SUPPLEMENTAL RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

APR1400 Design Certification

Korea Electric Power Corporation / Korea Hydro & Nuclear Power Co., LTD

Docket No. 52-046

RAI No.:	**261-8253**
SRP Section:	**07.01 – Instrumentation and Controls - Introduction**
Application Section:	**7.1**
Date of RAI Issue:	**10/20/2015**

Question No. 07.01-30

Describe how the Software Quality Assurance Plan relates to the APR1400 Quality Assurance Manual.

10 CFR 50.55a(h)(3) states, in part, that application filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. Clause 5.3 of IEEE Std 603-1991 requires safety system equipment to be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. Section 4, "Software Quality Assurance Plan," of Technical Report APR1400-Z-J-NR-14003, Rev. 0, “Software Program Manual,” describes the Software Quality Assurance Plan. However, it did not appear to describe the relationship between the Software Quality Assurance Plan and the APR1400 Quality Assurance Manual. Modify the APR1400 SPM to describe the relationship and interfaces between these two documents.

Response

To clarify that references to the “QAM” stated in the SPM Technical Report (TeR) are references to the APR1400 QAM (Reference 32 of the SPM TeR), the “Acronyms and Abbreviations” list will be revised as such.

Section 4.2.1 of the SPM Technical Report (TeR) describes the relationship between the Software Quality Assurance Plan (SQAP) and the APR1400 Quality Assurance Manual (QAM) as follows:

> Management of the SQAP is overseen by the managers of design team and V&V team. Organizationally, verification of the implementation of QA requirements is performed by the QA team in accordance with the QAM.

Other statements describing the relationship and interfaces between the SQAP and the QAM can be found in Section 4 of the SPM TeR.

Supplemental Response

The APR1400 QAM applies to all documents for the APR1400, including the SPM TeR. The SPM TeR applies to all software documents to be developed for the APR1400 I&C systems, including the SQAP for a specific I&C system for the APR1400.

Impact on DCD

There is no impact on the DCD.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical/Topical/Environmental Reports

The “Acronyms and Abbreviations” list of the SPM TeR will be revised as indicated on the attached markup.

QAM	~~quality assurance manual~~ ← APR1400 quality assurance manual
QIAS-N	qualified indication and alarm system – non-safety
QIAS-P	qualified indication and alarm system – P
RCPVMS	reactor coolant pump vibration monitoring system
RG	regulatory guide
RPCS	reactor power cutback system
RRS	reactor regulating system
RTM	requirements traceability matrix
SAT	site acceptance test(ing)
SBCS	steam bypass control system
SC	safety-critical
SCI	software configuration identification
SCM	software configuration management
SCMP	software configuration management plan
SCR	software change request
SDD	software design description
SDL	serial data link
SDN	safety system data network
SDOE	secure development and operational environment
SDP	software development plan
SInstP	software installation plan
SIntP	software integration plan
SMP	software management plan
SOE	sequence of event
SOMP	software operation and maintenance plan
SPADES+	safety parameter display and evaluation system plus
SPM	software program manual
SQAP	software quality assurance plan
SRS	software requirements specification
SSP	software safety plan
STP	software test plan
STrngP	software training plan
SVVP	software verification and validation plan
SysRS	system requirements specification
TER	test exception report

SUPPLEMENTAL RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

APR1400 Design Certification

Korea Electric Power Corporation / Korea Hydro & Nuclear Power Co., LTD

Docket No. 52-046

RAI No.:	**261-8253**
SRP Section:	**07.01 – Instrumentation and Controls - Introduction**
Application Section:	**7.1**
Date of RAI Issue:	**10/20/2015**

Question No. 07.01-31

Describe the software development lifecycle model that will be used to develop APR1400 safety-related I&C software.

10 CFR 50.55a(h)(3) states, in part, that application filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. Clause 5.3 of IEEE Std 603-1991 requires safety system equipment to be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. Section 4.8, "Tools, Techniques, and Methodologies," of Technical Report APR1400-Z-J-NR-14003, Rev. 0, “Software Program Manual,” states the use of the waterfall model of software development and testing techniques shall be employed. However, this is the only statement in the software program manual regarding the waterfall model. Based on recent experiences developing new nuclear power plant software, vendors use a cyclic model that incorporates several baselines of software that go through the various lifecycle phases multiple times versus a once-through development process such as the waterfall model. Will the APR1400 use a true waterfall model for software development or will it use a form of cyclic software development? Modify the APR1400 SPM to describe the type of software development lifecycle model that will be employed for the APR1400 safety-related software development.

Response

The SPM Technical Report (TeR) uses the life cycle phases of the waterfall model only as a framework, as does RG 1.152. Vendors can use their own lifecycle models provided that the required activities and tasks described in the SPM TeR are performed and the required outputs specified in the SPM TeR are provided. The statement describing the waterfall model in Section 4.8 of the SPM TeR will be removed to reflect this.

Supplemental Response

Section 4.8 will describe that the products developed in accordance with the SPM TeR are to use the life cycle phases of the waterfall model as a framework per RG 1.152.

Impact on DCD

There is no impact on the DCD.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical/Topical/Environmental Reports

Section 4.8 of the SPM TeR will be revised as indicated on the attached markup.

RAI 261-8253, 07.01-31

on the TER form in order to reproduce the problem. These steps shall be noted Sup. RAI 261-8253, 07.01-31 problem is not repeatable.

The extent of the retest shall be determined by the design team and V&V team based on the relative impact of the software change on the overall system operation. For SC and ITS class software, all changes require complete retest for the system or function, unless otherwise justified in writing including steps to ensure that new errors were not introduced.

4.7.2 Corrective Action

The design team and the V&V team shall establish, as a clear objective, the goal of resolving all test problems (via TERs) and review comments (via CRs) expeditiously to minimize the potential for unidentified effects during later life cycle phases.

The corrective action procedures used shall be based on the level of problem reported.

In addition, the design team shall adhere to the following corrective action methodology that:

- Problems are identified, evaluated, documented and, if required, corrected by the appropriate reporting mechanism (Section 4.7.1).
- Corrections or changes shall be controlled in accordance with the SCMP.
- Preventive actions and corrective actions are documented on the appropriate form and distributed to the design team.

Corrective actions shall be documented on TERs and CRs by the design team and shall be completed by the due date specified on the form.

4.8 Tools, Techniques, and Methodologies

During software development, a number of techniques will be used to help assure all software is designed, implemented, and documented in accordance with the objectives of building software which meets the requirements and which is maintainable over time in the most cost effective manner. The tools, techniques and methodologies employed in this process shall ensure that the software is verifiable from each phase of the project to the next.

Use of structured analysis and design techniques and methodologies helps to define and design systems from the "top-down", i.e., based upon the broad requirements of the end user. The data flow diagram describes only the functions themselves, without any mention of how or by what components they will be implemented. Structured methods also provide techniques and guidelines to aid in the software design. A structure chart breaks down functions into a sequence of tasks (corresponding to procedures or subroutines), with the input and output parameters shown. While the decomposition is left to the designer, the design methods recommend high cohesion with each software module (i.e., each software module performs only a single function) and simple coupling among the software modules.

~~The use of the waterfall model of software development and testing techniques shall be employed to help assure that the requirements are correctly translated into design and implementation products.~~

The use of automated tools for SCM shall be employed to the maximum extent possible.

The software development organization may use its own life cycle model provided that, within its work scope, the required activities and tasks described in this report are performed and the required outputs specified in this report are provided.

SUPPLEMENTAL RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

APR1400 Design Certification

Korea Electric Power Corporation / Korea Hydro & Nuclear Power Co., LTD

Docket No. 52-046

RAI No.:	**261-8253**
SRP Section:	**07.01 – Instrumentation and Controls - Introduction**
Application Section:	**7.1**
Date of RAI Issue:	**10/20/2015**

Question No. 07.01-32

Describe the scope of the factory and site acceptance testing.

10 CFR 50.55a(h)(3) states, in part, that application filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. Clause 5.3 of IEEE Std 603-1991 requires safety system equipment to be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. Section 13, "Software Test Plan," of Technical Report APR1400-Z-J-NR-14003, Rev. 0, “Software Program Manual,” describes the software test plan, but does not describe the scope of systems that will be tested in the factory and site acceptance tests. For example, in the factory acceptance test, will the Plant Protection System be tested alone or will it be tested while connected to other I&C systems? Also, will tests be conducted with the safety and non-safety I&C systems connected. Modify the APR1400 SPM to identify the scope of systems that will be connected and tested in an integrated fashion for the factory and site acceptance tests.

Response

The SPM Technical Report (TeR) is intended to describe generic software engineering process. The scope of systems to be tested will be described as the items being tested in system-specific planning document for the testing. This is described in Section 13.4.1 of the SPM TeR as follows:

> The purpose of a test plan is to specify scope, approach, resources, and schedule of the testing activities for the software system. The test plan shall identify the items being tested, the features to be tested, the testing tasks to be performed, the personnel responsible for each task, and the associated risks.

Supplemental Response

The system testing (Section 13.3.3 of the SPM TeR) will verify that the software products meet the system requirements for the software while the integration testing (Section 13.3.2 of the SPM TeR) will verify that the software products meet the software requirements.

The SPM TeR will be revised to clearly state that the actual planning documents for testing are to describe the scope of the system/software to be tested.

Impact on DCD

There is no impact on the DCD.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical/Topical/Environmental Reports

Section 13.4.1 of the SPM TeR will be revised as indicated on the attached markup.

Sup. RAI 261-8253, 07.01-32

13.3.3 System Testing

The objective of system testing (factory acceptance testing; FAT) is to verify that the entire executable code, including newly developed code, modified code, and any commercial or existing code, that have been integrated with the target hardware, successfully functions and fulfills all the system requirements related to the software.

A comprehensive system test is conducted for any safety I&C system. The system test evaluates the system performance in an environment that is real, or as close to real as can reasonably be created. Typically this environment is at the factory. A fully integrated system with the hardware and software, that is similar to the site environment, is required. The system test process demonstrates and proves correct and successful implementation of safety requirements and correct functioning of hardware-software combined system.

System testing includes the following tasks:

TS

System test procedures are prepared based upon the requirements of the design documents. The test specifications (if any) and procedures include test cases including the full range of data expected of the system.

13.3.4 Site Acceptance Testing

The objective of site acceptance testing is to confirm that the system was not damaged during shipment or installation.

The utility has the responsibility of site acceptance testing.

13.4 Test Documentation

All of formally issued test documentation shall be signed-off by all designated stakeholders.

All of formally issued test documentation shall be maintained as quality records and under the control of the SCM system.

13.4.1 Test Plan

The purpose of a test plan is to specify scope, approach, resources, and schedule of the testing activities for the software system. The test plan shall identify the items being tested, the features to be tested, the testing tasks to be performed, the personnel responsible for each task, and the associated risks.

A test plan shall contain the following information:

The test plan shall describe the scope of the system/software to be tested.