From: <Mark.J.Stofko@us.westinghouse.com>
To: <agh1@nrc.gov>
Date: 6/21/05 2:03PM
Subject: Draft NRC Review Plans

Allen,

It was a pleasure to meet you during the ACRS I&C Subcommittee Meeting last week. As we discussed, I have been working on the preparation of a proposed NRC review plan for the AP1000 Protection and Safety Monitoring System. This plan has evolved as a result of discussions between NRC and NEI regarding NEI 04-01, "Industry Guideline for Combined License Applicants Under 10 CFR Part 52." The draft plan is attached below, per your request.

We also discussed, my interest in closing out the one remaining open item in the Common Q safety evaluation, generic open item 7.8. This GOI relates to the "level 3 loop controllers" referenced in the Common Q topical report integrated solution, Appendix 4. The last time Westinghouse met with the staff on Common Q was at the White Flint office on December 4, 2003. The purpose of that meeting was to discuss changes to the Common Q Software Program Manual; but, we also had a brief discussion on what would be needed to close out GOI 7.8. I have discussed this briefly with Paul Loeser on March 8, 2005. I expect to have this additional material ready for submittal sometime during the third quarter of this year.

(See attached file: PMS NRC Review Plan-Rev D.doc)

Best regards,
-Mark

Mail Envelope Properties (42B85650.2B7 : 19 : 17079)

Subject:	Draft NRC Review Plans
Creation Date:	6/21/05 2:02PM
From:	<Mark.J.Stofko@us.westinghouse.com>
Created By:	Mark.J.Stofko@us.westinghouse.com

Recipients
nrc.gov
owf4_po.OWFN_DO
AGH1 (Allen Howe)

Post Office	**Route**
owf4_po.OWFN_DO	nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	1249	06/21/05 02:02PM
PMS NRC Review Plan-Rev D.doc		103936
Mime.822	145214	

Options

Expiration Date:	None
Priority:	Standard
Reply Requested:	No
Return Notification:	None
Concealed Subject:	No
Security:	Standard

AP1000 Protection and Safety Monitoring System (PMS)
NRC Review Plan
Revision D

Purpose:

The purpose of this document is to propose a schedule for the review of AP1000 PMS design. Review dates are selected, where meaningful NRC reviews can be accomplished based on the NRC's plan for technical review in the instrumentation and control systems area.

A schedule of proposed human factors engineering (HFE) reviews is being prepared in a separate document.

NRC Review Process:

The NRC will confirm that the as-built computer-based plant I&C system conforms to the certified design. The design acceptance criteria will be verified to be met as part of the I&C system Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC). The ITAAC reviews will be performed by the NRC prior to fuel load at specified points in the system lifecycle.

The NRC staff will use a two-part approach for the review of the PMS as follows:

- Detailed functional review at the block diagram level to ensure appropriate implementation of NRC requirements related to postulated single failures, common-mode failures, appropriate signal isolation, and other aspects of NRC review. This review will establish the detailed functional requirements for the I&C systems.
- Review of the implementation of digital I&C systems to meet the functional system requirements. Review points will be selected based on the system lifecycle process to verify that the implementation is proceeding in accordance with the design certification. A review will be done for each phase of the I&C system software and hardware development process.

The review guidance provided in SRP Chapter 7, Rev. 4, 1997, will be used by the staff in review of the I&C system design, installation and operation. Of particular note is the guidance in Appendix 7-A, Branch Technical Position (BTP) 14, "Guidance on Software Reviews for Digital Computer-Based I&C Systems" which applies to the plant-specific software application.

Technical Review Plan:

Table 1 below provides the review schedule. It includes the proposed review date for each lifecycle phase and a list of documents that will be available for the staff's review. The list of documents is correlated with the list of reference topics provided in BTP 14, Figure 7-A-1. Review dates are specified in "Months ARO". The phase definitions identified in parenthesis in Column 2 are consistent with the Common Q design terminology.

Table 2 below shows the relationship between the system lifecycle phases as defined in BTP 14, the Common Q design terminology, and the AP1000 Design Control Document (DCD).

Tables 3A through 3E below define the scope of each review with specific references to ITAACs that are included in the AP1000 DCD. These tables provide the details of each planned review including a cross reference of the contents of each available document with the design commitment and associated acceptance criteria that it attempts to satisfy.

Table 1. Review Schedule

Review Date (Months ARO)	Completion of System Lifecycle Phase	BTP 14, Figure 7-A-1 Reference Topics	Available Documents
12	Design Requirements (Concept Phase)	Software Management Plan Software Development Plan Software QA Plan Integration Plan Installation Plan Maintenance Plan Training Plan Operations Plan Software Safety Plan Software V&V Plan Software CM Plan	Software Program Manual Project Quality Plan Commercial Grade Dedication Plan AP1000 V&V Plan System Test Plan CMRR-Concept
26	System Definition (Requirements Analysis Phase)	Requirements Specifications Requirements Safety Analysis V&V Requirements Analysis Report CM Requirements Analysis Report	Generic Safety System Requirements AP1000 Safety System Requirements (SyDR) System Architecture Drawings Functional Requirements System Design Specification (incl HW Rqmts) Software Requirements Specification

Table 1. Review Schedule

Review Date (Months ARO)	Completion of System Lifecycle Phase	BTP 14, Figure 7-A-1 Reference Topics	Available Documents
			System Interface Requirements Requirements Phase V&V Report Requirements Phase RTM CMRR-Requirements
40	Hardware and Software Development, consisting of hardware and software design and implementation (Design Phase & Implementation Phase)	Design Specifications Hardware & Software Architecture Design Safety Analysis V&V Design Analysis Report CM Design Report Code Listings Code Safety Analysis V&V Implementation Analysis & Test Report CM Implementation Report	Hardware Design Drawings Custom Software Element Design Specifications Reusable Software Type Specifications Module/Unit Test Procedures Module/Unit Test Reports BPL Software Design Description LCL Software Design Description ITP Software Design Description ILC Software Design Description MUX Software Design Description MTP Software Design Description Design and Implementation Phase V&V Reports Design and Implementation Phase RTM CMRR-Design and Implementation

Table 1. Review Schedule

Review Date (Months ARO)	Completion of System Lifecycle Phase	BTP 14, Figure 7-A-1 Reference Topics	Available Documents
TBD	System Integration and Test (Test Phase)	System Build Documentation Integration Safety Analysis V&V Integration Analysis & Test Report CM Integration Report Validation Safety Analysis V&V Validation Analysis & Test Report CM Validation Report	
TBD	Installation (Installation and Checkout Phase)	Operations Manuals Installation Configuration Tables Maintenance Manuals Training Manuals Installation Safety Analysis V&V Installation Analysis & Test Report CM Installation Report	

Table 2. Lifecycle Phase Relationships

BTP 14, Figure 7-A-1	Common Q Design Terminology	DCD Table 2.5.2-8, Item 11
Planning Activities	Concept	Design requirements phase, may be referred to as conceptual or project definition phase
Requirements Activities	Requirements Analysis	System definition phase
Design Activities	Design	Hardware and software development phase, consisting of hardware and software design and implementation
Implementation Activities	Implementation or Coding	
Integration Activities	Test	System integration and test phase
Validation Activities		
Installation Activities	Installation and Checkout	Installation phase
Operations & Maintenance Activities	Operation and Maintenance	
	Retirement	

Table 3A. Design Requirements Phase Review (12 Months ARO)

DCD Table 2.5.2-8 ITAAC Reference	Design Commitment	Document Reference	Acceptance Criteria Satisfied
Item 11.a	PMS hardware and software is developed using a planned design process which provides for specific design documentation and reviews during the design requirements phase. This may be referred to as the conceptual or project definition phase.		A report exists and concludes that the process defines the organizational responsibilities, activities, and configuration management control for the establishment of plans and methodologies.

Table 3B. System Definition Phase Review (26 Months ARO)

DCD Table 2.5.2-8 ITAAC Reference	Design Commitment	Document Reference	Acceptance Criteria Satisfied
Item 11.b	PMS hardware and software is developed using a planned design process which provides for specific design documentation and reviews during the system definition phase.		A report exists and concludes that the process defines the organizational responsibilities, activities, and configuration management control for the specification of functional requirements.

Table 3C. Hardware and Software Development Phase Review (40 Months ARO)

DCD Table 2.5.2-8 ITAAC Reference	Design Commitment	Document Reference	Acceptance Criteria Satisfied
Item 11.c	PMS hardware and software is developed using a planned design process which provides for specific design documentation and reviews during the hardware and software development phase, consisting of hardware and software design and implementation.		A report exists and concludes that the process defines the organizational responsibilities, activities, and configuration management control for the documentation and review of hardware and software.

Table 3D. System Integration and Test Phase Review (TBD)

DCD Table 2.5.2-8 ITAAC Reference	Design Commitment	Document Reference	Acceptance Criteria Satisfied
Item 11.d	PMS hardware and software is developed using a planned design process which provides for specific design documentation and reviews during the system integration and test phase.		A report exists and concludes that the process defines the organizational responsibilities, activities, and configuration management control for the performance of system tests and the documentation of system test results.

Table 3E. Installation Phase Review (TBD)

DCD Table 2.5.2-8 ITAAC Reference	Design Commitment	Document Reference	Acceptance Criteria Satisfied
Item 11.e	PMS hardware and software is developed using a planned design process which provides for specific design documentation and reviews during the installation phase.		A report exists and concludes that the process defines the organizational responsibilities, activities, and configuration management control for the performance of installation tests and inspections.