Nuclear Operating Company
South Texas Project Electric Generating Station P.O. Box 289 Wadsworth, Texas 77483

December 30, 2009
U7-C-STP-NRC-090232

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
Revised Response to Request for Additional Information

Reference: Letter, Mark McBurnett to Document Control Desk, Response to Request for Additional Information, dated September 24, 2009, U7-C-STP-NRC-090162 (ML092710226)

Attached is a revised response to an NRC staff question included in Request for Additional Information (RAI) letter number 252 related to Combined License Application (COLA) Part 2, Tier 2, Chapter 7, Instrumentation and Controls.

The attachment to this letter revises the response to RAI 07-6 and replaces the one provided in Attachment 2 to the referenced letter in its entirety.

The COLA changes provided in this response will be incorporated in 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 32593779 D091
NRO

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

Executed on 12/30/09

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

jwc

Attachment:

Response 07-6 Revision 1

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
P. O. Box 149347
Austin, Texas 78714-9347

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

(electronic copy)

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

Steve Winn
Joseph Kiwak
Eli Smith
Nuclear Innovation North America

Jon C. Wood, Esquire
Cox Smith Matthews

J. J. Nesrsta
Kevin Pollo
L. D. Blaylock
CPS Energy

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.

REVISED RESPONSE:

The following information revises the original response submitted as Attachment 2 to the letter from Mark A. McBurnett to Document Control Desk, "Response to Request for Additional Information," dated September 24, 2009, U7-C-STP-NRC-090162 (ML092710226). Revisions to the original response are indicated by revision bars in the margin. This revision comprises a complete response to RAI question 07-6.

The significant revision is the deletion of the paragraphs related to the Electrical Power Distribution System (EPDS) at the end of COLA Part 2, Tier 2, Subsection 7.1S.2.1 as shown in the original response.

STPNOC does not intend to control the Electrical Power Distribution System (EPDS) feeder breakers through ELCS as originally described in the response to RAI 07-6. There was not sufficient detail in the COLA to identify the type of EPDS breaker control prior to adding the supplemental information of COLA Part 2, Tier 2, Subsection 7.1S.2 regarding the EPDS. Although manual soft control for the EPDS feeder breakers does not affect any analysis that is credited to support a licensing requirement or commitment, the manual control for these breakers will be hardwired. COLA Part 2, Tier 2, Figure 7.9S-1 was reviewed based on this change and it was determined that no changes are required. Removal of the EPDS discussion reverts the EPDS to the ABWR DCD.

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 and 7.1S.2, FPGA Based Platforms and Microprocessor Based Platforms, which 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 Safety Logic Functions (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 into 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 the I/O that is local to the SLF and from the 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 display is driven by a flat panel display subsystem.

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 maintenance technician functions.

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 chassis. 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 provides 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.