Standards

Does the Plan require a list of the international, national and industry standards adopted by the company, plus company standards and guidelines to be followed by the V&V organization?

Product: Software Configuration Management Plan

Property: Implementation - Measurement

Does the Plan require that data associated with configuration management be systematically collected and analyzed to determine the effectiveness of the Configuration Management effort?

Property: Implementation - Procedures

Does the Software Configuration Management Plan describe fully procedures for backup and disaster recovery?

Does the Software Configuration Management Plan describe fully procedures for managing software libraries?

Does the Software Configuration Management Plan require periodic reviews and audits of the configuration baseline, including physical audits of the baseline?

Does the Software Configuration Management Plan describe fully procedures to manage the change process?
Does the Software Configuration Management Plan describe fully procedures for reporting about Configuration Management activities?

Does the Software Configuration Management Plan describe fully procedures for maintaining a change history for each configuration item?

Does the Software Configuration Management Plan describe fully procedures for associating source code with the derived object code and executable modules?

Does the plan describe the process used to maintain and track purchased items?

Are record keeping requirements specified?

Does the Software Configuration Management Plan describe fully procedures for placing items under configuration control?

Does the Software Configuration Management Plan describe fully procedures for approving change requests?

Does the Software Configuration Management Plan describe fully procedures for tracking problem reports, and making sure that each problem reported has been correctly resolved?

Does the Software Configuration Management Plan describe fully procedures for identifying and naming configuration items?

Does the Software Configuration Management Plan describe the information required to approve a change request?

Does the Software Configuration Management Plan describe fully procedures for protecting configuration records?

Does the Software Configuration Management Plan describe fully procedures for keeping data files and tables synchronized with the software that uses them?

Property: Management - Organization

Does the Software Configuration Management Plan identify Software Configuration Management organizational interfaces and boundaries?

Does the Software Configuration Management Plan describe the Software Configuration Management organization?

Are reporting channels defined?

Property: Management - Purpose

Does the Plan define the purpose and scope of the Software Configuration Management activities?

Does the Plan list the general functions the Software Configuration Management organization will be expected to perform?

Property: Management - Responsibilities

Does the Software Configuration Management Plan define the responsibilities for carrying out each Software Configuration Management activity?

Does the Software Configuration Management Plan identify the person who has the authority to release any software, data and documents?

Does the Software Configuration Management Plan identify the person with authority to override normal Software Configuration Management procedures during exceptional situations?

Does the Plan define the duties of the configuration control board?

Property: Resources - Methods / Tools

Does the plan describe the methods, techniques and tools required to carry out each Configuration Management task?

Property: Resources - Standards

Does the Plan include a list of the international, national and industry standards to be used by the company, and any

company standards and guidelines that will be followed by the Software Configuration Management organization?

Have the safety analysts evaluated software safety requirements related to instrumentation interfaces by suitably rigorous methods?

Were the analysts that carried out the Requirements Safety Analysis well qualified to undertake the analysis?

Are the formal lines of communication for the Requirements Safety Analysis?

Product: V&V Requirements Analysis Report

Property: Review - General

If diverse requirements specifications have been used, has the verifier made a comparison among the specifications to ensure that they are functionally identical and consistent?

Does the Report reference documentation which indicates that formal reviews of the specifications have been undertaken?

Are the requirements properties to be verified, and the method of verification, clearly specified in the V&V plan?

Does the Report reference documentation provided which is sufficient for the satisfactory completion of the verification task?

Property: Review - Requirements Analysis

Have the verifiers analyzed software requirements related to timing and sizing by suitably rigorous methods?

Have the verifiers analyzed software requirements related to operator interfaces by suitably rigorous methods?

Have the verifiers analyzed software requirements related to functionality by suitably rigorous methods?

Have the verifiers analyzed software requirements related to security by suitably rigorous methods?

Has an ergonomic analysis been performed on information display requirements?

Have the verifiers analyzed software requirements related to reliability by suitably rigorous methods?

Have acceptance criteria been defined for each requirement?

Have the verifiers analyzed software requirements related to robustness by suitably rigorous methods?
Have the verifiers analyzed software requirements related to safety by suitably rigorous methods?

Have the verifiers analyzed software requirements related to instrumentation interfaces by suitably rigorous methods?

Property: Review - Requirements Properties

Have the verifiers ensured that the software requirements are accurate?

Have the verifiers ensured that the software requirements are complete?

Have the verifiers ensured that the software requirements can be traced forward to system acceptance tests?

Have the verifiers ensured that the software requirements are consistent with the System Design Description and the Safety Analysis Report?

Have the verifiers ensured that the software requirements are unambiguous?

Have the verifiers ensured that the reliability, robustness, safety, security and timing requirements have been met?

Have the verifiers ensured that implementation of the software requirements is feasible?

Have the verifiers ensured that each software requirement has a unique reference?

Does the software detailed design take into account all expected situations and conditions documented in the System Design Description, Safety Analysis Report, Software Requirements Specification and Software Architecture Design Description?

Was a design interface analysis performed to determine that the interfaces among the detailed design elements have been correctly designed?

Are the number, size, data rates, sampling frequencies and response times of all data channels defined in the Software Detailed Design Description?

Does the software detailed design implement the required program behavior with respect to each interface?

Are the specified models, algorithms, numerical techniques, signal conversion and data handling procedures within the state-of-the-practice?

Is each requirement in the Software Requirements Specification translated into detailed design specifications?

Was the hardware environment considered in the software detailed design?

Was the operational environment considered in the software detailed design?

Does the software detailed design consider all operating modes specified in the Software Requirements Specification?

Are all specific detailed design areas that create special difficulties identified and is a mitigation plan described?

Can the software detailed design be implemented within the constraints imposed on the system and on the development effort?

Does the Software Detailed Design Description describe a software detailed design that meets the requirements of the system and all constraints described in the Software Requirements Specification and Software Architecture Design Description?

Property: Consistency

Are there standard interfaces for data transfer?

Is the style of presentation and the level of detail consistent throughout the Software Detailed Design Description?

Are the detailed designs for similar or related functions consistent?

Is each software detailed design element consistent with documented descriptions and known properties of the operational environment within which the programs will operate?

Are there standard interfaces for human-machine interfaces?

If more than one formal detailed design method is used, are they mutually consistent?

Are the models, algorithms, and numerical techniques specified mathematically compatible with one another?

Are input and output specifications given in the software detailed design consistent with interface requirements imposed by the hardware or predeveloped software?

Is the software detailed design consistent with the hardware and software architecture?

Is the software detailed design consistent with the software requirements specification?

Do models, algorithms and numerical techniques specified in the software detailed design agree with standard references where such are appropriate?

Are there standard interfaces for peripheral interconnections?

Property: Correctness

If floating point arithmetic or recursion are used in the detailed design, is adequate justification given for their use?

Has an analysis of algorithm precision been performed to identify potential underflow and overflow conditions?

Has an analysis been performed to evaluate potential data handling problems?

Has an analysis been performed to evaluate data structures for data dependencies that circumvent isolation, partitioning, data aliasing, and fault containment issues?

Are all equations and algorithms defined correctly, and defined to a sufficient level of detail to permit coding?

Upon exit from each subroutine or procedure, is status checked (if status is provided) and the proper action taken if an error status is indicated?

Has an analysis of algorithms been performed to ensure that the algorithms are stable over the entire range of inputs and timing parameters?

Is the input to each unit checked for validity?

Is there convincing evidence that no interrupt will change the value of a safety-critical data item in an unanticipated manner?

Is there convincing evidence that no safety-critical data item can have its value changed in an unanticipated manner, or by an unanticipated detailed design element?

Is there convincing evidence that no safety-critical data item is used before being initialized?

Are equations, algorithms, and control logic evaluated for potential problems?

Are mechanisms present in the software detailed design that will maintain the currency and consistency of state variables?

Property: Reliability

Are there checks for missing and/or late messages?

Are there checks for memory-bound and write-protection errors?

Are there checks for clock shift?

Does the software detailed design include validity checks for all operator inputs?

Are there check codes on memory and transmission messages?

Does the analysis of reliability and availability include sufficient supportable data to guarantee meeting the reliability requirements?

Are there checks that reveal that a card has been removed?

Are all detected hardware and software failures reported?

Are there facilities for displaying the software status?

Does the software detailed design specify complete and correct error recovery techniques?

Does the software detailed design lead to well-defined output even if correct error recovery cannot be guaranteed?

Does the software detailed design include the capability to produce a well-defined output in the event that a failure is detected?

Have techniques been used to prevent failure propagation during program execution?

Product: V&V Design Analysis Report

Property: Review - Design Analysis

Have the verifiers analyzed software design elements related to robustness by suitably rigorous methods?

Have the verifiers analyzed software design elements related to reliability by suitably rigorous methods?

If the V&V analysis identifies shortcomings which require increased functionality in the design which was not initially required by the SRS, were appropriate change requests issued for the SRS and were these changes appropriately included?

Have the verifiers analyzed software design elements related to security by suitably rigorous methods?

Have the verifiers analyzed software design elements related to functionality by suitably rigorous methods?

Have the verifiers analyzed software design elements related to operator interfaces by suitably rigorous methods?

Have the verifiers analyzed software design elements related to safety by suitably rigorous methods?

Have the verifiers analyzed software design elements related to instrumentation interfaces by suitably rigorous methods?

Have the verifiers analyzed software design elements related to timing and sizing by suitably rigorous methods?

Property: Review - Design Qualities

Have the verifiers ensured that all the implementation constraints imposed by the software design are necessary?

Have the verifiers ensured that the Software Design Description is consistent with the Software Requirements Specification?

Have the verifiers ensured that the Software Design Description is complete?

Have the verifiers ensured that the Software Design Description is clear?

Have the verifiers ensured that implementation of the software design is feasible?

Have the verifiers ensured that the software design elements can be traced forward to system acceptance tests?

Have the verifiers ensured that the Software Design Description is accurate?

Have the verifiers ensured that the Software Design Description is unambiguous?

Have the verifiers ensured that the software design is correct?

Have the verifiers ensured that the software design elements can be traced forward to software integration tests?

Have the verifiers ensured that the Software Design Description is internally consistent?

Have the verifiers ensured that the reliability, robustness, safety, security and timing requirements have been met in the design?

Property: Review - General

Have the verifiers ensured that documentary evidence has been provided for satisfactory completion of the verification task?

If diverse design models have been used, has the verifier made a comparison between the various designs to ensure that they are functionally consistent?

Have the verifiers seen documentary evidence to indicate that formal reviews of the Software Design Description have been undertaken?

Are the software design qualities to be verified, and the method of verification, clearly specified in the V&V plan?

Property: Review Results

Has the verifier seen documented evidence that the software has been designed to the specified standards and guidelines?

Is there convincing evidence that the software design reviews have covered all requirements in the Software Requirements Specification and all design elements, data structures, and databases described in the Software Design Description?

Is there evidence that all specified corrective actions have actually taken place and all necessary documents updated with appropriate change control procedures?

Was the verification activity itself well documented?

Is there convincing evidence that the software design reviews have covered all standards and procedures applicable to the Software Design Description?

Have all required corrective actions been identified and documented which will remove any deficiencies in the Software Design Description?

Have all deficiencies in the design elements or in the Software Design Description identified by the verifiers been formally discussed with the development team, and formally documented?

Property: Review Team

Were the verifiers well qualified to undertake the verification?

Were the people that carried out the design verification known by name and do they understand their jobs?

Product: CM Design Report

Property: Change Control Board

Who are the members of the Change Control Board?

Does the configuration management system manage the safety impact of changes?

Do procedures exist that ensure that no safety-related design changes take place without formal approval of the Change Control Board?

Is the current location and person responsible for each design configuration object recorded?

Are all safety critical design configuration items labeled as such?

Is there a traceability matrix showing for each design element the requirement(s) from which it flows?

Are all design configuration items uniquely identified with an item code (or name) and a version number?

Does a configuration baseline exist for design elements and design analyses?

Is the status of each design configuration item recorded?

Property: Configuration Manager

Who is the configuration manager?

Does the configuration management system include arrangements for disaster protection and protection from subversion and sabotage of the design configuration items?

Does the configuration management system ensure that only approved versions of design configuration items are made available for use in coding?

Is the configuration manager well qualified?

Does the configuration management system ensure that a design configuration item can be released for change to only one person at a time?

Property: Problem Reporting and Change Management

Do procedures exist to assess the impact of requested design changes on the software requirements?

Does an anomaly reporting system exist for recording all identified anomalies and problems with the software design?

Does a means exist to ensure that all reported anomalies are resolved and the resolutions documented?

Are all anomaly reports, their resolutions, any resulting change requests and their resolutions archived for later retrieval?

Does a status accounting method exist for determining the status of all anomaly reports and change requests?

Product: V&V Implementation Analysis and Test Report

Property: Code Review - Code Analysis

Have the verifiers analyzed the code for correctness of algorithms, accuracy, precision, equation discontinuities, out-of-range conditions, breakpoints, and erroneous inputs?

Is there convincing evidence that the results of coding activities are within the timing and sizing constraints?

Have the verifiers found convincing evidence that adequate interface compatibility of software units with each other and with external hardware and software exists?

Is there convincing evidence that the software complies with system safety requirements?

Have the verifiers analyzed the code for proper error default handling for inappropriate or unexpected data in the input data stream?

Is there convincing evidence that no combination of independent, dependent or interdependent events could cause the system to operate in a hazardous manner?

Have the verifiers analyzed the code for consistent interfaces?

Is there convincing evidence that no single or multiple combinations of out-of-bounds or overloading input conditions can cause the system to operate in a hazardous manner?

Have the verifiers analyzed the code for proper event sequence?

Have the verifiers analyzed the code for correct data flow?

Have the verifiers analyzed the code for correct control flow?

Have the verifiers analyzed the code for completeness?

Have the verifiers analyzed the code for error definition, isolation and recovery?

Has non-critical code been analyzed to provide adequate confidence that it does not adversely affect the function of critical software?

Property: Code Review - Code Qualities

Have the verifiers ensured that the code elements can be traced to the software design and the software requirements?

Have programs, components, units, and functions been analyzed for design or coding errors which could cause or contribute to an undesired event affecting safety?

Have the verifiers checked to see if error status is checked and appropriate action taken after each procedure call where error status is returned?

If multitasking is used, or if a distributed system is used, can it be guaranteed that deadlock is avoided?

Have the verifiers seen documentary identification of those parts of the code that have been provided by well-proven library routines?

Have the verifiers ensured that all equations, algorithms and control logic have been evaluated for potential problems?

Have the verifiers ensured that data structure and usage in the code provides adequate confidence that the data items are defined and used properly?

Has the software been evaluated to ensure the feasibility of integration, operation and maintenance?

Have the verifiers ensured that all algorithms, components, units, and calculations been analyzed for proper operation?

Have the verifiers reviewed the code to determine that it conforms to the project's coding standards and guidelines?

Have the verifiers ensured that the software design elements can be traced forward to the code?

Property: Code Review - General

Have the verifiers seen documentary evidence to indicate that formal code reviews have been undertaken?

Have the verifiers ensured that documentary evidence exists to demonstrate satisfactory completion of the verification task?

Property: Code Review Results

Was the verification activity itself well documented?

Is there evidence that all specified corrective actions have actually taken place and appropriate documentation updated?

Is there convincing evidence that the software code reviews have covered all design elements, data structures, and databases described in the Software Design Description?

Have all required corrective actions been identified and documented which will remove any deficiencies in the code?

Have all deficiencies in the code elements identified by the verifiers been formally discussed with the development team, and formally documented?

Property: Code Review Team

Were the people that carried out the code verification known by name and do they understand their jobs?

Were the verifiers well qualified to undertake the verification?

Property: Unit Testing Activity

Do unit test results show that all paths between definitions of data and the uses of those data definitions were tested (data flow coverage)?

Is there a formal description of unit test cases, test inputs and test results?

Have the software units been tested to ensure that each satisfies its requirements?

Do unit test results show that each unit reproduces identical results given identical input data?

Have the testers ensured that documentary evidence exists to demonstrate satisfactory completion of the unit testing task?

Are the code qualities to be tested, and the method of testing, clearly specified in the unit test plan?

Have unit test results been evaluated to ensure adequate test coverage of units?

Do unit test results show that each logical path within the routine was tested (branch coverage)?

Do unit test results show that each loop within each routine was tested (loop coverage)?

If for some tests complete coverage is impractical, is there justification which shows that such lack of completeness cannot compromise safety?

Do unit test results show what will happen if actual input values exceed the design specifications in terms of values and frequency of occurrence?

Property: Unit Testing Results

Were coding errors which were detected during testing recorded?

Are unit test results documented?

Have all needed corrective actions been identified and documented which will remove the deficiencies in the code?

Have all deficiencies in the units tested been formally discussed with the development team and formally documented?

Is there convincing evidence that any coding errors which were detected during unit testing have been corrected and all necessary documentation updated?

Property: Unit Testing Team

Were the people that carried out the unit testing known by name and do they understand their jobs?

Were the verifiers well qualified to undertake the verification?

Product: CM Implementation Report

Property: Change Control Board

Do procedures exist that ensure that no safety-related code changes take place without formal approval of the Change Control Board?

Does the configuration management system control the safety impact of changes?

Who are the members of the Change Control Board?

Property: Configuration Baseline

Is there a traceability matrix showing for each code element the design element(s) from which it flows?

Is the current location and person responsible for each code configuration item?

Is the status of each code configuration item recorded?

Does a configuration baseline exist for code elements and code analyses and software tests performed?

Are all safety critical code configuration items labeled as such?

Are all code configuration items uniquely identified with an item code (or name) and a version number?

Property: Configuration Manager

Who is the configuration manager?

Is the configuration manager well qualified?

Is the actual software under code control?

Does the configuration management system ensure that a code configuration item can be released for change to only one person at a time?

Does the configuration management system ensure that only approved versions of code configuration items are made available for use in validation and installation?

Does the configuration management system include arrangements for disaster protection and protection from subversion and sabotage of the code configuration items?

Property: Problem Reporting and Change Management

Are all anomaly reports, their resolutions, any resulting change requests and their resolutions archived for later retrieval?

Does a means exist to ensure that all reported anomalies are resolved and the resolutions documented?

Does an anomaly reporting system exist for recording all identified anomalies and problems with the software code?

Do procedures exist to assess the impact of requested code changes on the software design and software requirements?

Does a status accounting method exist for determining the status of all anomaly reports and change requests?

Product: Integration Safety Analysis

Property: Integration Safety Analysis

Has the build procedure been analyzed to ensure that no hazards have been

Has the build information been analyzed to ensure that no hazardous events can occur?

Property: Integration Safety Analysis Results

Is there documented evidence that all specified corrective actions have actually taken place?

Have all required corrective actions been identified and documented which will obviate any safety-related deficiencies identified during software build operations?

Was the safety analysis activity itself well documented?

Property: Safety Documentation and Records

Are all build documents which have a safety impact under configuration control?

Is the person responsible for software safety build records known by name and does he understand his job?

Are all necessary build safety records under configuration control?

Do the build safety records identify the means used to track each hazard, the means of handling the hazard and the status of the hazard through the software build activities?

Property: Safety Organization and Responsibility

Does a single individual have overall responsibility for the conduct of the Software Safety Analysis?

Were sufficient resources made available to carry out the Software Safety Analysis?

Are the formal lines of communication for the Software Safety Analysis documented?

Were the analysts that carried out the Software Safety Analysis well qualified to undertake the analysis?

Who are the analysts that carried out the Software Safety Analysis?

Does the software safety organization have the authority to enforce software build activity compliance with system safety requirements and practices?

Product: V&V Integration Analysis and Report

Property: Review - General

Have the verifiers ensured that the system build documents accurately reflect the actual process of building the integrated system?

Have the verifiers seen documentary evidence to indicate that formal reviews of the software integration have been undertaken?

Are the software integration qualities to be verified, and the method of verification, clearly specified in the V&V plan?

Was the documentation provided to the verifiers sufficient for successful completion of the verification task?

Property: Review - Integration Analysis

Have the verifiers analyzed software integration elements related to security by suitably rigorous methods?

Have the verifiers ensured that the integrated software is compatible with the target hardware?

Have the verifiers analyzed software integration elements related to reliability by suitably rigorous methods?

Have the verifiers analyzed software integration elements related to safety by suitably rigorous methods?

Have the verifiers analyzed software integration elements related to timing and sizing by suitably rigorous methods?

Have the verifiers analyzed software integration elements related to functionality by suitably rigorous methods?

Have the verifiers analyzed software integration elements related to instrumentation interfaces by suitably rigorous methods?

Have the verifiers analyzed software integration elements related to operator interfaces by suitably rigorous methods?

Have the verifiers analyzed software integration elements related to robustness by suitably rigorous methods?

Property: Review - Integration Qualities

Have the verifiers ensured that the software integration was performed correctly?

Have the verifiers ensured that the integration is consistent with the implementation?

Have the verifiers ensured that the software integration is internally consistent?

Have the verifiers ensured that the software integration elements can be traced forward to software validation tests?

Have the verifiers ensured that the reliability, robustness, safety, security and timing requirements have been met in the integrated software system?

Have the verifiers ensured that the software integration description (in build documents) is clear?

Property: Review Results

Have all deficiencies in the integration elements or in the integration activity identified by the verifiers been formally discussed with the development team, and formally documented?

Have all required corrective actions been identified and documented which will remove any deficiencies in the integration activity?

Is there convincing evidence that the software integration reviews have covered all standards and procedures applicable to the integration effort?

Is there convincing evidence that all specified corrective actions have actually taken place and all necessary documentation updated?

Was the verification activity itself well documented?

Property: Review Team

Were the people that carried out the integration review known by name and do they understand their jobs?

Were the verifiers well qualified to undertake the verification?

Property: Testing Activity

Do integration test results show what will happen if actual input values exceed the design specifications in terms of values and frequency of occurrence?

Have the testers ensured that documentary evidence exists to demonstrate satisfactory completion of the integration testing task?

Are the integration qualities to be tested, and the method of testing, clearly specified in the integration test plan?

Is there a formal description of the integration test cases, test inputs and test results?

Have the software components been tested to ensure that each satisfies its requirements?

Have integration test results been evaluated to ensure test coverage of components?

Do integration test results show that each component reproduces identical results given identical input data?

Property: Testing Results

Have all deficiencies in the components tested been formally discussed with the development team and formally documented?

Have all needed corrective actions been identified and documented which will remove the deficiencies in the components?

Were errors which were detected during integration testing recorded?

Are integration test results documented?

Is there evidence that any errors which were detected during integration testing have been corrected and all necessary documentation updated?

Property: Testing Team

Were the verifiers well qualified to undertake the verification?

Were the people that carried out the integration testing known by name and do they understand their jobs?

Product: CM Integration Report

Property: Change Control Board

Who are the members of the Change Control Board?

Do procedures exist that ensure that no safety-related changes to the build procedures take place without formal approval of the Change Control Board?

Does the configuration management system control the safety impact of changes?

Property: Configuration Baseline

Are all safety-critical build configuration items labeled as such?

Is the current location and person responsible for each build configuration item recorded?

Is the status of each build configuration item recorded?

Does a configuration baseline exist for the software build activity and the tests performed on the results of the build activity?

Are all build configuration items uniquely identified with an item code (or name) and a version number?

Property: Configuration Manager

Who is the configuration manager?

Is the configuration manager well qualified?

Are the build procedures and files under configuration control?

Does the configuration management system ensure that a build configuration item can be released for change to only one person at a time?

Does the configuration management system ensure that only approved versions of build configuration items are made available for use in software, computer and application system validation and installation?

Does the configuration management system include arrangements for disaster protection and protection from subversion and sabotage of the build configuration items?

Property: Problem Reporting and Change Management

Does a status accounting method exist for determining the status of all anomaly reports and change requests?

Do procedures exist to assess the impact of requested changes to build configuration items on the software requirements, design and code?

Does an anomaly reporting system exist for recording all identified anomalies and problems with the software build configuration items?

Are all anomaly reports, their resolutions, any resulting change requests, and their resolution archived for later retrieval?

Does a means exist to ensure that all reporting anomalies are resolved and the resolutions documented?

Activity: Validation

Product: Validation Safety Analysis

Property: Safety Documentation and Records

Are all validation documents which have a safety impact under configuration control?

Do the validation safety records identify the means used to track each hazard, the means of handling the hazard, and the status of the hazard through the software validation activities?

Are all necessary validation safety records under configuration control?

Is the person responsible for software safety validation records known by name and does he understand his job?

Property: Safety Organization and Responsibility

Were sufficient resources made available to carry out the Software Safety Analysis?

Does a single individual have overall responsibility for the conduct of the Software Safety Analysis?

Does the software safety organization have the authority to enforce software compliance with system safety requirements and practices?

Are the formal lines of communication for the Software Safety Analysis documented?

Were the analysts that carried out the Software Safety Analysis well qualified to undertake the analysis?

Who are the analysts that carried out the Software Safety Analysis?

Property: Validation Hazards Analysis

Has the entire software system been analyzed to ensure that no hazards have been introduced?

Have the software requirements, design, code and integration been analyzed to ensure that no hazardous event can occur?

If a conflict exists between software and system safety requirements, have mitigation measures been identified and carried out to resolve the conflict?

Has the entire software system been analyzed to ensure that no hazards have increased in severity or frequency due to the software system?

Has the entire software system been analyzed to ensure that the software system does not interfere with the system safety requirements?

Property: Validation Safety Analysis

Has non-critical software been analyzed to provide adequate confidence that it does not adversely affect the function of safety-critical software?

Is there convincing evidence that the software will execute within the specified timing and sizing constraints under all operating modes?

Is there convincing evidence that correct interface compatibility of safety-critical software elements with each other and with external hardware and software exists?

Have the safety analysts evaluated the software system for data and control flow among modules?

Is there convincing evidence that the software complies with system safety criteria?

Have the safety analysts evaluated the safety-critical portions of the software system for proper error default handling for inappropriate or unexpected data in the input data stream?

Is there convincing evidence that no single or multiple combinations of software errors or input conditions can cause the application system to operate in a hazardous manner?

Is there convincing evidence that no combination of independent, dependent or interdependent events could cause the system to operate in a hazardous manner?

Property: Validation Safety Analysis Results

Have all required corrective actions been identified and documented which will obviate any safety-related deficiencies in the software?

Was the safety analysis activity itself well-documented?

Have all safety-related deficiencies in the software identified by analysts been formally discussed with the development team and formally documented?

Is there evidence that all specified corrective actions have actually taken place?

Product: V&V Validation Analysis and Test Report

Property: Review - General

Was documentation provided to the validators showing that formal reviews of the entire software system have been successfully completed?

Was the documentation provided to the validators sufficient for successful completion of the validation task?

Are the software qualities to be validated, and the method of validation, clearly specified in the V&V plan?

Property: Review - Validation Analysis

Have the validators analyzed the completed software elements related to safety by suitably rigorous methods?

Have the validators analyzed the completed software elements related to operator interfaces by suitably rigorous methods?

Have the validators analyzed the completed software elements related to instrumentation interfaces by suitably rigorous methods?

Have the validators analyzed the completed software elements related to functionality by suitably rigorous methods?

Have the validators analyzed the completed software elements related to security by suitably rigorous methods?

Have the validators analyzed the completed software elements related to robustness by suitably rigorous methods?

Have the validators analyzed the completed software elements related to reliability by suitably rigorous methods?

Have the validators analyzed the completed software elements related to timing and sizing by suitably rigorous methods?

Property: Review - Validation Qualities

Have the validators ensured that the completed software satisfies all requirements in the SRS?

Have the validators ensured that the completed software meets all system requirements?

Have the validators ensured that the completed software is consistent with the Software Requirements Specification?

Have the validators ensured that the completed software is internally consistent?

Have the validators ensured that the software system, as built, is complete?

Have the validators ensured that the reliability, robustness, safety, security and timing requirements have been met in the completed software?

Have the validators ensured that the software validation elements can be traced forward to system acceptance tests?

Have the validators ensured that the software validation elements can be traced forward to software installation tests?

Property: Review Results

Have all deficiencies identified by the validators been formally discussed with the development team, and formally documented?

Is there convincing evidence that any specified corrective actions have actually taken place and all appropriate documentation updated?

Is there convincing evidence that the software validation reviews have covered all standards and procedures applicable to the software?

Was the validation activity itself well documented?

Have all required corrective actions been identified and documented which will remove any deficiencies discovered during validation?

Property: Review Team

Were the people that carried out the software validation known by name and do they understand their jobs?

Were the validators well qualified to undertake the validation?

Property: Testing Activity

Has the entire software system been tested to ensure that it satisfies its requirements?

Does the test environment simulate real plant operating conditions?

Are all normal, steady state, abnormal and accident conditions included in the validation tests?

Have the testers ensured that documentary evidence exists to demonstrate satisfactory completion of the validation testing task?

Are the software qualities to be tested, and the method of testing, clearly specified in the validation test plan?

Is there a formal description of validation test cases, test inputs and test results?

Do validation test results show what will happen if actual input values exceed the software requirements specifications in terms of values and frequency of occurrence?

Do validation test results show that the software reproduces identical results given identical input data and identical states?

Do the test cases thoroughly test the timing performance and functional requirements of the complete system?

Have validation test results been evaluated to ensure test coverage of the software?

Was the validation test hardware environment consistent with that which will be used in the plant?

Has the complete system been performance tested under the most demanding conditions specified in the system design description?

Property: Testing Results

Is there convincing evidence that any errors which were detected during validation testing have been corrected and the necessary documentation updated?

Is there convincing evidence that all errors detected during testing were recorded?

Are validation test results documented?

Have all deficiencies in the software tested been formally discussed with the development team and formally documented?

Have all needed corrective actions been identified and documented which will remove the deficiencies in the software?

Property: Testing Team

Were the people that carried out the validation testing known by name and do they understand their jobs?

Were the test personnel well qualified to undertake the validation?

Product: CM Validation Report

Property: Change Control Board

Who are the members of the Change Control Board?

Does the configuration management system control the safety impact of changes?

Do procedures exist that ensure that no safety-related changes to requirements, design or code take place without formal approval of the Change Control Board?

Property: Configuration Baseline

Is the status of each configuration item recorded?

Are all configuration items used during validation uniquely identified with an item code (or name) and a version number?

Is the current location and person responsible for each configuration item used during validation recorded?

Are all safety-critical configuration items labeled as such?

Are all review, inspection and test plans, procedures, cases, data and results used or produced during validation under configuration control?

Is there a traceability matrix showing bi-directional traceability between requirements and build elements?

Does a configuration baseline exist for validating the software?

Property: Configuration Manager

Does the configuration management system include arrangements for disaster protection and protection from subversion and sabotage of the items undergoing validation?

Who is the configuration manager?

Is the configuration manager well qualified?

Are all elements required for validation under configuration control?

Does the configuration management system ensure that no configuration item can be released for change while it is undergoing validation?

Does the configuration management system ensure that only approved versions of configuration items are made available for validation?

Property: Problem Reporting and Change Management

Do procedures exist for assess the impact of requested changes on the software requirements, design and code?

Are all anomaly reports, their resolutions, and resulting change requests and their resolutions archived for later retrieval?

Does a means exist to ensure that all reported anomalies are resolved and the resolutions documented?

Does an anomaly reporting system exist for recording all identified anomalies and problems detected during validation?

Does a status accounting method exist for determining the status of all anomaly reports and change requests?

Property: Security

Can it be shown that the installation tables are protected from unauthorized changes?

Can it be shown that the installation tables introduce no new security threats into the safety systems?

Property: Traceability

Can the configuration tables be traced backwards to the code elements that require the configuration data?

Property: Verifiability

Is it possible to analyze, review or test each element of the configuration tables for correctness prior to operation?

Is it possible to analyze, review or test each element of the configuration tables for correctness periodically during operation?

Product: V&V Installation Analysis and Test Report

Property: Review - General

Was the documentation provided to the verifiers sufficient for successful completion of the installation task?

Are the software installation qualities to be verified, and the method of verification, clearly specified in the V&V plan?

Was documentation provided to the verifiers showing that formal reviews of the software installation have been successfully completed?

Property: Review - Installation Analysis

Have the verifiers analyzed the completed software installation elements related to robustness by suitably rigorous methods?

Have the verifiers analyzed software installation elements related to operator interfaces by suitably rigorous methods?

Have the verifiers analyzed software installation elements related to instrumentation interfaces by suitably rigorous methods?

Have the verifiers analyzed software installation elements related to timing and sizing by suitably rigorous methods?

Have the verifiers analyzed the completed software installation elements related to reliability by suitably rigorous methods?

Have the verifiers analyzed the completed software installation elements related to security by suitably rigorous methods?

Have the verifiers analyzed the completed software installation elements related to safety by suitably rigorous methods?

Have the verifiers analyzed software installation elements related to functionality by suitably rigorous methods?

Property: Review -Installation Qualities

Have the verifiers ensured that the reliability, robustness, safety, security and timing requirements have been met by the installed software?

Have the verifiers ensured that the software installation description is clear?

Have the verifiers ensured that the completed software meets all system requirements?

Property: Review Results

Is there convincing evidence that all specified corrective actions have actually taken place and the necessary documentation updated?

Was the verification activity itself well documented?

Have all required corrective actions been identified and documented which will remove any deficiencies in the software?

Have all deficiencies in the software identified by the verifiers been formally discussed with the development team, and formally documented?

Property: Review Team

Were the verifiers well qualified to undertake the verification?

Were the people that carried out the installation verification known by name and do they understand their jobs?

Property: Testing Activity

Have installation test results been evaluated to ensure test coverage of the software?

Do the installation test cases thoroughly test the timing performance and functional requirements of the installed system?

Are the software qualities to be tested, and the method of testing, clearly specified in the installation test plan?

Is there a formal description of installation test cases, test inputs and test results?

Do installation test results show what will happen if actual input values exceed the requirements specifications in terms of values and frequency of occurrence?

Are all normal, steady state, abnormal and accident conditions included in the installation tests?

Have the testers ensured that documentary evidence exists to demonstrate satisfactory completion of the testing task for the installation?

Does the installation test environment simulate real plant operating conditions?

Are all site-specific peculiarities taken into account during installation testing?

Has the installed software been tested to ensure that it still satisfies its requirements?

Do installation test results show that the software reproduces identical results given identical input data and identical states?

Has the installed system been performance tested under the most demanding conditions specified in the system design?

Was the installation test hardware environment the same as that which was used in the validation testing?

Property: Testing Results

Have all needed corrective actions been identified and documented which will remove the deficiencies in the code?

Is there convincing evidence that all errors detected during testing were recorded?

Are installation test results documented?

Is there convincing evidence that all errors detected during installation testing have been corrected and the necessary documentation updated?

Have all deficiencies in the software tested been formally discussed with the development team and formally documented?

Property: Testing Team

Were the people that carried out the installation testing known by name and do they understand their jobs?

Were the test personnel well qualified to undertake the installation testing?

Product: CM Installation Report

Property: Change Control Board

Who are the members of the Change Control Board?

Do procedures exist that ensure that no safety-related changes that place without formal approval of the Change Control Board?

Does the configuration management system control the safety impact of changes?

Property: Configuration Baseline

Is the status of each installation configuration item recorded?

Are all installation configuration items uniquely identified with an item code (or name) and a version number?

Does a configuration baseline exist for all software and associated documentation required for installation?

Are all safety-critical installation configuration items labeled as such?

Is the current location and person responsible for each installation configuration item recorded?

Property: Configuration Manager

Does the configuration management system ensure that installed software is under the control of the configuration manager?

Does the configuration management system ensure that only approved versions of software and documentation can be released to users?

Is the software being installed, and all associated documentation, under configuration control?

Is the configuration manager well qualified?

Who is the configuration manager?

Does the configuration management system include arrangements for disaster protection and protection from subversion and sabotage of installed configuration items?

Property: Problem Reporting and Change Management

Does an anomaly reporting system exist for recording all identified anomalies and problems that occur during installation?

Activity: Operations and Maintenance

Product: V&V Change Report

Property: Review - Change Analysis

Have the verifiers found convincing justification for inclusion in the changed software of any functions outside the scope of the requirements in the Software Requirements Specification?

Have the verifiers analyzed software change elements related to operator interfaces by suitably rigorous methods?

Have the verifiers analyzed software change elements related to safety by suitably rigorous methods?

Have the verifiers analyzed software change elements related to security by suitably rigorous methods?

Have the verifiers analyzed software change elements related to reliability by suitably rigorous methods?

Have the verifiers analyzed software change elements related to robustness by suitably rigorous methods?

Have the verifiers analyzed software change elements related to timing and sizing by suitably rigorous methods?

Have the verifiers analyzed software change elements related to instrumentation interfaces by suitably rigorous methods?

Have the verifiers analyzed software change elements related to functionality by suitably rigorous methods?

Property: Review - Change Qualities

Have the verifiers ensured that implementation of the software changes is feasible?

Have the verifiers ensured that the changed software is complete?

Have the verifiers ensured that the changed software satisfies the software requirements?

Have the verifiers ensured that the changed software is consistent with the Software Requirements Specification?

Have the verifiers ensured that the software documents remain unambiguous?

Have the verifiers ensured that the reliability, robustness, safety, security, and timing requirements continue to be met by the modified software?

Have the verifiers ensured that the changed software is internally consistent?

Property: Review - General

Was the documentation provided to the verifiers sufficient for successful completion of the verification task?

Are the software qualities to be verified, and the method of verification, clearly specified in the V&V plan?

Was documentation provided to the verifiers showing that formal reviews of the software modifications have been successfully completed?

Property: Review Results

Is there convincing evidence that the software change reviews have covered all requirements in the (possibly modified) Software Requirements Specification?

Is there convincing evidence that all specified corrective actions have actually taken place and the necessary documentation updated?

Is there convincing evidence that the software change reviews have covered all standards and procedures applicable to the software?

Was the verification activity itself well documented?

Have all deficiencies in the change elements identified by the verifiers been formally discussed with the development team, and formally documented?

Have all needed corrective actions been identified and documented which will remove any deficiencies in the changes?

Property: Review Team

Were the verifiers well qualified to undertake the review?

Were the people that carried out the change review known by name and do they understand their jobs?

Property: Testing Activity

Have the testers ensured that documentary evidence exists to demonstrate satisfactory completion of the testing task for the approved changes?

Has the entire software system been tested adequately to assure that it still satisfies its (possibly changed) requirements?

Do test results show that the software reproduces identical results given identical input data and identical states?

Do the test cases adequately test the timing performance and functional requirements of the modified system?

Are all normal, steady state, abnormal and accident conditions included in the tests?

Are the software qualities to be tested, and the method of testing, clearly specified in the test plan?

Is there a formal description of test cases, test inputs and test results?

Do test results show what will happen if actual input values exceed the (possibly modified) requirements specifications in terms of values and frequency of occurrence?

Have test results been evaluated to ensure test coverage of the software?

Has the changed system been performance tested under the most demanding conditions specified in the system design description?

Was the test hardware environment the same as that which will be used in the (possibly modified) plant?

Does the test environment simulate real plant operating conditions?

Are all site-specific peculiarities taken into account, so that the testing gives a true, credible, overall test of appropriate key characteristics?

Property: Testing Results

Are test results documented?

Were all errors detected during testing recorded?

Have all deficiencies in the software tested been formally discussed with the development team and formally documented?

Have all needed corrective actions been identified and documented which will remove the deficiencies in the software?

Is there convincing evidence that all errors detected during testing have been corrected and all necessary documentation updated?

Property: Testing Team

Were the people that carried out the unit testing known by name and do they understand their jobs?

Were the verifiers well qualified to undertake the verification?

Product: CM Change Report

Property: Change Control Board

Who are the members of the Change Control Board?

Does the configuration management system control the safety impact of changes?

Do procedures exist that ensure that no safety-related changes take place without formal approval of the Change Control Board?

Property: Problem Reporting and Change Management

Does an anomaly reporting system exist for recording all identified anomalies and problems with the software during operation?

Does an means exist to ensure that all reporting anomalies are resolved and the resolutions documented?

Are all anomaly reports, their resolutions, and resulting change requests, and their resolutions, archived for later retrieval?

Does a status accounting method exist for determining the status of all anomaly reports and change requests?

Do procedures exist to assess the impact of requested changes on the software requirements, design, code, integration, and installation?

LIST OF ACRONYMS

APS	Arizona Public Service Company
ASGT	Asymmetric steam generator transient
CEA	Control element assembly
CEAC	Control element assembly calculators
COLSS	Core operating limit supervisory system
CPC	Core protection calculator
CPCS	Core protection calculator system
DNBR	Departure from nucleate boiling ratio
Docs	Documents
ESFAS	Engineered safety features actuation system
FAT	Factory acceptance test
FCST	Four channel system test
FDR	Functional Design Requirements
FMEA	Failure modes and effects analysis
HDD	Hardware design description
HFAT	Hardware factory acceptance tests
HMI	Human/machine interface
HF	Human factors
ICS	Instrumentation and control systems
I/O	Input/output
LAR	License amendment request
LPD	Local power density
OCST	One channel system test
PVNGS	Palo Verde Nuclear Generating Station
PSAI	Plant specific action item
RCP	Reactor coolant pump
RCPSSS	Reactor coolant pump shaft speed sensor
RPS	Reactor protection system
RS	Reactor systems
RTM	Requirements traceability matrix
SCF	Single channel facility
SDD	System design description
SE	Safety evaluation
SPM	Software program manual
SQA	Software quality assurance
SRS	Software requirements specification
SysRS	System requirements specification
TR	Topical report
UFSAR	PVNGS Updated Final Safety Analysis Report
VOPT	Variable overpower trip
V&V	Verification and validation

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

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