From:	Cook, James W [jwcook@STPEGS.COM]
Sent:	Monday, June 29, 2009 6:46 PM
To:	Muniz, Adrian; Wunder, George
Subject:	U7-C-STP-NRC-090065
Attachments:	ltr and attach.pdf

Please find attached a courtesy copy of the letter to the NRC providing responses to questions contained in RAI letter #104. The official paper copies will be sent according to the addressee list.

If you have any questions, please contact me.

James Cook

Licensing Engineer STP 3 & 4
jwcook@stpegs.com
(409)504-0337

Mail Envelope Properties   (C7F098E3C31A0141A02043F0B8E656EE6DD1F9B0)

Subject: U7-C-STP-NRC-090065
Sent Date: 6/29/2009 6:46:09 PM
Received Date: 6/29/2009 6:46:17 PM
From: Cook, James W

Created By: jwcook@STPEGS.COM

Recipients:
"Muniz, Adrian" <Adrian.Muniz@nrc.gov>
Tracking Status: None
"Wunder, George" <George.Wunder@nrc.gov>
Tracking Status: None

Post Office: exgmb1.CORP.STPEGS.NET

Files	Size	Date & Time
MESSAGE	388	6/29/2009 6:46:17 PM
ltr and attach.pdf	720937	

Options
Priority: Standard
Return Notification: No
Reply Requested: No
Sensitivity: Normal
Expiration Date:
Recipients Received:

June 29, 2009
U7-C-STP-NRC-090065

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
Response to Request for Additional Information

Reference: Letter, Scott Head to Document Control Desk, "Response to Request for
               Additional Information," dated June 15, 2009 (U7-C-STP-NRC-090056,
               ML091690066)

Attached are responses to NRC staff questions included in Request for Additional Information
(RAI) letter number 104 related to Combined License Application (COLA) Part 2 Tier 2
Chapter 7. This submittal completes the response to this RAI letter.

The attachments provide responses to the RAI questions listed below:

        RAI 07.01-1
        RAI 07.03-1

The referenced letter provided a partial response to RAI 07.01-1. Attachment 1 provides a
revised and complete response to this question.

Where a revision to the COLA is required, 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.

If you have any questions regarding these responses, please contact me at (361) 972-7136, or
Bill Mookhoek at (361) 972-7274.

STI 32496464

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

Executed on   _6/29/09_

Scott Head
Manager, Regulatory Affairs
South Texas Project Units 3 & 4

jwc

Attachments:

    1.   Question 07.01-1
    2.   Question 07.03-1

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

(electronic copy)

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

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

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

Steve Winn
Eddy Daniels
Joseph Kiwak
Nuclear Innovation North America

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

Jon C. Wood, Esquire
Cox Smith Matthews

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

Alice Hamilton Rogers, P.E.
Inspections Unit Manager
Texas Department of Health Services
P. O. Box 149347
Austin, Texas 78714-9347

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
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852

RAI 07.01-1

QUESTION:

The STPNOC response (U7-C-STP-NRC-090009) to the NRC audit refers to the Toshiba and Westinghouse platform topical reports for conformance with the NRC regulations. The NRC Staff requests that STPNOC clarify the scope of I&C departures in relation to these topical reports and provide sufficient information within COLA depending on the clarification of the scope.

RESPONSE:

This question focuses on departure STD DEP T1 3.4-1 which is the subject of the relevant portion of STPNOC letter U7-C-STP-NRC-090009. The question requests supplemental information regarding STPNOC's digital I&C design and use of the topical reports for DAC/ITAAC closure. Response to this request is also provided.

For clarity, this response is separated into two major presentations, the RTIS-NMS (non-rewritable (NRW) Field Programmable Gate Array (FPGA)) platform, and the Engineered Safety Features Logic and Control System (ELCS) (Common-Q) platform.

RTIS-NMS Platform

This part of the response has five major sections. The first section provides a system overview for the Neutron Monitoring System (NMS) and Reactor Trip and Isolation System (RTIS). The second section provides a description of the equipment that is utilized for the NMS and RTIS. The third section describes the COLA departures and the relationship of the COLA departures to the equipment description. The fourth section clarifies that the NRW-FPGA Topical Reports identified in Attachment 5 to U7-C-STP-NRC-090009 has been withdrawn from NRC and provides some details on the Design Acceptance Criteria audit process. The final section provides a COLA markup to include additional information on the NRW-FPGA based platforms.

System Overview

The Safety-Related NMS consists of the following safety-related subsystems:

- Startup Range Neutron Monitoring (SRNM),

- Local Power Range Neutron Monitoring (LPRM),

- Average Power Range Neutron Monitoring (APRM), including Oscillation Power Range Neutron Monitoring (OPRM).

The SRNM monitors neutron flux from the source range to 15% of the rated power. The SRNM includes the following major elements:

1. The SRNM Subsystem has 10 SRNM channels, each having one fixed in-core regenerative fission chamber sensor.

2. SRNM detector signals are assigned to four divisions.

3. SRNM monitors neutrons over a 10-decade flux range. The counting method is used in the lower range, and the Campbelling technique (mean square voltage, or MSV measurement) are used in the higher range.

4. The calculation algorithm of the period-based trip circuitry generates the trip margin setpoint for the period trip protection function.

5. The SRNM provides various outputs for control console displays and to the Plant Computer Functions (PCF).

6. The SRNM provides alarm and trip outputs to the RTIS and the Rod Control Information System (RCIS) separately for both high flux and short period conditions, and instrument inoperative trip.

7. The SRNM sends an interlock signal indicating whether the SRNM power level is above or below a specific setpoint level for use in Anticipated Transient Without SCRAM (ATWS) logic.

The Power Range Neutron Monitor (PRNM) system monitors reactor power by measuring neutron flux level and issues a trip signal to RTIS when specified setpoints are exceeded. The NMS also provides power information of operation and control of the reactor to the PCF and the rod block monitor. The PRNM includes the following major elements:

1. There are 208 LPRM detectors in the core. LPRM detector signals are divided and assigned to four APRM channels corresponding to four divisions.

2. LPRM monitors local neutron flux at each LPRM detector signal in the power range up to 125% of rated power.

3. APRM monitors average neutron flux of LPRM signals and generates a high neutron flux trip, a simulated thermal power trip signal, and a Core Flow Rapid Coastdown trip to the RTIS.

4. OPRM monitors the LPRM signals for core instability and generates trips for RTIS.

5. On operator demand, LPRM units receive gain adjustment calibration information from Plant Information and Control System (PICS) through the APRM unit and accepted on each PRNM.

6. The APRM sends an interlock signal to permit ATWS protection action.

7. Alarms to the operator warning of the impending and actual occurrence of trips.

8. Indications of PRNM System failures or operational problems.

The NMS also includes the following non safety-related subsystems:

- Multi-Channel Rod Block Monitor and

- Automated Traversing In-core Probe.

These subsystems are described in FSAR Section 7.7.

The RTIS initiates an automatic reactor trip (scram) when certain conditions are present (e.g., Reactor Water Level L-3, D/W Pressure High, Reactor Pressure High, etc.). The RTIS also initiates Main Steam Isolation Valve (MSIV) closure when certain conditions are present (e.g., Reactor Water Level L-1.5, Main Steam Line Flow High, etc.). The RTIS consists of the following:

- Digital Trip Function (DTF),

- Trip Logic Function, and

- Output Logic Unit.

RTIS includes the following major elements:

1. Use four redundant instrument channels and the replication of the entire two-out-of-four combinational logic in all four divisions of the trip logic.

2. Full implementation of the single failure criterion and the physical separation and electrical independence between the RTIS divisions to ensure no credible failure will affect or defeat more than one division.

3. The RTIS initiates an automatic reactor trip (scram) by different conditions (e.g., Reactor Water Level L-3, D/W Pressure High, Reactor Pressure High, etc.)

4. MSIV Closure Logic initiates an automatic MSIV closure from different conditions (e.g., Reactor Water Level L-1.5, Main Steam Line Flow High, etc.)

FPGA-based System Description

The Digital I&C System design for NMS and RTIS use NRW-FPGA-based safety-related I&C systems.

The 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. Data is transferred between units over fiber optic 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 printed circuit board runs through channels, guiding the assembly into a position where the connector will mate with the backplane.

The design of HMI and modifiable setpoints of each module are based on the design of conventional analog-based or CPU-based Systems, specifically, an aluminum front panel, which provides a flat, front surface for the discrete Light Emitting Diodes (LEDs) for status, numeric LEDs for values, and dedicated function pushbutton switches. The front panel also provides captive screws, to ensure that the printed circuit board remains in the unit and operable through seismic events. Status indicators are provided on the front panels (e.g., single-channel trip signal).

The FPGA-based system also includes power supplies, analog and digital input/output modules, status modules, and all cabling and wiring necessary for operation. As an example, the LPRM module consists of a front panel with an HMI, a printed circuit board, the analog circuitry necessary to interface to the in-core detector, power supply for the in-core detector, FPGAs, and a limited amount of additional logic. An FPGA can only implement digital logic.

The system design uses multiple FPGAs on each module. The FPGA incorporates logic cells linked by one-time configurable connections that logically interconnect cells to meet different function requirements. In addition to logic cells, other configurable elements of an FPGA are (1) Input/Output (I/O) blocks, which serve as the interface between internal signal lines and the chip's external pins; and (2) interconnects, which route input/output (I/O) signals to appropriate destinations.

The FPGA-based systems are composed of logic designed specifically to be physically embedded on 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. In the FPGA used for Safety-Related, 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.

The functions on a given module execute in sequence, and data is transferred between FPGAs over serial and parallel communication links. That is, the first FPGA completes its function, and then provides data to the next FPGA. When that FPGA completes its function, it provides data to the third FPGA. Only when all FPGAs have finished, passing data to the next, do the two watchdog timers on the module reset and restart timing. Failure of any FPGA to complete and pass data to the next FPGA will result in all subsequent FPGAs on that module failing to start.

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

example, the NRW-FPGA-based PRM units generate an inoperable signal when power loss occurs, which is treated as an inoperable channel and, therefore, initiates a single-channel trip signal.

The advantage of the FPGA platform is that the logic execution is completely defined, simple (compared to computer-based systems). FPGAs provide stable technology to minimize the risk of technology obsolescence. Because the FPGA is implemented directly in digital logic, the FPGA executes application logic without operating systems or application software. Further, the FPGAs provide permanent, non-volatile, unchangeable storage of the system configuration.

The qualification is primarily based on the Electric Power Research Institute (EPRI) Technical Report TR-107330 "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996. The software qualification approach described in EPRI TR-107330 has been modified to fit the NRW-FPGA technology.

Key features of this process include use of a modified software lifecycle approach for logic design and qualification, and use of small logic elements, called Function Elements, to implement the logic based on their simplicity and testability.

COLA Departure

The relevant I&C departure from Tier 1 information is STD DEP T1 3.4-1. As described in the COLA Part 7 markup provided in U7-C-STP-NRC-090009, STD DEP T1 3.4-1 consists of the following changes:

1. Elimination of obsolete data communication technology

2. Elimination of unnecessary inadvertent actuation prevention logic and equipment

3. Clarification of digital controls nomenclature and systems

4. Final selection of platforms changed the implementation architecture

5. Testing and surveillance changes for Safety System Logic and Control (SSLC)

Changes (1), (4) and (5) are related to the FPGA-based system.

Elimination of Obsolete Data Communication Technology – Change (1)

The STP 3 & 4 COLA replaces the previous communication technology with high speed serial links (HSLs) to communicate Class 1E information.

For the FPGA-based systems, the inputs from the instrumentation are hard wired to the modules. Data is transferred between FPGAs over serial communication links. Data is transferred over fiber optic links. The modules communicate using simple, dedicated internal communication links.

The communication data links provided in the RTIS and NMS system have a one-way fiber optic communication link, providing fixed data sets from each safety-related division individually to the nonsafety-related systems, providing 1E to non-1E isolation, and offering no possibility of data transfer from the nonsafety to the safety equipment. This design eliminates any potential for data from one division being supplied to another division. In addition, for the fielded systems, the current FPGA-based system designs have no provided means to attach personal computers or other software-based tools.

The LPRM and APRM calibration data is transmitted from the nonsafety-related core monitor function of PICS to the safety related NMS. Plant personnel action to manually accept the data transfer to the operational safety side is required for such data to be accepted. NMS can receive calibration data from nonsafety-related maintenance support systems. On a divisional level, a division must be manually placed in inop and manually verified and accepted before such data is allowed in the portion of the device performing the safety function. Only limited data in a strict format will be accepted by the safety device. Although COLA Tier 1 Section 2.7.5 indicates that, "Data cannot be transmitted from the non-safety side to safety related equipment," the acceptance criteria for ITAAC Item 3 in Tier 1 Table 2.7.5 further clarifies this statement by prohibiting the control and timing signals between safety-related equipment and non-safety related equipment. Thus, limited data transfer, such as the one for NMS calibration described above, is allowed from nonsafety-related systems to safety-related systems.

Final selection of platforms changed the implementation architecture – Change (4)

The FPGA-based systems are not microprocessor based. The FPGA-based systems use logic chips that can be configured. The systems are composed of logic that Toshiba designed specifically to be physically embedded in FPGA chips using special tools. The logic is built from simple 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.

Testing and surveillance changes for SSLC – Change (5)

The FPGA-based system has self-diagnostic functions that continuously verify proper FPGA and communications performance and provide outputs used to alert the operator. Failure of any FPGA to complete and pass data to the next FPGA will result in all subsequent FPGAs on that

module failing to start. If this occurs in the FPGAs that implement the safety functions, the module is marked as inoperable.

The previous section described the communication links. No other capabilities exist for communication with external devices. There are no software based support tools for use at the nuclear plants, and no need for such tools. Repair of equipment is normally accomplished by simple module replacement in the field. Maintenance activities consist of maintenance of the FPGA logic to remove latent errors, to address revised requirements, or to accommodate modifications in the operating environment. Therefore, after a safety system is commissioned, no changes to the system can be performed without redesigning and re-commissioning the system.

In-service testability will meet the requirements described in FSAR Section 7.1.2.1.6.

In summary, there is no change in the ABWR DCD required safety and functional requirements of the RTIS or NMS resulting from STD DEP T1 3.4-1. The RTIS and NMS digital I&C platform departures associated with STD DEP T1 3.4-1 from the platform discussed in the certified ABWR DCD and evaluated and approved in the NRC Staff's FSER, NUREG-1503, are an improvement in both hardware and application.

Design Acceptance Criteria (DAC) Process

Topical Report UTLR 0001P, Revision 0 mentioned in Attachment 5 to U7-C-STP-NRC-090009 as being submitted for Generic Review, has been withdrawn. It will be replaced by a technical report or reports that discuss the details of the NRW-FPGA-based safety-related I&C system design. Specifically, Toshiba changed the processes described in the Generic Topical Report, and now applies 10 CFR 50 Appendix B processes to part of the Fuchu Complex design, development, and manufacturing facility. That part of the Fuchu Complex is responsible for the design, development, manufacturing, and testing of NRW-FPGA-based systems.

As the final I&C platform design evolves, STPNOC will make technical report(s) covering NRW-FPGA based platforms available for NRC Staff audit through the DAC ITAAC closure process. The technical report(s) will address Tier 1 Table 3.4 Items 7 through 10, 12, and 14 related to software life cycle, electromagnetic compatibility (EMC) qualification, and equipment qualification (EQ).

Note that STPNOC intends to close DAC related items after COL issuance. More information on I&C related DAC items will be provided to the NRC in separate correspondence.

COLA Markup

In this RAI, the staff requested STPNOC "to provide sufficient information within COLA," on the digital I&C platforms. For NRW-FPGA I&C platforms, the following supplemental COLA section will be included in Part 2, Tier 2, for COLA Revision 3.

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), including the Local Power Range Monitoring (LPRM) system, the Average Power Range Monitoring (APRM) system, the Oscillation Power Range Monitor (OPRM) system, and the Startup Range Neutron Monitoring (SRNM) system are Non-Rewritable (NRW)-Field Programmable Gate Array (FPGA)-based systems.

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 fiber optic 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.

ELCS Platform

This response for ELCS has five major sections. The first section provides a high level overview of the ELCS. The second section provides a description of the equipment that is utilized to implement the ELCS. The third section describes the COLA departures and the relationship of the COLA departures to the equipment description. The fourth section provides clarification of the Design Acceptance Criteria audit process. The fifth section provides a COLA markup to include additional information on the ELCS platform.

ELCS Overview

The ELCS provides the instrument and control functions of automatic actuation and control, manual control and display for the ESF Systems.

As shown in Tier 1 Figure 3.4b, the major elements of ELCS include sensor inputs, Digital Trip Function (DTFs), Safety Logic Function (SLFs) and Component Interface Module (CIMs) defined and described as follows:

1. Sensors provide signal input to the (DTF) I/O.

2. The DTF I/O provides signal data acquisition and signal output capability for each division's DTF. DTF I/O is provided in both remote locations and local to the DTF rack for hardwired signals. The remote DTF I/O communicates its information to the DTF utilizing high speed serial (HSL) communication with redundant fiber optic modems and associated redundant fiber optic data cable.

3. 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 SLFs in each division by means of fiber optic based HSL communication links. An individual DTF to SLF communication link consists of a single pair of fiber optic modems with a single fiber optic cable since the DTF and SLF are both located in the Main Control Room (MCR) area.

4. 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 command and control of ESF components from I/O that is local to the SLF rack 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 modems and associated fiber optic cables are redundant for the communication of ESF safety function actuation commands from the SLF to the SLF remote I/O.

5. The SLF remote I/O station provides signal data acquisition and signal output capability for each division's SLF. At the remote station a 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 SLF to the electromechanical ESF component. The CIM provides priority logic to override control when an ESF actuation occurs. Priority logic in the CIM also provides voting of redundant actuation 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 logic based on the feedback signals depending on the type of component.

In addition to the Class 1E actuation functions, ELCS provides the following safety-related support functions:

- Operator HMI, which is utilized for display and manual component control. Each division contains a dedicated Operator HMI on the Main Control Panel and on the Large Display Panel.

- The maintenance and test panel (MTP), which provides the technician interface for periodic testing, surveillance, and maintenance. Each division of ELCS has a dedicated MTP. The MTP also provides a unidirectional, fiber optically isolated, output link to the non-safety systems.

ELCS Platform Description

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

1. Controller, including high speed serial link communications

2. Input / Output

3. Intra-division Network communications

4. Flat Panel Display

5. Maintenance and Test Panel

6. Power Supplies

7. Component Interface Module

General

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

Controller

The controller contains two sections, a processor section and a communication section. The processor section contains a microprocessor and memory for the application program. The memory utilizes Flash Programmable Read Only Memory (PROM) for system software, Flash PROM for application software, and Random Access Memory (RAM).

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

The two controller sections communicate through dual ported shared memory. The shared memory provides for communications isolation between the processor section and communications section of the controller.

The backplane allows multiple controllers to be utilized in a single chassis. The controllers communicate to each other through shared memory that is located on the communication interface module located in the chassis. The communication interface module is also used for Intra-division communications.

The controller performs self-diagnostics, including an internal watchdog timer, and is capable of determining that the required module types are located in the appropriate slot.

Intra-Division Communication

The communication module provides the interface for the intra-division communication network. The intra-division network is a deterministic network that utilizes a bus master. Each controller will send and receive periodic messages from the intra-division network communication module. The MTP utilizes the intra-division network for diagnostic monitoring, periodic test and maintenance functions. The intra-division communication module performs communication diagnostics.

Input / Output (I/O)

The controller uses compatible I/O modules that are located in the chassis with the controller. Additional chassis of I/O modules can be added to the first controller chassis if additional I/O is

necessary. A range of modules is available including 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. Input/Output module diagnostic failures are reported to the controller.

Flat Panel Display

The flat panel display subsystem consists of a flat panel display with touch screen capability, a single board computer, and standard communication interfaces for communication on the intra-division network and fiber optically isolated outputs to external systems.

The Flat Panel Display subsystem communicates with the controller utilizing the intra-division network as previously described. The Flat Panel Display subsystem is also used as an isolated, unidirectional communication interface with non-safety systems. Fiber optic cabling provides the electrical isolation.

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 a controller chassis for monitoring diagnostics and providing a periodic test interface for other controllers. This controller is called the Interface and Test Processor (ITP)

Power Supply

The power supply subsystem provides low voltage direct current (DC) power for the ELCS equipment. The power supply subsystem contains redundant power supplies for each DC low voltage level that is required. One of the redundant power supplies is connected to vital 120 volt alternating current and the other supply is connected to the 125 VDC battery supply.

Component Interface Module (CIM)

In general, the CIM provides the interface between the ELCS actuation and the control command signals and the electromechanical device associated with the final ESF components.

Electromechanical components with non-standard signal interface requirements will not use a CIM, but will be interfaced with discrete I/O. Examples of components with non-standard interfaces include the following:

- Components that are controlled from the Remote Shutdown Panel (RSP), since these components require disconnection from ELCS and subsequent hardwired control from the RSP when the MCR is evacuated.

- Components controlled by analog output signals

- Control outputs for High Pressure Core Flooder (HPCF) (C), since there is a requirement for ELCS to interface with diverse control signals for HPCF (C).

COLA Departure

The STP 3 & 4 COLA includes the following changes:

1. Elimination of obsolete data communication technology

2. Elimination of unnecessary inadvertent actuation prevention logic and equipment

3. Clarification of digital controls nomenclature and systems

4. Final selection of platforms changed the implementation architecture

5. Testing and surveillance changes for SSLC

Changes (1) and (5) are related to the ELCS platform question.

Elimination of Obsolete Data Communication Technology – Change (1)

High Speed Serial Link Communication

The STP 3 & 4 COLA replaces the previous communication technology with HSLs to communicate Class 1E information. The section <u>FPGA-based System Description</u> of this response describes the controller and the associated HSL capability. The HSL is a true broadcast link that meets the communication isolation requirements of IEEE-Std-7.4.3-2.

The HSL communication is utilized for the following communication paths for STP Units 3&4:

- DTF remote I/O to DTF (redundant)

- DTF to SLF (non-redundant)

- SLF safety function actuation to SLF remote I/O (redundant)

Intra-division Communication

The Operator HMI and the Technician HMI utilize the Flat Panel Display subsystem described in the section <u>FPGA-based System Description</u>. The Operator HMI and technician HMI are connected to the controllers within a single division by means of an Intra-Division network.

For STP 3 & 4, the division also utilizes an electrically isolated, unidirectional gateway to provide communication to the non-safety PICS. This communication originates in the MTP described in the section <u>FPGA-based System Description</u>.

The intra-division network is deterministic. A failure of the intra-division network would not affect the actuation of the Class 1E ESF safety functions, since these safety functions utilize the HSL communication method.

Testing and Surveillance Changes for SSLC – Change (5)

The equipment described in the section <u>FPGA-based System Description</u> includes self-diagnostics. Both the HSL and Intra-division network utilize diagnostics to detect hardware failures and problems with communication messages. These diagnostics typically indicate fault detection when the equipment communicates with the controller, such as when the controller communicates with an I/O module over the backplane to perform I/O.

In addition to comprehensive, on-line self diagnostic capability, the ELCS provides a MTP for each division for maintenance and testing when an appropriate bypass function is in effect.

The MTP contains a flat panel display subsystem for the technician HMI interface and an Interface and Test Processor (ITP) for the test interface with the division's controllers.

The ITP is a controller chassis in a division that is independent from the controllers that perform Class 1E ESF safety function actuation. The ITP is a testing system which performs continuous

passive monitoring of expected outputs based on current inputs, and manually initiated active testing. The ITP man-machine interface is the MTP. The combination of the ITP and MTP enhances maintenance and surveillance testing.

In summary, there is no change to the ABWR DCD required safety and functional requirements of the ELCS resulting from STD DEP T1 3.4-1. There are only improvements in equipment and application. The ELCS digital I&C platform is consistent with the intent of the certified ABWR DCD and its evaluation and approval in the NRC Staff's FSER, NUREG-1503.

Design Acceptance Criteria (DAC) Process

As the final ELCS I&C platform evolves, STPNOC will make the following available for NRC Staff audit through the DAC-ITAAC closure process.

- Any change in the platform information for the ELCS that clarifies the scope of I&C departures with respect to the Westinghouse Common-Q topical report (WCAP-16097-P-A). This includes:

  - Definition of the equipment, software, and processes that are described in the topical report that will be utilized for the I&C departures.

  - Definition of the equipment that will be utilized in addition to that currently described in the topical report, such as improved input cards and component interface modules.

STPNOC intends to close DAC related items after COL issuance. More information on I&C related DAC items will be provided to the NRC in separate correspondence.

COLA Markup

In this RAI, the staff requested STPNOC "to provide sufficient information within COLA," on the digital I&C platforms. For the ELCS platform, the following supplemental COLA section will be included in Part 2, Tier 2, for COLA Revision 3.

7.1S.2 Microprocessor Based Platforms

The Engineered Safety Features Logic and Control System (ELCS) provides the instrument and control functions of automatic actuation and control, manual control, and display for the Engineered Safety Features (ESF) systems. The ELCS Controller subsystem is modular. A passive backplane connects individual module slots, which can house the controller module intra-division communication module, and input/output modules. Major elements of the ELCS include the following:

- Controller (including high speed serial link communications

- Input/Output (I/O)

- Intra-division network communications

- Flat panel display

- Maintenance and test panel

- Power supplies

- Component interface and module

Sensors provide signal inputs to the Digital Trip Function (DTF) I/O that provide signal data acquisition and signal output capability for each division's DTF.

The DTF provides a comparison of signal inputs to associated setpoints, which 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 fiber optic based HSL communication links.

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.

In addition to the Class 1E actuation functions, ELCS provides the following safety-related support functions:

- Operator Human-Machine Interface (HMI) for display and manual component control. Each division contains a dedicated Operator HMI on the Main Control Panel and on the Large Display Panel.

- Maintenance and Test Panel (MTP), which provides the technician interface for periodic testing, surveillance, and maintenance. Each division of ELCS has a dedicated MTP. The MTP also provides a unidirectional, fiber optically isolated, output link to the non-safety systems.

The equipment includes self-diagnostics to detect hardware failures and problems with communication messages. These diagnostics typically indicate fault detection when the equipment communicates with the controller, such as when the controller communicates with an I/O module over the backplane to perform I/O.

RAI 07.03-1

QUESTION:

Departure STD DEP T1 3.4-1 proposed to eliminate unnecessary inadvertent actuation
prevention logic and equipment. The NRC Staff requests that STPNOC provide a list of logic
and equipment in the ESF system that are selected to be deleted and sufficient bases for each
case.

RESPONSE:

Bases for Limiting the Application of Dual Redundant SLFs (replaces SLUs): The bases for
elimination of unnecessary, inadvertent actuation prevention logic and equipment are discussed
below. The ABWR DCD descriptions and figures show dual redundant Safety System Logic
Unit (SLU) processors for all ESF functions with a final 2-out-of 2 vote. The architecture was
intended to prevent inadvertent initiation of ESF functions due to single SLU processor failures.
The ABWR DCD design, assumed a small number of large processors implementing the control
logic on one-half or more of the ESF systems in a logic division. The current technology for the
STP Units 3&4 ELCS (ESF) platform (AC160-based Common Q) uses distributed Safety
System Logic Function (SLF) processing both to simplify the hardware and software
implementation and to reduce the extent of the effect of any electronic module failure. This
design represents a reliability and availability improvement through reduction in logic hardware
and components. This change limits implementation of the explicit commitment for dual-
redundant SLFs that are provided for ECCS systems, so that SLF failures cannot result in
inadvertent coolant injection. Dual-redundant SLFs are also applied to limit adverse operational
impact, such as due to inadvertent automatic rapid depressurization.

Departure STD DEP T1 3.4-1 proposes to eliminate unnecessary inadvertent actuation
prevention logic and equipment. The specific logic circuits affected are listed below and are
reflected in Technical Specifications Table 3.3.1.4-1 and its Bases.

TS Table 3.3.1.4-1 Item No.	TS Table 3.3.1.4-1 Function	Bases for Modification of 2-out-of-2 Vote
5c	Diesel Generator System Initiation	There is no significant operational or safety issue resulting from inadvertent diesel start. Power is available from DG, but not used.
5e	Diesel Generator Manual Initiation	There is no significant operational or safety issue resulting from inadvertent diesel start. Power is available from DG, but not used.
7a	Reactor Building Cooling Water/Reactor Service Water System Initiation	There is no significant operational or safety issue resulting from inadvertent Reactor Water systems start. Operation provides heat removal that is not needed.
7c	Reactor Building Cooling Water/Reactor Service Water Manual Initiation	There is no significant operational or safety issue resulting from inadvertent Reactor Water systems start. Operation provides heat removal that is not needed.
8a	Containment Atmospheric Monitoring System Initiation	There is no significant operational or safety issue resulting from inadvertent CAMs initiation. Monitoring of a non-contaminated atmosphere is of no consequence.
9a	Suppression Pool Cooling System Initiation	There is no significant operational or safety issue resulting from inadvertent Suppression Pool Cooling start. Operation provides heat removal from the pool that is not needed.
9c	Suppression Pool Cooling Manual Initiation	There is no significant operational or safety issue resulting from inadvertent Suppression Pool Cooling start. Operation provides heat removal from the pool that is not needed.
11	Containment Isolation Valves Divisional Manual Initiation	There is no significant operational or safety issue resulting from inadvertent initiation of divisional Containment Isolation Valves. At most, isolation will close one of two valves in lines that could be open during normal power operation and would represent an operational nuisance before the valve(s) is/are reopened.
12a	Reactor Core Isolation Cooling System Isolation Initiation	There is no significant operational or safety issue resulting from inadvertent RCIC isolation. Isolation of a non-operating RCIC system will have no consequence.
12c	Reactor Core Isolation Cooling Manual Isolation Initiation	There is no significant operational or safety issue resulting from inadvertent RCIC isolation. Isolation of a non-operating RCIC system will have no consequence.
13a	Reactor Water Cleanup System Isolation Initiation	There is no significant operational or safety issue resulting from inadvertent RWCU isolation. Isolation of the operating RWCU will only stop water filtration until the system is restarted.
14a	Shutdown Cooling System Isolation Initiation	There is no significant operational or safety issue resulting from inadvertent SD Cooling isolation. Isolation of a non-operating Shutdown Cooling system will have no consequence.

Bases Figure B 3.3.1.4-1, ESF Actuation Channel Structure for Containment Isolation ESF Support, provides a functional block diagram for the above ESF support systems.

Modification of 2-out-of-2 Output Vote: The ABWR DCD descriptions and figures show dual-redundant SLU processors for all ESF functions with a final 2-out-of-2 vote between two redundant SLU processors. The vote was intended to prevent inadvertent initiation of ESF functions due to single SLU processor failures.

The prevention of inadvertent actuation continues to be applied to ESF systems to prevent injection of high or low pressure water into the RPV or drywell/containment. Recent plant design for ESF coolant injection systems requires both valve alignment and pump start actions for coolant injection. However, the logic is simplified by using one SLF channel to control valves and the second one to control pumps, effectively accomplishing the same 2-out-of-2 vote while eliminating the redundant voter hardware. This change uses the system hardware in the pump and valves to accomplish the final vote, thus eliminating the use of redundant SLF channels for final 2-out-of-2 vote logic.

There are several components of actuated hardware in which a single logic processor and a single output card are used to generate an action. Without prevention logic, failure of the processor or the single output card would result in an inadvertent actuation for the automatic depressurization valves or isolation of reactor cooling or service water. For these cases, 2-out-of-2 vote logic is retained, with the recommendation that the logic also be duplicated in separate logic processors.

Summary

The described design change still meets applicable regulatory requirements and IEEE standards, as discussed in STPNOC letter U7-C-STP-NRC-090009 to the NRC. The change only removes equipment as described above and shown in revised COLA Rev. 2, Part 2, Tier 1, Section 3.4, Figure 3.4b, Safety System Logic & Control Block Diagram. The SLF for ECCS functions retains the redundant processing channel design.

No COLA revisions are required as a result of this RAI response.