STP Nuclear Operating Company

South Texas Project Electric Generating Station 4000 Avenue F – Suite A Bay City, Texas 77414

September 24, 2009
U7-C-STP-NRC-090162

U. S. Nuclear Regulatory Commission
Attention: Document Control Desk
One White Flint North
11555 Rockville Pike
Rockville MD 20852-2738

South Texas Project
Units 3 and 4
Docket Nos. 52-012 and 52-013
<u>Response to Request for Additional Information</u>

Attached are the responses to the NRC staff questions included in Request for Additional Information (RAI) letter numbers 252, 254, 255, 256, 257, and 258 related to Combined License Application (COLA) Part 2, Tier 1 ITAAC and Tier 2, Chapter 7, Instrumentation and Controls. This submittal completes the responses to these RAI letters.

Attached are responses to the RAI questions listed below:

RAI 07-5
RAI 07-6
RAI 07.01-14
RAI 07.07-10
RAI 07.09-8
RAI 07.02-2
RAI 07.02-3
RAI 07.02-4
RAI 07.02-5
RAI 14.03.05-4
RAI 14.03.05-5
RAI 14.03.05-6
RAI 14.03.05-7
RAI 14.03.05-8

When a change to the COLA is indicated, it will be incorporated into the next routine revision of the COLA following NRC acceptance of the RAI response.

There are no commitments in this letter.

STI 32541312

D091
NRO

If you have any questions, please contact me at (361) 972-7206, or Bill Mookhoek at (361) 972-7274.

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

Executed on 9/24/09

MA McBurnett

Mark A. McBurnett
Vice President, Oversight and Regulatory Affairs
South Texas Project Units 3 & 4

jwc

Attachments:

1. RAI 07-5
2. RAI 07-6
3. RAI 07.01-14
4. RAI 07.07-10
5. RAI 07.09-8
6. RAI 07.02-2
7. RAI 07.02-3
8. RAI 07.02-4
9. RAI 07.02-5
10. RAI 14.03.05-4
11. RAI 14.03.05-5
12. RAI 14.03.05-6
13. RAI 14.03.05-7
14. RAI 14.03.05-8

cc: w/o attachment except*
(paper copy)

Director, Office of New Reactors
U. S. Nuclear Regulatory Commission
One White Flint North
11555 Rockville Pike
Rockville, MD 20852-2738

Regional Administrator, Region IV
U. S. Nuclear Regulatory Commission
611 Ryan Plaza Drive, Suite 400
Arlington, Texas 76011-8064

Kathy C. Perkins, RN, MBA
Assistant Commissioner
Division for Regulatory Services
Texas Department of State Health Services
P. O. Box 149347
Austin, Texas 78714-9347

Alice Hamilton Rogers, P.E.
Inspections Unit Manager
Texas Department of State Health Services
P.O. Box 149347
Austin, TX 87814-9347

C. M. Canady
City of Austin
Electric Utility Department
721 Barton Springs Road
Austin, TX 78704

*Steven P. Frantz, Esquire
A. H. Gutterman, Esquire
Morgan, Lewis & Bockius LLP
1111 Pennsylvania Ave. NW
Washington D.C. 20004

*George F. Wunder
*Adrian Muniz
*Stacy Joseph
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852

(electronic copy)

*George F. Wunder
*Adrian Muniz
*Stacy Joseph
Loren R. Plisco
U. S. Nuclear Regulatory Commission

Steve Winn
Eddy Daniels
Joseph Kiwak
Nuclear Innovation North America

Jon C. Wood, Esquire
Cox Smith Matthews

J. J. Nesrsta
R. K. Temple
Kevin Pollo
L. D. Blaylock
CPS Energy

RAI 07-5

QUESTION:

COLA FSAR Tier 1 Section 2.7.5 design description has been replaced in its entirety based on STD DEP T1 3.4-1. In the design description for ECF, it is stated, "The ECFs are implemented through the use of divisionally dedicated networks and/or data links provided with the safety related digital system platforms. Some of the platforms use data links only or networks only and some of the platforms use a combination of both data links and networks." Whereas in the subsequent paragraph, it is stated, "Data communication is provided between redundant safety related divisions to support coincident logic functions. The data communication is implemented through fiber optic based data links to ensure interdivisional isolation." How does the interdivisional communication take place for the platforms that do not use data links? Also, define the terms "data link" and "network" and explain the differences.

RESPONSE:

Both the Reactor Trip and Isolation System (RTIS) and ESF Control and Logic System (ELCS) utilize data links for interdivision communication. ELCS utilizes a network within a division, but that network does not cross division boundaries.

The Reactor Trip and Isolation System (RTIS) utilizes only data links. A data link is defined as having a point to point communication connection between the sending unit and the receiving unit.

A network is defined as a communication method that connects multiple devices together to allow communication between the devices.

The ESF Logic and Control System (ELCS) utilizes an intra-division network to communicate between multiple processors and human-machine interfaces within a single division. The intra-division network communication is buffered from the ELCS controller by a communication module contained in the same rack that houses the ELCS controller. The intra-division communication module also performs communication diagnostics. The ELCS intra-division network is a deterministic network that utilizes a bus master. Each ELCS division includes an independent intra-division network. The intra-division network does not communicate outside the ELCS division. Each controller will send and receive periodic messages from the intra-division network communication modules. It allows communication between the control room safety displays, the Maintenance and Test Panel (MTP), and ELCS controllers for one division. This bus is used to communicate status and diagnostic data from the ELCS controllers for display on the safety displays and MTP. It is also used to communicate test signals and data from the MTP and control room safety displays to the ELCS controllers. Each ELCS division includes an independent intra-division network. The intra-division network does not communicate outside the ELCS division.

<u>High Speed Serial Link Communication</u>

Each ELCS controller contains two processors. One processor is dedicated to performing the safety functions. The second processor is responsible for performing the unidirectional high speed serial link communications. The safety function processor shares a dual ported memory with the communications processor to allow data exchange. The ELCS communication processor has two independent receive communication ports and one independent transmit port.

The ELCS utilizes a high speed serial link (HSL) to communicate Class 1E safety function actuation information. The HSL is a true broadcast link that meets the communication isolation requirements of IEEE-Std-7.4.3-2. The HSL is utilized in a multi-drop communication method. In this method the transmission source is sent to multiple fiber optic modems which convert the HSL signal to utilize fiber optic communication media. The identical unidirectional signals are then connected to multiple receivers. An example of multi-drop communication is the transmission of a single division's Digital Trip Function (DTF) output actuation status signals to the other three divisions of Safety Logic Functions (SLFs).

For STP 3&4, the HSL communication is utilized for the following ELCS communication paths:

- DTF remote I/O to DTF
- DTF to SLF
- SLF safety function actuation to SLF remote I/O

There is no COLA revision required as a result of this RAI response.

RAI 07-6

QUESTION:

Based on STD DEP T1 3.4-1, the applicant has revised COLA FSAR Tier 1 subsection A of Section 3.4 that provides design description of the proposed Safety System Logic and Control (SSLC). According to 10 CFR Part 52, Appendix A, Tier 1 information, such as, design descriptions, interface requirements, and site parameters are derived from Tier 2. The NRC staff is unable to locate the SSLC design details in COLA FSAR Tier 2 that would form the basis for the SSLC design description provided in COLA FSAR Tier 1 Section 3.4. The staff requests STPNOC to resolve this inconsistency.

RESPONSE:

The following text will be added to STP 3&4 COLA Part 2, Tier 2, Subsections 7.1S.1 and 7.1S.2, in a future COLA revision. This addition enhances and replaces the Subsections 7.1S.1, FPGA Based Platforms and 7.1S.2, Microprocessor Based Platforms, that were proposed in the STPNOC response to RAI 07.01-1, letter number U7-C-STP-NRC-090065, June 29, 2009.

7.1S Site Specific Instrumentation and Control Platforms

This site specific supplemental section provides platform information for safety-related instrumentation and control (I&C) systems.

7.1S.1 Field Programmable Gate Array Based Platforms

The Reactor Trip and Isolation System (RTIS) and the Neutron Monitoring Systems (NMS) are Non-Rewritable (NRW)-Field Programmable Gate Array (FPGA)-based systems. NRW-FPGA based systems are configurable logic devices that process digital signals in a deterministic way.

7.1S.1.1 Reactor Trip and Isolation System

The Reactor Trip and Isolation System (RTIS) provides the logic and control functions for the Reactor Protection System (RPS) and Main Steam (MS) isolation. RPS is described in greater detail in Section 7.2. The RTIS is one part of the Safety System Logic and Control (SSLC).

The RTIS consists of modules for Digital Trip Functions (DTFs), Trip Logic Functions (TLFs), Output Logic Units (OLUs), and Load Drivers (LDs). The RTIS also contains a separate module for Suppression Pool Temperature Monitor (SPTM). The SPTM is described in Section 7.6.1.7.

The RTIS contains four redundant divisions of DTFs. The DTFs take digitized sensor information from sensors or the SPTM as input. For each system function, the DTF is a comparison of inputs to pre-programmed threshold levels (i.e., setpoints) for possible trip action. The result of the DTF is a discrete trip decision for each setpoint comparison. Each safety division performs the same DTF trip decision based on the independent inputs associated with its own division.

The trip decisions from the DTF in each division are used as input to the TLF performed by each of the four safety divisions. The DTF trip decision results are passed to other divisions through isolated communication links as described in Section 7.9S. The TLF processes DTF trip decisions from all four safety divisions resulting in trip output decisions based on 2-out-of-4 coincidence logic format. The logic format is fail-safe (i.e. loss of signal causes trip conditions) for the TLF and associated DTF. Loss of signal or power to a single division's equipment performing the TLF causes a tripped output state from the TLF, but the 2-out-of-4 configuration of the actuator load drivers prevents simultaneous deenergization of both pilot valve solenoids.

The TLF also receives input directly from the Neutron Monitoring System (NMS) and manual control switches. The details of the NMS system are provided in Section 7.6.1.1.

The trip coincident logic output from the TLF is sent to Output Logic Units (OLUs). The OLUs use devices that provide a diverse interface for the following manual functions:

- Manual reactor trip (per division: 2-out-of-4 for completion).
- MSIV closure (per division: 2-out-of-4 for completion).
- MSIV closure (eight individual control switches).
- RPS and MSIV trip reset.
- TLF output bypass

The OLUs distribute the automatic and manual trip outputs to the MSIV pilot valve and scram pilot valve actuating devices and provide control of trip seal-in, reset, and TLF output bypass (division-out-of-service bypass). Bypass inhibits automatic trip but has no effect on manual trip. The OLUs also provide a manual test input for de-energizing a division's parallel load drivers (part of the 2-out-of-4 output logic arrangement) so that scram or MSIV closure capability can be confirmed without solenoid de-energization. The OLUs are located external to the TLU equipment that implements the TLF so that manual MSIV closure or manual reactor trip (per division) can be performed either when a division's logic is bypassed or when failure of sensors or logic equipment causes trip to be inhibited.

If a 2-out-of-4 trip condition is satisfied within the TLF, all four divisions' trip outputs produce a simultaneous coincident trip signal (e.g., reactor trip) and transmit the signal through hardwired connections to OLUs that control the protective action of the final actuators. The load drivers for the solenoids are themselves arranged in a 2-out-of-4 configuration, so that at least two divisions must produce trip outputs for protective action to occur.

Bypass logic implemented by RTIS is described in Section 7.2.1.1.4.1(2) and shown on Figure 7.2-2.

Each of the four RTIS divisions are powered from their respective divisional Class 1E power supply. In the RTIS, independence is provided between Class 1E divisions, and also between the Class 1E divisions and non-Class 1E equipment.

7.1S.1.2 Neutron Monitoring System

A detailed description of the Neutron Monitoring System (NMS) is provided in Section 7.6.1.1 and 7.7.1.6 for safety related function and non-safety related functions, respectively.

7.1S.1.3 Platform Description

The Reactor Trip and Isolation System (RTIS) and the Neutron Monitoring Systems (NMS) are implemented using Non-Rewritable (NRW)-Field Programmable Gate Array (FPGA)-based platforms.

Each FPGA-based system is a modular, chassis-based, rack-mounted system. FPGA-based systems are built as units, which provide the chassis and backplanes. The units perform specific functions, based on the modules placed in the backplane. Therefore, each module has unique architectural features, based on the differences in interfaces and requirements. The module design is implemented using only FPGAs. The design uses relatively simple medium-scale integrated discrete logic chips for all simple logic functions, such as a monostable multivibrator to implement a watchdog timer. Data is transferred between units over optical links.

Each module consists of one or more printed circuit boards and a front panel. The purpose of the front panel is to fix boards to the unit and to provide mounting for a Human-Machine Interface (HMI) and setpoints adjustment. The FPGA-based system also includes power supplies, analog and digital input/output modules, status modules, and all cabling and wiring necessary for operation. Each circuit board can contain one or more FPGAs.

The FPGA-based systems use logic chips that can be configured. The logic is physically embedded in FPGA chips using special tools. The logic is built from simple functional elements (FEs) that are designed to perform simple logic functions that can be combined and arranged in specific patterns to perform signal processing and logic operations, and thus construct the logic necessary to perform a defined function. Once the logic is embedded, the logic is hard coded and cannot be changed. After the logic is defined and embedded, the FPGA components are treated as hardware. An FPGA can only implement digital logic.

The FPGA-based system has self-diagnostic functions that continuously verify proper FPGA and communications performance and provide outputs used to alert the operator.

Each FPGA-based systems have the following attributes:

- Intra-Division Communication

  Data is transferred between units over optical links by the communication modules. The safety related system has a one-way optical communication data link, providing fixed data sets to each safety-related system and to the nonsafety-related system with Class 1E to non-Class 1E isolation. RTIS offers no possibility of data transfer from the nonsafety to the safety equipment.

- Input / Output (I/O)

  There are I/O modules that are located in the units. Analog Output (AO) module has analog outputs up to 16 channels. There are several types of AO modules for different output ranges. AO Module provides electrical isolation capability from safety to nonsafety system. Digital I/O module has 4 digital inputs and 16 digital outputs. External inputs and internals are isolated using photo couplers and solid-state relays.

- Power Supply

The power supply module provides low voltage direct current (DC) power for equipped modules in each unit. The safety-related system has redundant power supply module in each unit. The RTIS equipment is divisionally powered from multiple Class 1E power sources, one of which is DC backed.

7.1S.2 Microprocessor Based Platforms

The Engineered Safety Features and Control System (ELCS) will be implemented with a microprocessor based platform.

7.1S.2.1 Engineered Safety Features Logic and Control System (ELCS)

The Engineered Safety Features Logic and Control System (ELCS) provides the instrumentation and control functions of automatic actuation, control and display for the Engineered Safety Features (ESF) systems.

The ELCS contains four redundant divisions of DTFs. The four divisions of DTF safety function actuation status are communicated to three divisions of SLFs, which correspond to the three divisions of ESF actuated equipment. Each SLF performs two-out-four logic on the four redundant DTFs. The DTF to SLF communication and isolation features are described in section 7.9S.

Each ELCS division is powered from independent power sources.

For the four redundant divisions of ELCS DTFs, any single division of sensors from one DTF can be manually bypassed, causing the ESF safety function actuation logic in the SLFs to become two-out-of-three, while the bypass state is maintained. The bypass status is indicated in the main control room until the bypass status is removed. Only one division can be placed in bypass. An interlock rejects attempts to remove more than one division from service at a time.

As shown in Tier 1 Figure 3.4B, each of the three ESF component actuation divisions contains a minimum of two SLFs. One of the two SLFs processes initiation logic for functions that service the reactor vessel at low pressure (e.g. RHR), while a second SLF provides the same support for the vessel at high pressure (e.g. Reactor Core Isolation Cooling (RCIC system and High Pressure Core Flooder (HPCF)) system).

The SLF logic for ECCS functions (i.e. initiation of Reactor Core Isolation Cooling, High Pressure Core Flooder or Automatic Depressurization) is implemented using two redundant SLF processing channels per division. The two redundant channels receive the data from the four redundant divisional DTFs, manual control switch inputs and contact closures. The two redundant SLF processing channels perform the same ESF safety function action logic.

The two redundant SLF processing channels must agree for initiation of the ESF safety function to occur. Two SLF processing channels are used to prevent the inadvertent system level actuation of the ESF safety functions that inject coolant of the core or depressurization.

However, in the event of a failure detected by self diagnostics within either processing channel, a bypass (ESF output channel bypass) is applied automatically (with manual backup) such that the failed SLF processing channel is removed from service. The remaining SLF processing channel provides one-out-of-one operation to maintain availability during the repair period. SLF processing channel failures are alarmed in the main control room. If a failed channel is not automatically bypassed, the operator is able to manually bypass the failed channel.

The two-out-of-two voting of the two SLF processing channels is performed on a component basis with non-microprocessor based equipment or with a separate actuation for a valve from one SLF processing channel and a related pump actuation from the second SLF processing channel, where both are required to initiate coolant injection.

As shown in Tier 1 Figure 3.4b, each ELCS division includes the following major elements:

- Sensors provide signal input to the ELCS. For ELCS safety functions, the appropriate sensors are connected to the Digital Trip Function.

- The Digital Trip Function receives input signals directly and also receives remote input signals from a Remote Digital Logic Controller (RDLC). The RDLC communicates the remote input signals to the DTF utilizing high speed serial link (HSL) communication with redundant fiber optic modems and optical data cable. HSL communication is described in Section 7.9S.

- The DTF provides a comparison of signal inputs to associated setpoints to determine the trip status for each ESF safety function. The DTF communicates trip status to the Safety Logic Function (SLFs) in each division by means of optical-based HSL communication links.

- An individual DTF to SLF communication is provided with single fiber optic cable since the DTF and SLF are both located in the MCR area.

SLFs are provided in each of the three ESF divisions that provide electromechanical component actuation. Each division's SLFs receive ESF safety function actuation status signals from each of the DTFs in the four redundant divisions. The division's SLFs calculate ESF system level actuation status by determining whether there is a two-out of-four coincidence of DTF ESF safety function trip signals. The SLF also receives hardwired signals for control of ESF components from I/O that is local to the SLF and from SLF I/O that is located remote from the MCR. The SLF communicates ESF actuation commands to the SLF I/O stations that are located in areas that are remote from the MCR by HSL. The fiber optic cables are redundant for the communication of ESF safety function actuation commands from the SLF to the SLF remote I/O.

The SLF Remote Digital Logic Controller (RDLC) provides I/O and ESF component actuation. At the RDLC a Component Interface Module (CIM) is provided for each controlled electromechanical component assigned to the SLF. The CIM interfaces the ESF actuation command signals (or control commands in the absence of actuation) from the SLFs to the electromechanical ESF component.

The CIM provides priority logic to override control when an ESF actuation occurs. Logic in the CIM also provides voting of redundant SLF processing channels signals, for ESF safety functions that require SLF redundancy. The CIM receives component position and status feedback signals from the component control circuit. The CIM provides local control capability for maintenance.

Each ELCS division has an intra-division network that connects the ELCS controllers with flat panel safety displays in the main control room and a Maintenance and Test Panel. The intra-division network is described in section 7.9S

For each ELCS division, there are two safety display stations in the main control room. Each safety displays are driven by a flat panel display subsystems.

Each ELCS division has a permanently connected Maintenance and Test Panel (MTP) and an Interface and Test Processor (ITP). The MTP and ITP are utilized for the maintenance technician functions.

Electrical power Distribution System (EPDS)

Each of the three safety related divisions of EPDS has a flat panel safety display in the main control room. The operator utilizes a division's safety display for manual control of selected safety related EPDS components.

Each division's safety display utilizes an intra-division network to communicate the operator commands to a controller and to provide status information from the controller to the safety display. The flat panel display and controller are the same as those utilized for ELCS.

The controller communicates with Remote Digital Logic Controllers (RDLCs) with high speed serial links (HSLs). The RDLCs provide signal outputs that represent the operator's manual commands to the EPDS component control logic and provide for signal inputs for EPDS component status information for display to the operator. The RDLCs are the same as those utilized for ELCS, with the exception that the HSL communication links are not redundant.

7.1S.2.2 ELCS Platform

The platform that implements the ELCS has the following major elements:

- Controller, including high speed serial link communications

- Intra-division Network communications
- Input / Output
- Flat Panel Display
- Maintenance and Test Panel
- Power Supplies
- Component Interface Module

The ELCS Controller subsystem is modular. A passive backplane connects individual module slots, which can house the following module types:

- Controller module
- Intra-division communication module
- Input / output modules

7.1S.2.3 ELCS Controller

The controller contains two sections, a processing section and a communication section. The processing section contains a microprocessor and memory for the applications programs. The processing section memory utilizes Flash PROM for system software, Flash PROM for application software, and RAM.

The communication section contains another microprocessor and memory for communications with other Controllers in different chasses. The communications memory utilizes Flash PROM for system software and RAM. The communications section performs the HSL communications functions and the HSL diagnostics.

The two controller sections communicate through shared memory. The shared memory provides for communications isolation. The ELCS Controller performs self-diagnostics, including an internal watchdog timer, and is able to determine that the required module types are located in the appropriate slot.

The backplane allows multiple Controllers to be utilized in a single chassis. The controllers communicate through shared memory that is located on the Intra-division communication module.

- Intra-Division Communication

The communication module provides the interface for the intra-division communication network. The intra-division communication module performs communication diagnostics. Intra-division communications are described in section 7.9S.

- Input / Output (I/O)

The Controller uses compatible I/O modules that are located in the chassis with the controller. Additional chasses of I/O modules can be added to the first Controller chassis if additional I/O is necessary. A range of modules is available covering analog and digital signals of various types. In addition, there are modules for temperature measurement and rotational speed measurement.

The system software in the Controller automatically checks that all modules are operating correctly at system startup. Module diagnostic failures are reported to the Controller.

- Flat Panel Display

The flat panel display subsystem consists of the flat panel display with touch screen capability, a single board computer, and standard communication interfaces for communication to the intra-division network

For STP Units 3 and 4, the RTIS and NMS utilize the ELCS flat panel display subsystem to display selected information. Each division of RTIS and NMS send data to a communication interface associated with the same ELCS division. The RTIS and NMS utilize serial fiber optic data links over fiber optic media. The communication interface then communicates the RTIS and NMS information to an interface module on each flat panel display subsystem. The data flow is unidirectional from RTIS and NMS to the ELCS communication interface.

- Maintenance and Test Panel (MTP)

The MTP will be used for technician surveillance, maintenance and test functions for each division. The MTP provides the means for the operator or technician to change setpoints, insert and remove bypasses, support periodic testing, and display detailed system diagnostic messages. The MTP provides features that support the administrative control of these activities.

The MTP utilizes a flat panel display subsystem in conjunction with the ITP for monitoring diagnostics and providing a periodic test interface for other Controllers. The MTP and ITP are connected to the intra-division network.

The MTP flat panel display subsystem also includes a communication interface to the non-safety system. The MTP communication interface to the non-safety systems provide for communication isolation to assure that data flows in a unidirectional manner from the ELCS to the non-safety systems. The communication interface utilizes an optical connection to the non-safety systems to provide electrical isolation.

- Power Supply

The power supply subsystem provides low voltage direct current (DC) power for the ELCS equipment that requires it. ELCS equipment is divisionally powered from multiple Class1E power sources, one of which is DC backed.

- Component interface Module (CIM)

In general, the CIM provides the interface between the ELCS actuation and control command signals and the electromechanical device associated with the final ESF components. Electromechanical components with non-standard signal interface requirements may not use a CIM, but could be interfaced with discrete I/O.

RAI 07.01-14

QUESTION:

In the STPNOC letter U7-C-STP-NRC-090009, dated February 9, 2009, the applicant provided the conformance to the Regulatory Guides (RG), Codes and Standards, that are applicable to I&C platform departures. Enclosure 2b of this letter contains proposed revisions to COLA Tier 2 Table 1.9S-1, "Site-Specific Conformance with Regulatory Guides," and a new Table 1.9S-1a, "IEEE Standards Applicable to the STP 3&4 Platforms," which document the RG, Codes, and Standards applicable to the departed I&C design. Footnotes 1 and 2 to these tables refer to the proposed technologies for Reactor Trip & Isolation System (RTIS), Neutron Monitoring System (NMS), and ESF Logic & Control System (ELCS), i.e., Toshiba FPGA platform and Westinghouse Common Q platform. These footnotes make a distinction in the Rev. levels of RG and IEEE Std. applicable to the RTIS/NMS and the ELCS. The reason for this distinction is the bases of prior NRC generic approval of the Westinghouse Common Q platform. Subsequently, in the STPNOC letter U7-C-STP-NRC-090076, dated July 22, 2009, the applicant stated that the design approval approach for STP 3 & 4 safety-related digital I&C systems no longer relies on the approval of the Westinghouse and Toshiba topical reports referred to in the footnotes, which are no longer relevant to the information in the tables, and therefore these two footnotes will not be incorporated into the COLA. However, the applicant did not change the RG and IEEE Std. revision numbers associated with these footnotes. Please note that all departures form the referenced certified design in the COLA are required to meet the current regulations. Since the NRC approval of the ELCS design no longer relies on the pre-approved Westinghouse Common Q platform, the ELCS design should also conform to the current regulation and associated IEEE Std. and Regulatory Guides (similar to the RTIS and NMS design). Update FSAR Tables 1.9S-1, 1.9S-1a, and related sections of the COL application addressing the ELCS design compliance to the current regulations.

RESPONSE:

As described in the RAI, STPNOC letter U7-C-STP-NRC-090076 stated that the design approval approach for STP 3 & 4 safety-related digital I&C systems no longer relies on the approval of the Westinghouse and Toshiba topical reports, and that the two footnotes in Table 1.9S-1 and 1.9S-1a would not be incorporated. However, this statement needs to be clarified, as discussed below.

The Toshiba Field Programmable Gate Array (FPGA) platform is being used for the Neutron Monitoring System (NMS) and Reactor Trip and Isolation System (RTIS). Topical report UTLR-0001-P Rev. 0 referred to in STPNOC letter U7-C-STP-NRC-090009 has been withdrawn from NRC review. Instead, as previously communicated to the NRC, the Toshiba FPGA platform information will be provided in technical reports to be supplied for STP 3&4 as part of the DAC closure process. As such, the STP 3&4 COLA does not rely on approval of UTLR-0001-P. Therefore, reference to the UTLR-0001-P topical report is no longer relevant and will not be incorporated into the COLA.

The Westinghouse Common Q platform is being used for the Engineered Safety Feature (ESF) Logic and Control System (ELCS). The statement in STPNOC letter U7-C-STP-NRC-090076 that indicated that the design approval approach for the STP 3&4 safety-related digital I&C system does not rely on approval of the Common Q platform has been reviewed by STPNOC, and STPNOC is clarifying this statement to mean that STPNOC was not relying on an NRC approval of the Common-Q topical report as part of this COLA since the Common Q platform had been previously approved by the NRC for generic use. It has been STPNOC's continuing intent that the STP 3&4 ELCS platform is based on the NRC-approved Common Q topical report, WCAP-16097-P-A, Revision 0. Therefore, the reference to the Common Q topical report in STP 3&4 FSAR Table 1.9S-1 as provided in STPNOC letter U7-C-STP-NRC-090009 is still applicable, and will be included in the STP 3&4 COLA.

Incorporation of the Common Q platform for the STP 3&4 ELCS, by reference to the NRC approved topical report and associated SERs, is consistent with the intent of the NRC policy related to use of topical reports. The policy aims to minimize industry and NRC time and effort by providing for a streamlined review and approval of the safety-related subject with subsequent referencing in licensing actions, rather than repeated reviews of the same subject (ref: NRR Office Instruction LIC-500, "Processing Requests for Reviews of Topical Reports"). Per 10 CFR 52.79(a)(41), the COLA should address the Standard Review Plan in effect six months before the COLA docket date, and as such it is expected the departures to the certified design should address that SRP. However, 52.79(a)(41) also states, "Where a difference exists, the evaluation shall discuss how the proposed alternative provides an acceptable method of complying with the Commission's regulations, or portions thereof, that underlie the corresponding SRP acceptance criteria. The SRP is not a substitute for the regulations, and compliance is not a requirement." Further, SRP 7.3 (Revision 5, March 2007), which addresses ESF control systems, states in Section III, "The reviewer will select material from the procedures described ... typical reasons for non-uniform emphasis [in application of the SRP procedures] are ... the utilization in the design of features previously reviewed and found acceptable." The Common Q platform was previously reviewed and found acceptable, as documented in the applicable SERs, as described below. In its letter approving this topical report, the NRC stated that "We do not intend to repeat our review of the matters described in the report, and found acceptable, when the report appears as a reference in license applications, except to assure that the material presented is applicable to the specific plant involved." As such, for clarity the FSAR identifies the requirements to which this platform is approved, and these requirements are submitted as an acceptable alternate to current NRC guidance.

As part of the Common Q platform generic review process, the NRC issued Generic Open Items (GOIs) 7.1 thru 7.10. Subsequently, the NRC issued two SERs (NRC Safety Evaluation Report, "Safety Evaluation by the Office of Nuclear Reactor Regulation Related to the Westinghouse Common Q Platform Closeout of Generic Open Items and Approve Changes to Topical Report CENPD-396-P, Rev. 01, Common Qualified Platform", February 24, 2003. [ML030550776]; and NRC Safety Evaluation Report, "Safety Evaluation for the Closeout of Several of the Common Qualified Platform Category 1 Open Items Related to Reports CENPD-396-P, Revision 1 and CE-CES-195, Revision 1 (TAC No. MB0780)," June 22, 2001. [ML011690170]) that generically closed all of the GOIs, with the exception of GOI item 7.8. This GOI relates to the "level 3 loop controllers" referenced in the Common Q topical report integrated solution (Appendix 4). The level 3 loop controllers (LCs) provide component control based on signals from the ESF actuation system. The Component Interface Module (CIM) is being used to implement this function in the STP 3&4 ELCS. Westinghouse will be submitting a revision to the Common Q topical report to close GOI 7.8.

As part of the review process, the NRC also issued Plant Specific Action Items (PSAIs) 6.1 thru 6.14. These action items were provided by the NRC as a checklist for any utility that would be implementing a Common Q I&C system(s) upgrade. The PSAIs were written for an operating plant implementing a Common Q system(s) upgrade, therefore some of the language, may not directly be applicable to a new plant.

A technical report will be prepared that summarizes the resolution of the 10 GOIs, including GOI item 7.8, and the impact of the 14 PSAIs on the Common Q based STP 3&4 ELCS plant specific design. A technical report will also address any STP 3&4 specific design features that are required for implementation of the Common Q platform for ELCS for STP 3&4. The PSAIs and plant specific design features will be in accordance with the latest regulatory guides and codes and standards. These technical reports will be provided as part of DAC closure process.

In summary, the STP 3&4 ELCS platform is based on the NRC-approved Common Q topical report, WCAP-16097-P-A, Revision 0. The Common Q platform was previously reviewed and found acceptable, as documented in the applicable SERs. Incorporation of the Common Q platform for the STP 3&4 ELCS by reference to the NRC approved topical report and associated SERs is consistent with the intent of the NRC policy related to use of topical reports, the Common Q SER approval letter, and SRP 7.3. All subsequent design to address the Common Q PSAIs and plant specific design features will be in accordance with the latest regulatory guides and codes and standards, and will be documented in technical reports that will be provided as part of the DAC closure process. As such, use of the NRC-approved Common Q platform, including its applicable regulatory guide, codes and standards, is acceptable and appropriate for the STP 3&4 COLA.

The updates to FSAR Tables 1.9S-1 and 1.9S-1a, which were originally provided in STPNOC letter U7-C-STP-NRC-090009, are provided below. These changes will be incorporated into a future revision of the COLA. Changes from COLA Revision 3 are highlighted in gray shading.

Table 1.9S-1 Site-Specific Conformance with Regulatory Guides

No.	Title	Rev.
Division 1		
1.47	1.47 Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems	0 (1973)
1.53	1.53 Application of the Single-Failure Criterion to Safety Systems	2 (11/03) 0 (1993) for ELCS[1]
1.62	Manual Initiation of Protection Actions	0 (1973)
1.75	Independence of Electrical Safety Systems	3 (2/05) 2 (1978) for ELCS[1]
1.100	Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants	2 (1988)
1.118	Periodic Testing of Electric Power and Protection System	3 (1995) 2 (1978) for ELCS[1]
1.152	Criteria for Use of Computers in Safety Systems of Nuclear Power Plants	2 (2006) 1 (1996) for ELCS[1]
1.168	Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	1 (2004) 0 (1987) for ELCS[1]
1.169	Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	0 (1997)
1.170	Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	0 (1997)
1.171	Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	0 (1997)
1.172	Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	0 (1997)
1.173	Developing Software Life Cycle Process for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	0 (1997)
1.180	Guidelines for Evaluating Electromagnetic and Radio- Frequency Interference in Safety-Related Instrumentation and Control Systems Instrumentation and Control Systems	1 (2003) 0 (2000) for ELCS[1]
1.209	Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants	0 (2007) for ELCS see note 2

[1] The Common Q Digital Platform was submitted for generic use and was approved for reference as described in Topical Report WCAP-16097-P-A, Revision 0, "Common Qualified Platform Topical Report." This topical report includes the SERs dated August 11, 2000, June 22, 2001, and February 4, 2003, and is consistent with the referenced industry standards and Regulatory Guides that reference Note 2. The Westinghouse "Software Program Manual for Common Q Systems" (SPM), WCAP-16096-NP-A also incorporates standards and Regulatory Guide requirements. The requirements that this platform were licensed to are submitted as an acceptable alternate to current requirements based on the original NRC review and SERs. This topical report was reviewed against Rev. 2 (1978).

[2] RG 1.209 endorses IEEE 323-2003. The ELCS conforms to IEEE 232-1983 as shown above and as discussed in Note 1.

Table 1.9S-1a IEEE Standards Applicable to the STP 3&4 Platforms

IEEE No.	Category	Rev.
IEEE 7-4.3.2	Digital Computers and Software	2003 1993 for ELCS[1]
IEEE 323	EQ	2003 1983 for ELCS[1]
IEEE 338	Periodic Testing	1987
IEEE 344	Seismic	1987
IEEE 379	Single Failure	2000 1994 for ELCS[1]
IEEE 384	Independence	1992
IEEE 603	I&C	1991
IEEE 828	Configuration Management	1990
IEEE 829	Software Test Documentation	1983
IEEE 830	Software Requirements Specifications	1993
IEEE 1008	Software Unit Testing	1987
IEEE 1012	V&V	1998
IEEE 1028	Software Reviews and Audits	1997
IEEE 1042	Software Configuration Management	1987
IEEE 1074	Software Life Cycle Processes	1995

[1] The Common Q Digital Platform was submitted for generic use and was approved for reference as described in Topical Report WCAP-16097-P-A, Revision 0, "Common Qualified Platform Topical Report." This topical report includes the SERs dated August 11, 2000, June 22, 2001, and February 4, 2003, and is consistent with the referenced industry standards and Regulatory Guides that reference Note 2. The Westinghouse "Software Program Manual for Common Q Systems" (SPM), WCAP-16096-NP-A also incorporates standards and Regulatory Guide requirements. The requirements that this platform were licensed to are submitted as an acceptable alternate to current requirements based on the original NRC review and SERs. This topical report was reviewed against Rev. 2 (1978).

RAI 07.07-10

QUESTION:

STP 3 & 4 COLA acknowledges the Departure STP DEP 7.7-10 requires prior NRC approval. In STP DEP 7.7-10, "Control Rod Drive Control System Interfaces," the departure "Description" briefly summaries the changes to Subsection 7.7.1.2.1 of the reference ABWR DCD. However, the departure "Description" does not sufficiently identify all the changes including revisions to allowed operator single and ganged rod movement manual commands, deletion of the description of CRD Control System Withdrawal Cycle, and Insert Cycle interfaces. Further, the departure "Evaluation Summary" does not provide sufficient justification for the NRC staff to complete its review and approval of these significant departure changes. Identify all the changes to Subsection 7.7.1.2.1, parts (1), (2), (3), and (4), and complete the justification in a manner that will allow NRC approval of the departure.

RESPONSE:

STPNOC will provide an update to STP 3 & 4 COLA Part 2, Tier 2, Subsection 7.7.1.2.1 and COLA Part 7, Section 2.2, STD DEP 7.7-10 to provide clarification and additional information about the changes and their justifications.

COLA Part 7, Section 2.2, STD DEP 7.7-10, the Description will be revised as follows, with the changes (in gray background) to be included in a future COLA revision:

Description

Subsection 7.7.1.2.1 of the reference ABWR DCD provides the Rod Control and Information System (RCIS) interfaces with the Control Rod Drive (CRD) Control System for Single Rod Movement (Subsection 7.7.1.2.1(1)), Withdrawal Cycle (Subsection 7.7.1.2.1(2)), Insert Cycle (Subsection 7.7.1.2.1(3)), and Ganged Rod Motion (Subsection 7.7.1.2.1(4)). This COLA change implements the following revisions in the listed DCD subsections:

- The Performance and Monitoring Control System (PMCS) normal operational manual mode CRT display is replaced with the RCIS Dedicated Operator Interface on the Main Control Room Panel.

- The description of allowed operator single and ganged rod movement manual commands is revised.

- The name of the subsection "Introduction" is changed to "Single Rod Movement."

- A discussion of the Rod Action and Position Information (RAPI) rod block operations is added.

- The description of RAPI normal rod movement operations is revised. The revised text includes description of operation of the Rod Server Modules (RSMs), the Rod Brake

Controllers (RBCs), the Synchro-to-Digital Converters (SDCs), and the Fine Motion Control Rod Drives (FMCRDs).

- The ~~descriptions of the CRD Control System Withdrawal Cycle and Insert Cycle interfaces are deleted.~~ name of the subsection "Ganged Rod Motion" is changed to "Ganged Rod Movement."

- The description of ganged rod movement interface is revised.

In addition, the COLA Part 7 Evaluation Summary for STD DEP 7.7-10 will be revised as follows:

Evaluation Summary

This proposed change provides a more clear and complete description of this non-safety RCIS design implementation and operation. These RCIS changes are a result of ABWR DCD I&C design evolution based on multiple years of operating experience at a Japanese ABWRs. The approved ABWR DCD design and functional requirements still are satisfied with improved, state-of-the-art, I&C equipment systems.

COLA Part 2, Tier 2 FSAR, Subsection 7.7.1.2.1 will be revised with the changes (in gray background) to be included in a future COLA revision. Item (1) fourth through fourteenth paragraphs will be changed and additional paragraphs inserted under Item (2) as shown below:

(1) ~~*Introduction*~~ Single Rod Movement

~~*The CRT display*~~ The RCIS DOI *provides the operator with a capability to move a single rod or a ganged selection.* ~~*For this discussion, the operator selects a single rod for withdrawal.*~~ ~~*Four*~~ Three *rod movement commands* ~~*(poke points)*~~ *serve as a means to initiate all rod movements controlled from this display. They are identified as* ~~*"SINGLE ROD", "ROD GANG",*~~ *"STEP",* "NOTCH", and ~~or~~ "CONTINUOUS"~~, and "IN" or "OUT"~~.

~~When a "STEP" movement is performed for a selected single rod, the rod moves a nominal distance of 18.3 mm, with the associated rod step position value corresponding to the number of "STEP" withdrawal movements from the normal full-in position value. A rod at normal full-in position has an associated rod step position value of "0" steps withdrawn. A rod at normal fullout position has an associated rod step position value of "200" steps withdrawn, as the normal full-out position value is 3660 mm below the normal full-in position value of 0 mm.~~

~~When a "NOTCH" movement is performed for a selected single rod, the rod moves a nominal distance of 73.2 mm (i.e. 4 times the nominal step movement distance), with the restriction that the nominal stopping position for the "NOTCH" movement in terms of the distance withdrawn from the normal full-in position is an integer multiple of 73.2 mm. For example, if the selected rod were~~

~~initially at a step position value of "6" steps withdrawn and one "NOTCH" withdrawal movement is performed, the selected rod would stop at a step position value of "8" steps withdrawn. If a "NOTCH" insert movement was then performed, the selected rod would stop at a step position value of "4" steps.~~

~~When a "CONTINUOUS" movement is performed for a selected single rod, the rod target stopping position value is continuously updated to an integer multiple of 18.3 mm as long as the operator continuously depresses the "withdraw" (or "insert") movement pushbutton. For example, if the selected Rev. 02 Control Systems Not Required for Safety 7.7-13 STP 3 & 4 Final Safety Analysis Report rod were initially at a step position value of "8" steps withdrawn and a "CONTINUOUS" withdrawal movement is performed, the rod target stopping position value would be updated initially to "1312" steps and then would be updated at a predetermined rate corresponding to the nominal continuous rod movement speed to "14", "15", etcposition which adds 4 steps to the current position. When the operator ceases to continuously depress the "withdraw" movement pushbutton in this case, the rod target stopping position value then no longer changes and the rod then moves to and stops upon reaching the applicable rod target stopping position value. A "CONTINUOUS" withdrawalinsertion movement would be similar, except the nominal rod target position value would decrease, instead of increase, while the "insert" movement pushbutton remains depressed.~~

~~Manual gang movements in the "STEP", "NOTCH" and "CONTINUOUS" movement modes would be accomplished in a similar manner to that described above; however, all operable rods of the selected gang move simultaneously during each movement operation. Also, normal manual rod movements are limited such that insertion rod movement beyond normal fullin or full-out position is not allowed unless RCIS is placed in a special test mode used for performing the CRD coupling check surveillance test.~~

~~*The operator first identifies the rod status from the rod status requestor information display, then makes a decision for either a withdrawal or an insertion of a control rod and sets up the display. The operator can request rod status information by actuating poke points on the CRT for the required rod.*~~ Then, to request the desired movement in the selected movement mode, the operator then activates the ~~"insert" or~~ "withdraw" (or "insert") movement command by activating associated hard pushbutton switches located adjacent to the RCIS DOI on the main control panel.

~~The RAPI of the RCIS enforces rod blocks based upon signals internal or external to the system. These rod blocks can prevent desired rod movements or stop rod movements, if activated while normal rod movements are underway. This applies to both single rod movement and ganged rod movement modes.~~

~~The internal signals include those signals from the ATLM and RWM subsystems of RCIS. During normal RCIS operating conditions with no single channel bypass condition active, if there is any disagreement between the two channel logic of the~~

~~subsystems of the RCIS, rod block signals are transmitted to the rod server module.~~

~~Examples of external input signals which could cause rod withdrawal blocks include rod block signals from the SRNM and APRM subsystems of the NMS; and FMCRD separation status signals received via associated datalink signal transmission from the CRD system to the RCIS. A complete list of rod block conditions is provided later in this section.~~

~~When normal rod movements are performed, the RAPI of the RCIS transmits the appropriate rod movement command signals to a dual channel file control module (FCM) located in a RCC. These rod movement command signals are received at the dual channel FCM and routed to rod server processing channel (RSPC) A and RSPC B of the rod server modules (RSMs) of the selected rod in RCCs. The RSPCs transmit signals to channel A and channel B inputs for the corresponding inverter controller and transmit brake energization signals to the associated rod brake controller (RBC). The inverter controller then performs two-out-of-two voting on the command signals received and activates the proper power control signals to the SMDM to accomplish the FMCRD motor movement desired. The rod brake controller similarly performs two-out-of-two voting and mechanically releases the FMCRD brake just prior to the start of FMCRD motor movement and then reengages the FMCRD brake after the normal rod movement is complete.~~

~~The SDCs of the RSM also interface with instrumentation of the FMCRD (a subsystem of the CRD), collects absolute rod position for the corresponding FMCRD by converting the Synchro A and Synchro B analog signals into digital data representing the FMCRD rod position for use in the associated RSPCs' logic and transmission (via the RCIS dedicated multiplexing network) to the RAPI logic and for the RAPI to transmit rod position data to other systems and subsystems and to the RCIS DOI.~~

(2) *Withdrawal Cycle* ~~Not Used~~

Following is a description of the selected rod withdrawal movement in the manual mode.

After operator selection of a rod and rod movement mode, which are "STEP," NOTCH," or "CONTINUOUS," on the RCIS DOI on the main control panel, then the operator depresses the "withdraw" hard pushbutton switch. If a "STEP" movement is initiated by the operator for a selected single rod, the rod moves a nominal distance of 18.3 mm, with the associated rod step position value displayed on the RCIS DOI corresponding to the number of "STEP" withdrawal movements from the normal full-in position value. A rod at normal full-in position has an associated rod step position value of "0" steps withdrawn. A rod at normal full-out position has an associated rod step position value of "200" steps withdrawn, as the normal full-out position value is 3660 mm below the normal full-in position value of 0 mm.

If a "NOTCH" movement is initiated by the operator for a selected single rod, the rod moves a nominal distance of 73.2 mm (i.e., four times the nominal step movement distance), with the restriction that the nominal stopping position for the "NOTCH" movement in terms of the distance withdrawn from the normal full-in position is an integer multiple of 73.2 mm. for example, if the selected rod were initially at a step position value of "6" steps withdrawn and one "NOTCH" withdrawal movement is selected and performed, the selected rod would stop at a step position value of "8" steps withdrawn. If a "NOTCH" insert movement was then performed, the selected rod would stop as a step position value of "4" steps.

If a "CONTINUOUS" movement is initiated by the operator for a selected single rod, the rod target stopping position value is continuously updated to an integer multiple of 18.3 mm as long as the operator continuously depresses the "withdraw" (or "insert") movement pushbutton. For example, if the selected rod were initially at a step position value of "8" steps withdrawn and a "CONTINUOUS" withdrawal movement is performed, the rod target stopping position value would be updated initially to "12" steps and then would be updated at a position which adds 4 steps to the current position. When the operator ceases t continuously depress the "withdraw" movement pushbutton in this case, the rod target stopping position value then no longer changes and the rod then moves to and stops upon reaching the applicable rod target stopping position value.

Manual gang movements in the "STEP," NOTCH," and "CONTINUOUS" movement modes would be accomplished in a similar manner to that described above; however, all operable rods of the selected gang move simultaneously during movement operation. Also, normal manual rod movements are limited such that rod movement beyond normal full-in or full-put position is not allow unless RCIS is placed in a special test mode used for performing the CRD coupling check surveillance test.

During all of these operator selections for rod withdrawals there is continuous monitoring of the selection and movement by the Rod Action and Position Information (RAPI) function. The RAPI of the RCIS enforces the rod block function based upon signals internal or external to the system. If a rod block is activated while normal rod movements are underway, it can prevent desired rod movements or stop rod movements. This rod block function applies in both single rod movement and ganged rod movement modes.

The RAPI internal signals include those signals from the Automated Thermal Limit Monitor (ATLM) and Rod Worth Minimizer (RWM) subsystems of the RCIS. During normal RCIS operating conditions with no single channel bypass condition active, if there is any disagreement between the two channel logic of the subsystems of the RCIS, rod block signals as transmitted to the rod server module. Examples of external input signals which could cause rod withdrawal blocks include rod block signals from the Startup Range Neutron Monitor (SRNM) and the Average Power Range Monitor (APRM) subsystems of the Neutron Monitoring System (NMS) and Fine Motion Control Rod Drive

(FMCRD) separation status signals from the CRD system to the RCIS. A complete list of the rod block conditions is provided later in this section.

When normal rod movements are performed, the RAPI of the RCIS transmits the appropriate rod movement command signals to rod server processing channel (RSPC) A and RSPC B of the rod server module (RSM) of the selected rod in the Remote Communication Cabinets (RCCs). The RSPCs transmit signals other corresponding inverter controller and transmit brake energization signals to the associated rod brake controller (RBC). The inverter controller then performs two-out-of-two voting on the command signals received and activates the proper power control signals to the stepping motor driver module (SMDM) to accomplish the FMCRD motor movement desired. The rod brake controller similarly performs two-out-of-two voting and mechanically releases the FMCRD brake just prior to start of FMCRD motor movement and then reengages the FMCRD brake after the normal rod movement is complete.

The Synchro-to-Digital Converters (SDCs) of the RSM also interfaces with instrumentation of the FMCRD (a subsystem of the CRD), collect absolute rod position for the corresponding FMCRD by converting the Synchro A and Synchro B analog signals into digital data representing the FMCRD rod position for use in the associated RSPCs' logic and transmission (via the RCIS dedicated multiplexing network) to the RAPI logic and for the RAPI to transmit rod position data to other systems and subsystems and to the RCIS DOI.

~~*Following is a description of steps the operator performs at the RCIS dedicated operator's interface panel in selecting a rod for movement in the manual mode. The operator depresses the manual rod movement mode switch, which enables the RCIS for manual mode. The operator then verifies indicator/alarm status at the control panel for the following conditions:*~~

Item (3) in this subsection will also be changed as shown below:

(3) *Insert Cycle* ~~Not Used~~

An operator action to insert a rod while in the manual mode would be processed in a similar manner as above.~~*, except that signals for an insertion of the rod would be decoded at the rod server module (RSM). On receiving the correct signals from the RSM, the stepper motor driver module would provide power pulses to the FMCRD motor such that control rod insertion would result.*~~

The control room operator uses the same controls for insertion of the control rods, except the "insert" hard pushbutton switch on the RCIS DOI is depressed. When a "STEP" insertion movement is selected and performed, the selected rod is inserted and stops as the next step position. When a "NOTCH" insertion movement is selected and performed, the selected rod is inserted and stops as the next notch position. A "CONTINUOUS" insertion movement is similar to "CONTINUOUS" withdrawal movement, except upon selection the nominal target position value decreases instead of increasing, while the "insert" movement pushbutton remains depressed.

No additional change is required in this subsection for *(4)* Ganged Rod Movement.

RAI 07.09-8

QUESTION:

COLA FSAR Tier 1 Section 2.7.5 states that data cannot be transmitted from the non-safety-related side to safety-related equipment. However, COLA FSAR Tier 2 Section 7.9S.2.2 allows the manual data transmission from the non-safety related PICS to the safety-related NMS. Provide sufficient information on how the manual operation does not adversely impact the safety-related NMS.

RESPONSE:

As described in the STPNOC response to RAI 07.09-1, data cannot be transmitted from the non-safety equipment to on-line safety-related equipment because of the communication interface and electrical isolation design features. The response also discusses the separate offline method used to transfer LPRM calibration data from Plant Information and Control System (PICS) to the Neutron Monitoring Systems (NMS). This includes placing the NMS division to receive data in an inoperative status, requiring a key lock switch be enabled at the NMS to allow transfer, and having manual verification before the NMS division is placed back in service. NMS design allows transfer of only a limited data set in a strict, predefined format. This transfer of data is further discussed in COLA Part 2, Tier 2, Subsection 7.9S.2.5.7, Independence.

There is no COLA revision required as a result of this RAI.

RAI 07.02-2

QUESTION:

Departure STD DEP T1 3.4-1 proposed changes to the safety-related instrumentation and control (I&C) architecture which impact COLA FSAR Figure 7.2-2 for the safety related reactor protection system (RPS). The bypass unit (BPU) with inputs and output to/from each division shown on the original Figure 7.2-2 in the ABWR DCD was deleted without any explanation in the COLA FSAR. In addition, some interlocks, such as “reset permissive”, “from one ACT (reset permissive)”, and “trips from NMS Div x”, were included on the original figure, but are circled as changes on Figure 7.2-2 in the COLA FSAR. There are many changes to COLA FSAR Figure 7.2-2 which are not explained. Clarify and explain in the COLA Departures Report and FSAR all changes made to Figure 7.2-2.

RESPONSE:

A markup of STP 3&4 COLA Tier 2 Figure 7.2-2 is provided with the response to RAI 07-7 (Reference STP letter U7-C-STP-NRC-090157, dated September 22, 2009) and will be included in a future COLA revision.

Each change to Tier 2 Figure 7.2-2 is discussed below.

The figure has been revised to more clearly identify division channel DTF inputs to the Trip Logic Function (TLF). This change is addressed in the response to RAI 07-7.

The figure has been revised to remove the Remote Multiplexing Unit (RMU) and the Multiplexing Unit (MUX). This is included in Departure STD DEP T1 3.4-1 and is described in its COLA Part 7 Description with the changes associated with the elimination of obsolete data communication technology.

The figure has been revised to remove the trip input from high main steam line radiation to the MUX based on Departure STD DEP T1 2.3-1.

The figure has also been revised to make a number of nomenclature changes, which are consistent with Departure STD DEP T1 3.4-1. These are described in the STD DEP T1 3.4-1 COLA Part 7 Description for the clarifications of digital controls nomenclature and systems changes.

The following clouded portions of Tier 2, Figure 7.2-2 were changes from COLA Revision 2 that reverted them back to DCD Figure 7.2-2 and are incorporated by reference, therefore no additional departure description is necessary:

- the addition of the reset permissive from the trip actuators (ACTs) to the Output Logic Unit (OLU),
- the addition of the reset permissive from one ACT to the Manual Scram Logic Devices (MLU),

- the addition of the trip inputs from the Neutron Monitoring System (NMS) divisions to the TLF, and

- the addition of the non-coincident NMS disable in the division manual switch input to the TLF.

An additional change to Tier 2 Figure 7.2-2 was shown in the response to RAI 07-7 to remove an erroneous arrow.

Departure STD DEP T1 3.4-1 also clarifies the nomenclature for the Bypass Unit (BPU) to Bypass Interlock Function. A description of the Bypass Interlock Function is included in the Background for STP 3&4 Technical Specification Bases Section B 3.3.1.1 provided in FSAR Section 16. The Technical Specifications Bases state that, "The bypass interlock function enforces restrictions on bypassing multiple divisions of related functions." The bypass logic described in FSAR Section 7.2.1.1.4.1(2) is unchanged. The Bypass Unit (BPU) was removed from FSAR Figure 7.2-2 because it is no longer a separate unit. The following additional FSAR changes will be made to clarify this change. Gray highlighting shows the changes.

FSAR Section 7.2.1.1.4.1(2) will be revised as follows in a future COLA revision:

(2) *Divisions of Trip Logics*

Equipment within a division of trip logic includes primarily manual switches, ~~*bypass units (BPUs)*~~bypass interlock functions, *trip logic* functions~~*units*~~ *(*~~*TLUs*~~TLFs) *and output logic units (OLUs). The various manual switches provide the operator means to modify the RPS trip logic for special operation, maintenance, testing and reset. The* bypass interlock functions enforce restrictions on bypassing multiple divisions of related functions. The bypass interlock functions ~~*BPUs*~~ *perform bypass and interlock logic for the channel sensors bypass, main steamline isolation trip special bypass and division trip logic unit bypass. These three bypasses are all manually initiated through* bypass ~~*individual keylock*~~ *switches within each of the four divisions. Each* bypass switch~~*BPU*~~ *sends a separate bypass signal for all four channels to the* ~~*TLU*~~TLF *in the same division for channel sensors bypass and MSL isolation trip special bypass. Each* bypass switch~~*BPU*~~ *sends the* ~~*TLU*~~TLF *bypass signal to the OLU in the same division.*

The ~~*TLUs* trip logic functions (~~TLFs~~)~~ *perform automatic scram initiation logic based on reactor operating mode, channel and division trip conditions and bypass conditions. Each* ~~*TLU*~~ TLF *receives* ~~*bistable*~~ bypass *input signals from the* bypass switch~~*BPU*~~ *and various switches in the same division and receives isolated* ~~*bistable*~~ trip *inputs from all four sensor channels* of RPS *and divisions of the NMS.*

The OLUs perform division trip, seal-in, reset and trip test function. Each OLU receives bypass inputs from the bypass switch~~*BPU*~~, *trip inputs from the* ~~*TLU*~~TLF *and various manual inputs from switches within the same division and provides* *discrete trip outputs to the trip actuators in the same division. Each OLU also receives an isolated discrete division trip reset permissive signal from equipment associated with one of the two divisions of scram logic circuitry.*

*All equipment within a division of trip logic is powered from the same division of Class 1E power source. However, different pieces of equipment may be powered from separate DC power supplies, and the ~~BPU, TLU~~*TLF *and OLU within a division must be powered from separate DC power supplies.*

The COLA Part 7 Description for Departure STD DEP T1 3.4-1 will be revised as follows in a future COLA revision.

(3) Clarifications of digital controls nomenclature and systems

The reference ABWR DCD defined many functional design requirements in terms typically reserved for hardware. Examples include the terms “module,” “unit,” and “system.” the terminology was corrected to refer to the requirement as a “function.” The terminology was corrected to refer to the requirement as a “function” to eliminate the confusion associated with purely functional requirements and not physical requirements defined in the DCD.

Examples include:

- Digital Trip Module (DTM) to Digital Trip Function (DTF)
- Trip Logic Unit (TLU) to Trip Logic Function (TLF)
- Safety System Logic Unit (SLU) to Safety System Logic Function (SLF)
- Plant Computer System (PCS) to Plant Computer Function (PCF)
- Essential Multiplexer System (EMS) to Essential Communication Function (ECF)
- Bypass Unit (BPU) to Bypass Interlock Function

RAI 07.02-3

QUESTION:

In Departure STD DEP T1 3.4-1, STPNOC took a deviation from the certified ABWR DCD on the safety-related instrumentation and control (I&C) architecture. In the safety related reactor protection system (RPS), the reference DCD Section 7.2.1.1.6.1(3) requires 5 milliseconds or more for all sequence-of-event (SOE) signals. But for the proposed new I&C architecture, the COLA FSAR changed the time resolution to 25 milliseconds or more for the safety-related nuclear steam supply system (NSSS) systems while keeping the original time resolution for the non-safety related balance-of plant (BOP) systems. Provide sufficient information to support this change.

RESPONSE:

STP 3&4 COLA Rev. 3, Part 2, Tier 2, Subsection 7.2.1.1.6.1(3), will be changed in a future revision as follows to revert to the reference ABWR DCD value of 5 ms for the sequential events interval.

~~*(3) Computer Alarms*~~

~~*Upon detection of a status change of any of the preselected sequential events contacts, the sequence-of-events log shall be initiated and shall signal the beginning of an event. This log will include both NSSS and BOP inputs. Changes of state received 5 milliseconds or more apart*~~ ~~for BOP systems and approximately 25 milliseconds or more apart for NSSS systems~~ ~~*are sequentially differentiated on the printed log, together with time of occurrence, which shall be printed in hours, minutes, seconds, and milliseconds. Use of the alarm typewriter and computer is not required for plant safety. The printout of trips is particularly useful in routinely verifying the correct operation of pressure, level, and valve position switches as trip points are passed during startup, shutdown, and maintenance operations.*~~

RAI 07.02-4

QUESTION:

In Departure STD DEP T1 3.4-1, STPNOC took deviations on the data communication and other systems from the generic ABWR DCD. Revise the original COLA FSAR Figure 7A-1 in section 7A accordingly to reflect all the changes contained in Departure STD DEP T1 3.4-1.

RESPONSE:

Figure 7A-1, Safety System Logic and Control (SSLC), was replaced with Figure 7.9S-1, Data Communications Interfaces. This removal should have been identified in the COLA and will be included in Tier 2, Appendix 7A in a future revision as shown below.

Figure 7A-1 ~~***Safety System Logic and Control (SSLC)***~~ **Not Used (See Figure 7.9S-1)**

RAI 07.02-5

QUESTION:

The NRC Staff requests that STPNOC address the following items in the COL application:

1. Departure STD DEP T1 3.4-1 proposed to eliminate references to the essential multiplexing system (EMS). However, EMS is still used in COLA FASR Tier 2 Section 7.2.1.1.4.2(2)(d). Correct this inconsistency.

2. STD DEP 7.3-5, Water Level Monitoring, proposed to use the standard ABWR nomenclature of Level 1.5, Level 1, etc. to replace "Low", "Low-Low", respectively. However, COLA FSAR Tier 2 Section 7.2.2.1(3), 7.2.2.2.3.1(12)(a), Table 7.2-2, 7.3.1.1.1.1(3), 7.3.1.1.1.3(h) still use low-water level. Correct this inconsistency.

3. COLA FSAR Sections 7.2.2.2.3.1(8), (10), and (12) refer to Paragraphs 4.8, 4.10, and 4.12 of IEEE 603-1991. Should the referenced Paragraphs be 6.4, 6.5, and 6.6 of IEEE 603-1991, respectively? Update these sections accordingly.

4. "Transducers" for level and pressure have been changed to transmitters in some places, such as Section 7.3.1.1.1.3 in the COLA FSAR, but it's not changed in other places. To be consistent, STPNOC should change transducer to transmitter throughout, as appropriate.

5. "RCIC is automatically isolated on detection or high steam flow or high temperature..." in section 7.3.1.1.1.3(4)(a) should be changed to "RCIC is automatically isolated on detection of high steam flow or high temperature..."

6. COLA FSAR Section 7.2.2.2.4 does not show the range for the turbine first-stage pressure, as claimed in departure STD DEP 7.2-6. Correct this inconsistency.

7. COLA FSAR Section 7A.2, Revised Response (7) includes 125 VAC which should be changed to 120 VAC.

8. COLA FSAR Section 7A.7, Items 7A.5(4) and 7A.6(4) includes RTIF which should be revised to RTIS.

9. COLA FASR Tier 2 Section 7.7.1.5(7)(c) used ARRM which should be changed to APRM.

10. COLA FASR Tier 2 Section 7.7.1.7(1) used PGS which should be changed to PGCS.

11. Departure STD DEP 7.3-18 is referred to in COLA FSAR Section 7.3, but COLA Part 7, Departures Report" does not include this departure. Correct this inconsistency.

12. Departure STD DEP 7.3-1 includes only two subsections for replacing the specific time interval with reference to Table 6.3-1. But, the specific time interval has also been replaced with reference to Table 6.3-1 in Section 7.3.1.1.1.3. Correct this inconsistency.

13. In Evaluation Summary of STD DEP 7.3-13, it says "Also, it does affect any method..." Should this be revised to read "Also, it does not affect any method..."? Update this section accordingly.

14. Section 7.1.2.6.2(1)(d) still uses the system logic on high radiation in the MSL tunnel area although Departure STD DEP T1 2.3-1 deleted the logic related to the high radiation in the MSL tunnel area. Correct this inconsistency.

15. Section 7.5.2.1(2)(b) in COLA FSAR should be revised to 7.5.2.1(2)(a).

RESPONSE:

Below are responses to the fifteen requests in this RAI. Corrections to the indicated items have been made in COLA Revision 3 or will be submitted in a future COLA revision.

1. Reference to 'EMS' was removed from Subsection 7.2.1.1.4.2(2)(d) in STP 3&4 COLA Revision 3.

2. Response to this request is broken into three parts.

   - FSAR Subsections 7.2.2.1(3), 7.2.2.2.3.1(8)(a), 7.2.2.2.3.1(12)(a) and Table 7.2-2 are related to STD DEP 7.3-5 which will be revised as shown below. Reactor Water Level input to the scram function of RPS is Level 3. '(Level 3)' will be added to each instance for clarity.

     The first sentence in Subsection 7.2.2.1(3) will be changed as shown below:

     The scram initiated by the main steamline ~~radiation monitoring system~~ isolation valve closure and reactor vessel low-water level (Level 3) *satisfactorily limits the radiological consequences of gross failure of the fuel or RCPB.*

     Subsection 7.2.2.2.3.1(8)(a) will be changed as shown below:

     (a) Reactor vessel low water level (Level 3) *trip*

     Subsection 7.2.2.2.3.1(12)(a) will be changed as shown below:

     (a) Reactor vessel low water level (Level 3) *trip*

In Table 7.2-2, the following line corresponding to water level will be changed as shown below:

Table 7.2-2 Channels Required for Functional Performance of RPS

~~*Reactor vessel low level*~~	~~*4*~~

This table shows the number of sensors required for the functional performance of the reactor protection system.	
Channel Description	**# Sensors**
Reactor vessel low level **(Level 3)**	*4*
~~*Main steamline radiation*~~	~~*4*~~

In COLA Part 7, Section 3.0, STD DEP 7.3-5 the description will be revised to identify for clarity the addition of the Level 3 designation to the RPS low water level trip as follows:

> Subsections 7.3.1.1.1.2 and 7.3.1.1.1.4 of the reference ABWR DCD describes the equipment design for the ADS and RHR/LPFL I&C using the terms "Low" and "Low- Low" when describing the initiation inputs from the Reactor Water Level instrumentation. These terms are replaced by the standard ABWR nomenclature of Level 1.5 and Level 1, respectively, for initiating signals. This instrumentation also provides initiating signals for other levels, such as Level 2, Level 3, and Level 8, etc. Additional clarity for low water level initiating a scram is achieved by adding "(Level 3)" after "Reactor vessel low water level" in Subsections 7.2.2.1 (3) and 7.2.2.2.3.1 (8)(a) and (12)(a), and Table 7.2-2.

- In Subsection 7.3.1.1.1.1(3), it is not appropriate to reference Level 1.5 in the first paragraph under item (a) as indicated. For clarity, the word "low" will be removed and the sentence will read "Reactor vessel water level is monitored..." The next paragraph from the DCD (not changed) explains how drywell pressure is monitored. The subsequent COLA paragraph explicitly states that reactor water level, Level 1.5, or high drywell pressure initiates HPCF. There is no confusion in this section.

The first sentence in the first paragraph of Subsection 7.3.1.1.1.1(3) under (a) Initiating Circuits will be changed as shown below:

> *Reactor vessel ~~low~~ water level is monitored by four level transmitters (one in each of the four electrical divisions) that sense the difference between the pressure due to a*

constant reference leg of water and the pressure due to the actual height of water in the vessel.

- The reference to Subsection 7.3.1.1.1.3(h) appears to be in error and the indicated instance could not be found. However, "(Level 2)" will be added to Sections 7.3.1.1.1.3(4)(b) and 7.3.1.1.1.3(4)(d) for clarity as reactor water Level 2 or high drywell pressure will initiate RCIC. FSAR Subsection 7.3.1.1.1.2(3)(h) will also be clarified.

  The first sentence in Subsection 7.3.1.1.1.2(3)(h) will be changed as shown below:

  The signal cables, solenoid valves, SRV operators and accumulators, and RV low-water level (Level 2) *instrument lines are the only essential I&C equipment for the ADS located inside the drywell.*

  The second sentence in Subsection 7.3.1.1.1.3(4)(b) will be changed as shown below:

  The scheme used for initiating the RCIC System is shown in Figure 7.3- 3 (RCIC IBD). RCIC initially starts on the sensing of either a low water level signal (Level 2) or a high drywell pressure signal. This initiates a sequence of valve openings and a RCIC turbine ramp rate which results in rated flow to the reactor vessel in a time interval consistent with Table 6.3-1.

  The first sentence in the second paragraph of Subsection 7.3.1.1.1.3(4)(d) will be changed as shown below:

  The RCIC System is actuated by high drywell pressure or by reactor low water level (Level 2).

3. COLA FSAR Subsection 7.2.2.2.3.1 was revised from IEEE 279 to IEEE 603. Cross references were revised accordingly. However the subsections referenced in the RAI were not updated. The Section References will be replaced with appropriate sections.

   Subsection 7.2.2.2.3.1 will be changed as shown below:

   (8) Derivation of System Inputs (Paragraph ~~4.8~~6.4)

   (10) Capability for Test and Calibration (Paragraph ~~4.10~~6.5)

   (12) Operating Bypasses (Paragraph ~~4.12~~6.6)

4. The terms "transducer" and "transmitter" for level and pressure can be used interchangeably. Both convert an input into an electrical output signal. A search of the ABWR DCD Part 2 Tier 2 and COLA Revision 2 has identified the following additional sections where transducers are referenced: FSAR Subsections 7.2.1.1.4.1(1), 7.2.1.1.4.2(2), 7.3.1.1.1.1(1), 7.7.1.8(10), 10.4.1.5.2 and FSAR Figure 7.2-2. The existing application of this term is considered acceptable.

No COLA Change is required with response to this RAI question.

5. This was a typographic error. In COLA Revision 3 the "or" was replaced with "of" in the eighth paragraph in Subsection 7.3.1.1.1.3(4)(a) as shown below:

   RCIC is automatically isolated on detection ~~or~~of high steam flow or high temperature in the RCIC room. Either of these is an indication of a steam line leak or break.

6. This is not in Subsection 7.2.2.2.4, rather it is in Table 7.2-1 which follows the referenced section in COLA Revision 2. STD DEP T1 2.2-1 was revised and the discussion of the turbine first stage pressure input signal to RPS was reverted back to the DCD description. STD DEP 7.2-6 added turbine first-stage pressure to Table 7.2-1; however, the range was omitted during final word processing. The range of 0-6 MPaG has been added to FSAR Table 7.2-1 in COLA Revision 3.

7. The revised response to NRC Request (7) in COLA FSAR Section 7A.2 contained a typographical error. "125" will be replaced with "120".

   The Revised Response (7) will be corrected as shown below:

   Revised ***Response (7)***—Multiplexers are not used. Safety related data communication is performed as an integral function of the SSLC systems. *The ~~multiplexer system~~* equipment implementing the ECFs *receives its power from the four-divisional battery-backed* ~~125~~120 *~~VDC~~* VAC *buses (*uninterruptible*). These are discussed in Subsection 8.3.2 and illustrated in Figure 8.3-4.*

8. Revised responses in COLA FSAR Subsection 7A.7, Items 7A.5(4) and 7A.6(4) contains a typographical error. 'RTIF' will be replaced with 'RTIS'.

   The Second Paragraph of the Revised Response for Items 7A.5(4) and 7A.6(4) will be corrected as shown below:

   In order to reduce plant construction costs and simplify maintenance operation, the ABWR protection systems are designed with a partially *"shared sensors" concept. The ~~SSLC~~* ~~RTIF~~RTIS System *is the central processing mechanism ~~and~~* that *produces logic decisions for both RPS and* MSIV isolation functions. The ELCS is the central processing mechanism that produces logic decisions for all *ESF safety system functions. Redundancy and "single failure" requirements are enhanced by a full fourdivision modular design using two-out-of-four voting logic on inputs derived from LOCA signals which consist of diverse parameters (i.e., reactor low level and high drywell pressure). Many additional signals are provided, in groups of four or more, to initiate RPS scram (Table 7.2-2).*

9. COLA FSAR Section 7.7.1.5(7)(c) contained a typographical error. In COLA Revision 3, 'ARRM' has been corrected in the second sentence to read 'APRM'.

10. COLA FSAR Subsection 7.7.1.7(1) contains a typographical error, 'PGS' will be replaced with 'PGCS'.

    The seventh sentence of Subsection 7.7.1.7(1) will be corrected as shown below:

    The ~~PGS~~PGCS performs the overall plant startup, power operation, and shutdown functions.

11. STD DEP 7.3-18 was not included in COLA Revision 0 although it was listed associated with COLA FSAR Section 7.3. References to this departure, which was not used, will be deleted from FSAR Section 7.3 and COLA Part 7 Section 5.

    In COLA Revision 3, STD DEP 7.3-18 was deleted from the list of Departures in Section 7.3 as shown below:

    STD DEP 7.3-17
    ~~STD DEP 7.3-18 (Figures 7.3-1, 7.3-2)~~
    STD DEP 7.7-2

    In COLA Part 7 Table 5.0-1, the following line will be changed as shown below:

~~STD DEP 7.3-18~~	~~Tier 2 Section 7.3~~

    In COLA Part 7 Table 5.0-2, the following line has been changed in the COLA Revision 3 as shown below:

~~Tier 2 Section 7.3~~	~~STD DEP 7.3-18~~

12. The COLA Part 7 departure description will be revised to add RCIC and reference to FSAR section 7.3.1.1.1.3

    The first sentence of STP 3&4 COLA Part 7 STD DEP 7.3-1 Description will be revised as follows:

    Subsections 7.3.1.1.1.1, 7.3.1.1.1.3 and 7.3.1.1.1.4 of the reference ABWR DCD provide specific times for the High Pressure Core Flood System, the Reactor Core Isolation Cooling System and the Low Pressure Flooder

    The first sentence of the second paragraph of the Evaluation Summary will be revised as follows:

> Specific response times for the Low Pressure Flooder, Reactor Core Isolation Cooling, and the High Pressure Core Flood systems exist both in the text narrative in Section 7.3 and in tables in Section 6.3 of the DCD.

13. The Evaluation Summary for STD DEP 7.3-13 provided in COLA Revision 2 Part 7 contains a typographical error, "not" will be added to the discussion of methods used for evaluation.

    The ninth sentence of STP 34 COLA Part 7 Departure Report, STD DEP 7.3-13 Evaluation Summary will be revised as follows:

    > Also, it does not affect any method used for evaluation in establishing the design bases or in the safety analyses.

14. As noted in STD DEP T1 2.3-1 of COLA Revision 2 Part 7 Departures Report, information pertaining to main steam line (MSL) high radiation monitoring and process radiation monitoring system was to have been deleted from Section 7.1.

    Contents of Subsection 7.1.2.6.2(1)(d) will be deleted entirely and replaced with "Not Used" as shown below:

    > *(d)* Not Used ~~*Provide channel trip inputs to the RPS and LDS*~~ ~~to the system logic~~ ~~*on high radiation in the MSL tunnel area. If the*~~ ~~protection system logic is satisfied,~~ ~~*the following shall be initiated:*~~ ~~system will initiate shutdown of the mechanical vacuum pump and closure of the mechanical pump discharge line isolation valve.~~
    >
    > ~~*(i) Reactor scram.*~~
    >
    > ~~*(ii) Closure of the main steamline isolation valves.*~~
    >
    > ~~*(iii) Shutdown of the mechanical vacuum pump and closure of the mechanical pump discharge line isolation valve.*~~

15. The FSAR Subsection 7.5.2.1(2) pertaining to Drywell Pressure was incorrectly renumbered duplicating the number used for the Containment Pressure (Wetwell Pressure). The numbering in Subsection 7.5.2.1(2) for Drywell Pressure has been corrected in COLA Revision 3.

RAI 14.03.05-4

QUESTION:

Based on Tier 1 departure STD DEP T1 3.4-1, the applicant, in the FSAR Tier 1 Table 2.7.5, has primarily taken departures that relate to nomenclature changes resulting from the proposed I&C architecture. As described in Tier 1 Section 2.7.5, the essential communication functions are accomplished as a part of the safety related I&C systems and equipment that make up Safety System Logic and Control (SSLC). The non-essential communication functions are performed through a plant wide, distributed network identified as the Plant Data Network (PDN) system. The proposed data communication architecture is significantly different from the certified Multiplexing System. The NRC Staff requests that STPNOC include the inspections, test, and/or analysis that address specific features of the proposed data communication functions inherent to the SSLC platforms, such as timing and load, etc. In addition, Item 3 of Table 2.7.5 states that "Data cannot be transmitted from the non-safety-related side to equipment implementing the ECFs." However, there is a data communication from the non-safety-related side to the safety-related system although the transmission is manually controlled. The NRC Staff requests that STPNOC provide sufficient clarification for this inconsistency and include the test and inspection of this manually controlled data communication as an ITAAC item in Table 2.7.5. Refer to RAI 3139 related to Chapter 7.9S for additional information.

RESPONSE:

The safety-related I&C systems are deterministic. The response times for the system elements, including architecture, communications (including timing and loading) and processing elements will be analyzed in accordance with BTP 7-21 to verify that the systems' performance characteristics are consistent with the safety requirements established in the design basis for these systems.

The NRC requests clarification for the manual transfer of data from nonsafety-related to safety-related equipment implementing the ECFs. STPNOC's response to RAI 07.09-1 clarifies the design and administrative controls provisions to implement this transfer of data. That is, the NMS also includes a separate off-line method that is used to transfer calibration data from PICS to the NMS. When the NMS is online and not bypassed, data transfer to the NMS from the non-safety system is blocked by a key-lock switch. When calibration information is to be transferred from the nonsafety-related core monitor function of the PCF, the NMS division desired to receive the information must be placed in an inoperative status and a key lock switch must be enabled to allow the data transfer. Only a limited data set in a predefined format will be accepted by the NMS. Before the data can be utilized by the NMS, manual verification and acceptance is required.

Regarding the request for additional ITAAC, STPNOC's position is that the existing ITAAC is appropriate as discussed in the response to RAI 14.03.05-8.

STP 3&4 COLA Part 2, Tier 1, Subsection 2.7.5, sixth paragraph below Essential Communication Functions (ECF), is being changed as shown below.

Data communication from safety-related to non-safety related systems or devices is isolated through the use of an isolating transmission medium and buffering devices. Data cannot be transmitted from the non-safety side to safety related equipment when the equipment is in service.

RAI 14.03.05-5

QUESTION:

Based on STD DEP T1 3.4-1, the applicant revised the I&C architecture related nomenclature used in Table 3.4, ITAAC Item 3 Design Commitment. However, the types of Class 1E power sources was not changed, which is now inconsistent with the proposed power sources for RTIS and ELCS described in Tier 1 subsection A of Section 3.4. Also, the revised Design Commitment does not include the equipment implementing the ESF SLF in Division IV, and ESF RDLC in all four divisions. The NRC staff requests STPNOC to resolve this inconsistency between ITAAC Design Commitment and Tier 1 Design Description, and identify the ITAAC that addresses the equipment implementing the ESF SLF in Division IV, and ESF RDLC in all four divisions.

RESPONSE:

STD DEP T1 3.4-1 revised COLA Part 2, Tier 1, Subsection 3.4.A to generically reference Class 1E for power sources of SSLC instead of specific Class 1E AC or Class 1E DC power. This was done for clarification, following the architectural splitting of Safety System Logic and Control (SSLC) into Reactor Trip and Isolation System (RTIS) (AC powered) and ESF Logic and Control System (ELCS) (DC powered). COLA Part 2, Tier 1, Table 3.4, ITAAC Item 3 Design Commitment specifically references Class 1E AC power for RTIS and Class 1E DC power for ELCS; however, for consistency, COLA Part 2, Tier 1, Subsection 3.4.A will be revised as shown below.

STD DEP T1 3.4-1 further revised the ITAAC Design Commitment to replace for RTIS the references to Digital Trip Module (DTM) and Trip Logic Unit (TLU) with equipment implementing the Digital Trip Function (DTF) and Safety Logic Function (SLF), respectively. The ITAAC Design Commitment, as described in the COLA Part 2, Tier 1, Table 3.4, is correct. The ELCS is comprised of four divisions of inputs and DTFs, which feed the three divisions of SLFs corresponding to the three divisions of ESF equipment to perform the safety functions.

The ABWR DCD Tier 1, Table 3.4 ITAAC Item 3 Design Commitment listed for ELCS the references to DTM and SLU for Divisions I, II and III and the DTM for Division IV. The departure has modified this to identify the DTF and SLF for Divisions I, II, and III and the DTF for Division IV, which is correct.

For the STP 3 & 4 COLA, STD DEP T1 3.4-1 effectively replaced the Remote Multiplexing Unit (RMU) with the Remote Digital Logic Controllers (RDLC). The RDLC is generically covered under COLA Part 2, Tier 1, Table 2.7.5 ITAAC Item 6 Design Commitment, as part of each division of equipment implementing the Essential Communication Function (ECF) which lists the same divisional Class 1E power as COLA Part 2, Tier 1, Table 3.4 ITAAC Item 3.

COLA Part 2, Tier 1, Subsection 3.4.1 (to be changed back to Subsection A) under "The ELCS portion of SSLC ..." after the Item (4) paragraph is being revised and will be included in a future COLA revision. Changes are shown in gray shading.

~~*"The DTM, TLU, and OLUs for RPS and MSIV in each of the four instrumentation divisions are powered from their respective divisional Class 1E AC sources. The DTMs and SLUs for ESF 1 and ESF 2 in Divisions I, II, and III are powered from their respective divisional Class 1E DC sources.*~~ RTIS and ELCS equipment is ~~divisionally~~ powered from their respective divisional~~multiple~~ Class 1E ~~AC~~ power sources. ~~at least one of which is DC backed (uninterruptible).~~ ~~*In SSLC, independence*~~ For RTIS, the equipment implementing the DTF, TLF, and OLUs for RPS and MSIV in each of the four instrumentation divisions is powered from their respective divisional Class 1E AC sources. For ELCS, the equipment implementing the DTF and SLF for ESF in Divisions I, II and III is powered from their respective divisional Class 1E DC sources, as is the equipment implementing the ESF DTF in Division IV. Independence is *provided between Class 1E divisions, and also between Class 1E divisions~~,~~ and ~~also~~ non-Class 1E equipment."*

RAI 14.03.05-6

QUESTION:

Based on STD DEP T1 3.4-1, the applicant revised the ESF output channel bypass design commitment and related ITA and acceptance criteria in Table 3.4, ITAAC Item 4. The staff is unable to evaluate this change due to the vagueness of the departed ESF design description in Tier 1 Section 3.4 (RAI 3213, Question 12836). The NRC staff requests STPNOC to evaluate the impact on this ITAAC resulting from potential changes to the ESF design description.

RESPONSE:

The Engineering Safety Features (ESF) output channel bypass described in the reference ABWR DCD is to account for failure of a redundant Safety System Logic Function (SLF) detected with self-diagnostics. STD DEP T1 3.4-1 changes the architecture as described in the departure description. The final 2 out of 2 vote performed on functions requiring redundant SLF processing is performed in non-microprocessor based hardware as described in COLA Part 2, Tier 1, Section 3.4.A for ESF Logic and Control System (ELCS) processing step (3). Also, the functions that are implemented with redundant SLF processors are described in the same section and based on COLA Part 2, Tier 2, Section 16 B 3.3.1.4.

The output channel bypass remains in the ESF design. The ITA and Acceptance Criteria in Table 3.4, ITAAC Item 4 have been modified as part of STD DEP T1 3.4-1. The modification of the ITA accounts for nomenclature change from Safety System Logic Unit (SLU) to SLF and the removal of the Remote Multiplexing Unit (RMU). The ITA c(1) remains functionally the same as in the DCD. ITA c(2) repeats the testing of c(1), but with the automatic output channel bypass disabled and a manual output channel bypass operating. ABWR DCD ITA 4c(2) and Acceptance Criteria 4c(2) will be restored to Tier 1 Table 3.4 with the nomenclature changes as shown below.

Tier 1, Subsection 3.4.A deleted the description of the output channel bypass. The replacement text is being added as shown below.

> ~~*ESF1 and ESF2 logic are each processed in two redundant channels within each divisional train of ESF equipment. In order to prevent spurious actuation of ESF equipment, final output signals are voted 2-out-of-2 at the remote multiplexing units by means of series-connected load drivers at the RMU outputs. However, in the event of a failure detected by self-test within either processing channel, a bypass (ESF output channel bypass) is applied automatically (with manual backup) such that the failed channel is removed from service. The remaining channel provides 1-out-of-1 operation to maintain availability during the repair period. Channel failures are alarmed in the main control room. If a failed channel is not automatically bypassed, the operator is able to manually bypass the channel by a hardwired connection from the main control room.*~~ In the ELCS, the two redundant SLF processing channels must agree for initiation of the ESF safety function to occur. Two SLF processing channels are used to prevent the inadvertent system level actuation of the ESF safety functions that inject coolant to the core or depressurize the reactor vessel.
>
> However, in the event of a failure detected by self diagnostics within either processing channel, a bypass (ESF output channel bypass (with manual backup)) is provided such that the failed SLF processing channel is removed from service. The remaining SLF processing channel provides one-out-of-one operation to maintain availability during the repair period. SLF processing failures are alarmed in the main control room. If a failed channel is not automatically bypassed, the operator can manually bypass the failed channel.

COLA Part 2, Tier 1, Table 3.4 Instrumentation and Control will be revised as shown below.

Inspections, Tests, Analyses and Acceptance Criteria		
Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
Safety System Logic and Control		
4. SSLC provides the following bypass functions: a. Division-of-sensors bypass b. Trip logic output bypass c. ESF output channel bypass, **where applied**	4. Tests will be performed on the as-built SSLC as follows:	4. Results of bypass tests are as follows:
	a(1) Place one division of sensors in bypass. Apply a trip test signal in place of each sensed parameter that is bypassed. At the same time, apply a redundant trip signal for each parameter in each other division, one division at a time. Monitor the voted trip output ~~at~~ from each ~~TLU and SLU~~ **equipment component that implements a TLF or SLF**. Repeat for each division.	a(1) No trip change occurs at the voted trip output ~~of~~ **from** each ~~TLU and SLU~~ **equipment component that implements a TLF or SLF**. Bypass status is indicated in main control room.
	a(2) For each division in bypass, attempt to place each other division in division-of- sensors bypass, one at a time.	a(2) Each division not bypassed cannot be placed in bypass, as indicated at OLU output; bypass status in main control room indicates only one division of sensors is bypassed.
	b(1) Place one division in trip-logic-output bypass. Operate manual auto-trip test switch. Monitor the trip output at the RPS OLU. Operate manual autoisolation test switch. Monitor the trip output at the MSIV OLU. Repeat for each division.	b(1) No trip change occurs at the trip output of the RPS OLU or MSIV OLU, respectively. Bypass status is indicated in main control room.
	b(2) For each division in bypass, attempt to place the other divisions in trip-logic- output bypass, one at a time.	b(2) Each division not bypassed cannot be placed in bypass, as indicated at OLU output; bypass status in main control room indicates only one trip logic output is bypassed.
	c(1) Apply common test signal to any one pair of ~~dual-SLU~~ **redundant SLF** signal inputs. Monitor test signal at ~~voted 2-out-of-2~~ output ~~in RMU area~~ **from equipment performing the ECF in local areas**. Remove power from **equipment performing** one *SLU* **SLF**, restore power, then remove power from equipment performing other ~~SLU~~ **SLF**. Repeat test for all pairs of ~~dual SLUs~~ **redundant sets of equipment implementing a SLF** in each division.	c(1) Monitored test output signal does not ~~change state~~ **initiate the system function** when power is removed from ~~either SLU~~ **the equipment performing any single SLF**. Bypass status and loss of power to ~~SLU~~ **equipment performing the SLF** are indicated in main control room.
	c(2) Disable auto-bypass circuit in bypass unit. Repeat test c(1), but operate manual ESF loop bypass switch for each affected loop.	c(2) Monitored test output signal is lost when power is removed from either ~~*SLU*~~ **SLF**, but is restored when manual bypass switch is operated. Bypass status, autobypass inoperable, and loss of power to ~~*SLU*~~ **SLF** are indicated in main control room.

RAI 14.03.05-7

QUESTION:

Based on STD DEP T1 3.4-1, the applicant changed EMS to ECF and NEMS to NECF in Table 3.4, ITAAC Item 12. This ITAAC is for EMC compliance testing of the electrical and electronic components used in the SSLC and other microprocessor-based, software controlled equipment. Note that ECF and NECF are functions and not the electrical or electronic components they replaced, namely essential and non-essential multiplexing systems. The NRC staff requests STPNOC to evaluate the applicability of ITAAC Item 12 to ECF and NECF.

RESPONSE:

STP 3&4 COLA Tier 1 Table 3.4, ITAAC Item 12 requires the COL applicant to develop an Electromagnetic Compatability (EMC) Qualification Plan that requires, for each system qualified, system documentation that includes confirmation of component and system testing for the effects of high electrical field conditions and current surges. The DCD explicitly listed the Essential Multiplexing System (EMS) and Non-Essential Multiplexing System (NEMS) in this ITAAC item. STD DEP T1 3.4-1 changed nomenclature of EMS and NEMS to ECF and NECF respectively. The STP 3&4 EMC Qualification Plan, U7-PROJ-J-P-EN02-0001, includes qualification of all equipment related to safety functions and explicitly calls out the ECF and NECF. Refer to the STPNOC response to RAI 07.08-1 for details regarding the EMC Equipment Qualification Plan. For clarity, ITAAC Item 12 will be revised to explicitly state "equipment performing the Essential Communication Function (ECF)" and "equipment performing the Non-Essential Communication Function (NECF)" to retain the intention of the DCD ITAAC in a future revision.

COLA Tier 1 Table 3.4 ITAAC, Item 12, will be revised as shown below. Changes are shown in gray shading.

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
Electromagnetic Compatibility		
12. Electrical and electronic components in the systems listed below are qualified for the anticipated levels of electrical interference at the installed locations of the components according to an established plan: a. Safety System Logic and Control b. ~~*Essential Multiplexing System*~~ **Equipment performing the Essential Communication Function (ECF)** c. ~~*Non-Essential Multiplexing System*~~ **Equipment performing the Non Essential Communication Function (NECF)** d. Other microprocessor-based, software controlled systems or equipment The plan is structured on the basis that electromagnetic compatibility (EMC) of I&C equipment is verified by factory testing and site testing of both individual components and interconnected systems to meet EMC requirements for protection against the effects of: a. Electromagnetic Interference (EMI) b. Radio Frequency Interference (RFI) c. Electrostatic Discharge (ESD) d. Electrical surge [Surge Withstand Capability (SWC)]	12. The EMC compliance plan will be reviewed.	12. An EMC compliance plan is in place. The plan requires, for each system qualified, system documentation that includes confirmation of component and system testing for the effects of high electrical field conditions and current surges. As a minimum, the following information is documented in a qualification file and subject to audit: a Expected performance under test conditions for which normal system operation is to be ensured. b. Normal electrical field conditions at the locations where the equipment must perform as above. c. Testing methods used to qualify the equipment, including: (1) Types of test equipment. (2) Range of normal test conditions. (3) Range of abnormal test conditions for expected transient environment.

RAI 14.03.05-8

QUESTION:

In enclosure 4f of the STPNOC letter U7-C-STP-NRC-090009, dated February 9, 2009, the applicant evaluated the Tier 1 ITAAC for conformance to the SRP 14.3. In this evaluation, STP concluded that the SRP 14.3 does not address specific DAC related ITAAC, therefore requirements of the SRP 14.3 are not applicable to the departed DAC/ITAAC in Tier 1, Chapter 3. Based on following reasons, the NRC staff requests STPNOC to reevaluate departed Tier 1 ITAAC for conformance to the SRP 14.3 guidance:

1. On SRP pages 14.3-21 and 14.3-22, definition of DAC and its use as additional certified design material is explained,

2. On page 14.3-22, the SRP states, "The design information and appropriate design methodologies, codes, and standards provided in the DCD Tier 2, together with the design descriptions and DAC, should be sufficiently detailed to provide an adequate basis for the staff to make a final safety determination regarding the design, subject only to satisfactory design implementation and verification of the DAC by the COL applicant or licensee. The DAC are a set of prescribed limits, parameters, procedures, and attributes upon which the NRC relies, in a limited number of technical areas, in making a final safety determination in support of the design certification. The acceptance criteria for the DAC should be objective; that is, they should be inspectable, testable, or subject to analysis using pre-approved methods, and should be verified as a part of the ITAAC performed to demonstrate that the as-built facility conforms to the certified design. Thus, the acceptance criteria for DAC are specified together with the related ITAAC in Tier 1, and both are part of the design certification. The DAC and the ITAAC, when met, ensure that the completed design and as-constructed plant conforms to the design certification. The material in the DCD Tier 2 for each of the DAC areas should include, as appropriate, sample calculations or other supporting information to illustrate methods that are acceptable to the staff for meeting the Tier 1 DAC commitments."

and

3. On page 14.3.5-5, the SRP states, "The applicant may provide design acceptance criteria (DAC) in lieu of detailed system design information. In this case, the DAC should be sufficiently detailed to provide an adequate basis for the Staff to make a final safety determination regarding the design, subject only to satisfactory design implementation and verification of the DAC by the COL applicant or licensee. Implementation of the DAC should be verified as part of the ITAAC performed to demonstrate that the as-built facility conforms to the certified design."

RESPONSE:

In STPNOC letter number U7-C-STP-NRC-09009, dated February 9, 2009, a response to the NRC request to address applicability of SRP 14.3 and 14.3.5 to STP 3&4 ITAAC was provided. STPNOC's response stated that:

> "STPNOC evaluated the guidance of SRP 14.3 and 14.3.5 to evaluate if any new ITAAC is warranted or if any existing ITAAC need to be modified as a result of the changes identified in STD DEP T1 3.4-1. The results of that evaluation are summarized in **Enclosure 4.f.**
>
> The I&C platform changes identified in STD DEP T1 3.4-1 are to the design of the subsystems that communicate the functions as described in the DCD, and do not change the functions themselves, the ITAAC as described in the DCD remain completely applicable and valid. Therefore changes to the I&C ITAAC are neither required nor appropriate. For clarity, the system nomenclature was updated, but this only changes the callout of the system performing the function, and does not change the function or acceptance criteria. Further, the changes in STD DEP T1 3.4-1 do not introduce any new functions in addition to those already described in the DCD, and therefore no new I&C ITAAC are necessary."

As requested in the RAI, the departed Tier 1 ITAAC have been reevaluated for conformance to SRP 14.3 and 14.3.5 guidance. A summary of this review and the conclusions are provided below. The following supersedes Enclosure 4.f of STPNOC letter U7-C-STP-NRC-09009.

- The ITAAC that can be considered I&C related Design Acceptance Criteria (DAC) are provided in STP 3&4 COLA Part 2 Tier 1, Section 3.4 Table 3.4 Items 7-15. This is supported by the ABWR DCD Subsection 14.3.3.4 and NUREG-1503 Section 14.3.3.4. As noted therein, the DAC provide the process and acceptance criteria by which the details of the I&C systems' design are developed, designed and evaluated.

- As discussed in STPNOC letter U7-C-STP-NRC-090009 as noted above, departure STD DEP T1 3.4-1 changes include elimination of obsolete data communication technology, elimination of unnecessary actuation logic, clarification of digital controls nomenclature, and surveillance changes. These changes do not have any impact on the overall I&C systems' development and qualification processes. Therefore, the current I&C DAC ITAAC are applicable and valid, and no new I&C related DAC ITAAC are warranted or necessary.

- The other I&C related ITAAC (including but not limited to FSAR Tier 1 Table 2.2.5, Table 2.2.7, Table 2.7.5, and Table 3.4 Items 1 though 6 and 16) verify I&C systems functionality. None of the I&C related ITAAC are platform specific. Departure STD DEP T1 3.4-1 changes related to elimination of obsolete data communication technology and clarification of digital controls nomenclature do not change functionality. Limited revisions have been made in COLA Part 2 Tier 1 Section 3.4 to address the STD DEP T1 3.4-1 elimination of unnecessary actuation logic and surveillance changes. No further changes are necessary, and no new I&C related ITAAC are warranted because STD DEP T1 3.4-1 does not introduce any new functionality.

Thus, the conclusions of STPNOC letter number U7-C-STP-NRC-09009, dated February 9, 2009, that the current I&C related ITAAC are adequate and that no new I&C related ITAAC are warranted, remain valid. The current DAC ITAAC support the SRP 14.3.5 guidance, in that the satisfactory design implementation and verification of these DAC will result in a design that meets the DCD requirements and satisfies the design basis as approved in the FSER. The mapping of detailed design documentation to the requirements of DAC related ITAAC will be completed in the ITAAC closure processes. A significant portion of the high-level documentation needed to implement the detailed design was identified in STPNOC letter U7-C-STP-NRC-09009, including the schedule for completion. The combination of detailed design documentation, technical reports and approved processes along with the ITAAC closure mapping of DAC requirements to implementing documents will provide adequate basis to demonstrate satisfactory implementation.

There is no COLA revision required as a result of this RAI response.