Nuclear Operating Company

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

September 22, 2009
U7-C-STP-NRC-090157

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

Attached are the responses to the NRC staff questions included in Request for Additional Information (RAI) letter numbers 250, 251, and 253 related to Combined License Application (COLA) Part 2, Tier 2, Chapter 7, Instrumentation and Controls. This submittal completes the responses to these RAI letters. Also included are responses to questions in RAI letter numbers 252 and 255.

Attached are responses to the RAI questions listed below:

RAI 07.03-2	RAI 07-1
RAI 07.03-3	RAI 07-2
RAI 07.03-4	RAI 07-3
RAI 07.09-1	RAI 07-4
RAI 07.09-2	RAI 07-7
RAI 07.09-3	RAI 07-8
RAI 07.09-4	RAI 07-9
RAI 07.09-5	RAI 07-10
RAI 07.09-6	RAI 07-11
RAI 07.09-7	RAI 07.07-7
	RAI 07.07-8
	RAI 07.07-9

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

STI 32539432

D091
NRO

There are no commitments in this letter.

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

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

Executed on 9/22/09

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

jwc

Attachments:

1. RAI 07.03-2
2. RAI 07.03-3
3. RAI 07.03-4
4. RAI 07.09-1
5. RAI 07.09-2
6. RAI 07.09-3
7. RAI 07.09-4
8. RAI 07.09-5
9. RAI 07.09-6
10. RAI 07.09-7
11. RAI 07-1
12. RAI 07-2
13. RAI 07-3
14. RAI 07-4
15. RAI 07-7
16. RAI 07-8
17. RAI 07-9
18. RAI 07-10
19. RAI 07-11
20. RAI 07.07-7
21. RAI 07.07-8
22. RAI 07.07-9

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
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852

(electronic copy)

*George F. Wunder
*Adrian Muniz
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 07.03-2

QUESTION:

Departure STD DEP T1 3.4-1 took a deviation from the certified ABWR DCD on the data communication and control system. For the safety related residual heat removal (RHR) system, COLA FSAR Tier 2 Section 7.3.1.1.1.4(3)(i) states that "this action must occur within a limited interval." Provide specific time requirement for this action and also include what would happen and any mitigations are provided if the operator does not act within the limited time interval.

RESPONSE:

STD DEP 7.3-10 "ESF Logic and Control System (ELCS) Mode Automation" is the basis for the changes to COLA Part 2, Tier 2, Subsection 7.3.1.1.1.4(3)(i) and there is no time requirement on the RHR mode initiation switch between actuation of the "Armed" position, to pressing of the "Initiate" push button. These actions are part of operator training, in response to plant conditions and plant operating procedures.

COLA Part 2, Tier 2, Subsection 7.3.1.1.1.4(3)(i), Operational Considerations, will be revised as shown below.

> The pumps, valves, piping, etc., used for the LPFL are used for other operating modes of the RHR System. Initiation of the LPFL mode is automatic and no operator action is required for at least 30 minutes. ~~The operator may control the RHR pumps and injection valves manually after LPFL initiation to use RHR capabilities in other modes if the core is being cooled by other emergency core cooling systems.~~ Other RHR modes ~~are~~ may be activated by Mode switches in the MCR. For example to enter the Containment Spray mode, this switch is first "Armed" and then the "Initiate" Push button is pressed. ~~This action must occur within a limited interval~~. This assures that this is an intentional action by the operator. Also to transfer to these and other RHR Modes, mode specific permissives must be met. This reduces or eliminates the possibility of operator error.

RAI 07.03-3

QUESTION:

Departure STD DEP T1 2.4-2 proposed changes to the feedwater line break mitigation which include the monitoring of the feedwater line differential pressure. The COLA FSAR Tier 2 Section 7.3.1.1.2(3)(w) added the monitoring of the feedwater line differential pressure. Provide sufficient information on how and where the feedwater line differential pressure is measured. In addition, provide sufficient information on how the detection of the feedwater line differential pressure is to be used in the feedwater pump control logics.

RESPONSE:

The differential pressure between the two feedwater (FW) lines is measured by four safety-related differential pressure transmitters connected to the FW lines inside the drywell. The FW pumps discharge feedwater into a common header in the turbine building. This common header branches into the two feedwater lines, which then inject the water into the feedwater spargers, internal to the reactor pressure vessel (RPV).

During normal plant operation, the differential pressure between the two feedwater lines is expected to be small. During a postulated break of one feedwater line inside the drywell, the differential pressure is expected to be large, because the broken line would be discharging into the low pressure drywell, and the intact line would be discharging into the high pressure RPV. Each feedwater line differential pressure signal is compared to a set value, and its trip signal goes to a two-out-of-four voter logic. The output of this logic goes to an AND gate, into which the other input is the output of a two-out-of-four voter logic of high drywell pressure trip signals that indicates a LOCA has occurred. This trip function is performed by the Leak Detection and Isolation System. The postulated condition of a feedwater line break and a high drywell pressure will cause the operating condensate pumps to trip, which terminates feedwater flow into the drywell. The feedwater line differential pressure instrumentation and drywell pressure instrumentation are classified as safety-related for the mitigation of a postulated feedwater line break inside the drywell. The design requirements for the equipment performing the condensate pump trip are in STP 3&4 COLA Part 2, Tier 2, Subsection 8.3.1.1.1 "Medium Voltage Class 1E Power Distribution System," and the breakers are shown in COLA Part 2, Tier 2, Figure 8.3-1 "Electrical Power Distribution System Single Line Diagram," sheet 1.

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

RAI 07.03-4

QUESTION:

COLA FSAR Sections 7.3.2.3.2, 7.3.2.4.2, and 7.4.2.3.2 state that the parent RHR system annunciates activity at the loop level and the individual mode of the RHR system is not separately annunciated. STD DEP 1.8-1 updated the IEEE 603 "Standard Criteria for Safety Systems for Nuclear Generating Stations" to the 1991 version, as required in 10 CFR 50.55a(h). According to Section 5.8 of IEEE 603-1991 system status indication shall be provided. Since there are a few operation modes (low pressure flooder, wetwell and drywell spray cooling, and suppression pool cooling) for the RHR system, the display of the operation mode for the RHR system should be provided to minimize the possibility of ambiguous indications that could be confusing to the operator. Provide adequate justification for this design.

RESPONSE:

According to the reference ABWR DCD Tier 2 Subsection 5.4.7.1.1, the RHR system has four principal functions, thus four modes of operation:

- Low Pressure Flooder (LPFL)
- Suppression Pool Cooling (SPC)
- Wetwell and Drywell Spray Cooling (WDSC)
- Shutdown Cooling

Each loop of RHR (A, B, or C) can perform multiple modes of operation; however, only one loop can perform one functional operation at a time. Therefore, different operations can be performed at the same time by different loops, if necessary. In the reference ABWR DCD, Subsections 7.3.2.3.2, 7.3.2.4.2, and 7.4.2.3.2 state "The parent RHR System annunciates activity at the loop level (i.e., "RHR LOOP A, B, C ACTIVATED"). However, the individual mode at the RHR system level is not separately annunciated." This statement has been incorporated by reference into the STP 3&4 COLA. Because "status indication" is the intent of the requirement in Section 5.8 of IEEE 603-1991, just as it was with Section 4.19 of IEEE 279-1971, the loop level of notification to the operator satisfies the industry standards.

Along with the use of modern video display units (VDUs) in the main control room console, the human system interface design criteria will be employed to present the optimal mode status information/indication to the control room operator.

There are no COLA changes required as a result of this RAI.

RAI 07.09-1

QUESTION:

COLA FSAR Tier 2 Section 7.9S.2.2 and Figure 7.9S-1 took Departure STD DEP T1 3.4-1 on the data communication systems from the generic ABWR DCD. Departure DEP T1 3.4-1 also took departures from the generic ABWR DCD on the platforms for engineered safety features (ESF) logic & control system (ELCS), neutron monitoring system (NMS), reactor trip & isolation system (RTIS), and plant information & control system (PICS) systems. For the safety related ELCS, NMS, and RTIS systems, provide sufficient information on how the communication interface is addressed between safety related and non-safety systems, and also among different platforms (TOSDIA-FPGA, TOSMAP (C2000 and HCNT), Common-Q, Ovation, multiplexing system for RCIS, and platform for radiation monitoring system),

RESPONSE:

The STP 3&4 Data Communications System is described in FSAR Tier 2 Section 7.9S. Figure 7.9S-1 provides an overview of the communication interfaces between different systems. Communication interfaces are described in Subsections 7.9S2.3 and 7.9S2.4. Additional information on the communication interfaces between systems is provided with this RAI response.

Engineered Safety Features (ESF) Logic and Control System (ELCS)

A high level block diagram of one division of the ELCS data communication interfaces is shown in Figure 7.9S-1. Each of the four redundant divisions has a Digital Trip Function (DTF). Because there are no ESF components assigned to division IV, this division does not include Safety System Logic Functions (SLFs) and their associated Remote Digital Logic Controllers (RDLCs).

As shown in the figure, each division's DTF receives input signals directly and also receives remote input signals from an RDLC. The RDLC communicates the remote input signals to the DTF utilizing high speed serial link (HSL) communication, using redundant fiber optic modems and associated redundant fiber optic cable.

The ELCS utilizes 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 fiber optic communication media. The identical unidirectional signals are then connected to multiple receivers, with one receiver in each division. Use of multi-drop helps reduce the possibility of Byzantine faults. An example of multi-drop communication is the transmission of a single division's DTF output actuation status signals to the three divisions of SLFs.

The DTF provides a comparison of signal inputs to associated setpoints to determine the trip status for each ELCS safety function. Each division's DTF communicates the DTF's safety function actuation status to each SLF utilizing a unidirectional HSL.

SLFs are provided in each of the three ELCS divisions that provide electromechanical component actuation. Each division's SLFs receive ELCS safety function actuation status signals from each of the DTFs in the four redundant divisions. The division's SLFs determine ELCS system level actuation status by implementing the two-out of-four coincidence voting logic of DTF ELCS safety function trip signals. The SLF also receives hardwired signals for command and control of ELCS components from I/O that is local to the SLF and from SLF I/O that is located remote from the main control room.

The SLF communicates ELCS actuation commands to the RDLCs by redundant HSL links. The RDLCs provide input and output capability, including actuation of ESF components. The RDLCs provide communication of input signals by separate redundant HSL links

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 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.

Each ELCS division also includes an intra-division network. The ELCS utilizes an intra-division network to communicate between multiple ELCS controllers 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 performs communication diagnostics.

The 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 inter-division network communication modules. This network provides communication between the safety control room displays, the Maintenance and Test Panel (MTP), and ELCS controllers. This bus is used to communicate status and diagnostic data from the ELCS controllers for display on the main control room safety displays and MTP. It is also used to communicate test signals and data from the MTP and safety control room display control data to the ELCS controllers.

For each of the four ELCS divisions, the ELCS communication interface to the non-safety related systems is contained in the Maintenance and Test Panel (MTP). There is one MTP for each ELCS safety division. The MTP contains a single board computer with an interface to the intra-division network in the ELCS division. The information to be transmitted to the non-safety Plant Information and Control System (PICS) is received by the intra-division communication interface and stored by the MTP for periodic transmission. On a predetermined interval, the MTP will transmit information to the PICS by means of a separate Ethernet interface and fiber optic cable. The MTP is designed such that information can be transmitted in one direction only on the fiber optic cable. The fiber optic cable provides electrical isolation.

The process radiation monitoring system provides analog and discrete input signals to the ELCS for display in the main control room and communication to PICS.

As shown in Figure 7.9S-1, the Reactor Trip & Isolation System (RTIS) and Neutron Monitoring System (NMS) communicate data and status to ELCS for display in the main control room.

The ELCS video display stations in the main control room are used to display ELCS information and a selected set of data from the RTIS and NMS. The RTIS and NMS provide one way fiber optic links to ELCS. ELCS has a communication interface that receives the RTIS and NMS information and provides data to the ELCS safety display controllers for display.

Reactor Trip and Isolation System

RTIS consists of Suppression Pool Temperature Monitor (SPTM), primary functions of Reactor Protection System (RPS), and Main Steam Isolation Valve (MSIV) subsystem. Each system or subsystem consists of four redundant divisions. A high level block diagram of one division of the RTIS data communication interfaces is shown in FSAR Figure 7.9S-1. A markup of Figure 7.9S-1 is provided as a result of this RAI response and will be included in a future COLA revision.

SPTM sensor signals are hardwired to the SPTM Input/Output (I/O). SPTM communicates trip status information to RPS DTFs by fiber optic communication links.

The RPS and MSIV have four divisions of DTFs. Sensor signals are hardwired to the DTF I/O for each division. Each division's DTF determines the trip status for each signal. The DTF communicates its division's trip status information to the Trip Logic Function (TLF) by fiber optic communication links. Because individual divisional trip determinations must be shared between divisions, to support two-out-of-four voting logic for divisional trip outputs, the DTF also communicates its trip status information to the other three divisional TLFs by means of isolated communication links. The links provide a qualified and isolated, point-to-point, single direction communication path between divisions to preserve divisional independence.

The TLF in each division determines the system level actuation of RPS and MSIV safety functions utilizing two-out-four voting logic. In each division, the TLF communicates trip status information to the Output Logic Unit (OLU) by fiber optic communication links. The OLU in each division communicates via the Load Driver that initiates the safety function. The RPS Load Drivers are hardwired to its scram solenoid valve, and the MSIV Load Driver is hardwired to its MSIV solenoid valve.

Each RTIS division provides fiber optic communication links to an ELCS communication interface, ELCS provides the information for display on the safety displays in the main control room.

Each of the four RTIS divisions communicates data and status to the non-safety related Plant Information and Control System (PICS) through separate communication interfaces in the DTF, TLF, and SPTM modules. The communication interface for each division consists of a one way fiber optic communication link that provides fixed data sets from each safety division to the non-safety related PICS. The communication interface is designed to prevent any data transfer from the non-safety PICS to the RTIS. The fiber optic cable provides electrical isolation and the Transmit module provides the functional isolation.

Neutron Monitoring System

NMS consists of Local Power Range Monitor (LPRM), Average Power Range Monitor (APRM) with Oscillation Power Range Monitor (OPRM), and the Startup Range Neutron Monitor (SRNM) systems. Each system consists of four redundant divisions. A high level block diagram of one division of the NMS data communication interfaces is shown in FSAR Figure 7.9S-1. A markup of Figure 7.9S-1 is provided as a result of this RAI response and will be included in a future COLA revision.

The LPRM monitors local neutron flux in the power. For each of the four NMS divisions, an LPRM module measures the flux levels from one of the hardwired LPRM detector inputs. The LPRM module communicates to the APRM with one way fiber optic communication links that provide fixed data sets of LPRM information.

For each of the four NMS divisions, the APRM computes a core average neutron flux from the divisional LPRM detectors and a core flow input (from the differential pressure across the core support plate). When the APRM detects the trip condition it provides a hardwired signal to the RTIS as a sensor input. Each divisional APRM communicates the LPRM information to the divisional OPRM function over a one way fiber optic communication link that provides fixed data sets of LPRM information.

For each of the four NMS divisions, the divisional OPRM receives the data from the divisional LPRMs, and receives the core flow level and the core average neutron flux from the divisional APRMs. The OPRM trip protection algorithm detects thermal hydraulic instability and provides hardwired signals to the RTIS's voter logic for reactor trip determination.

The divisional SRNM monitors neutron flux while in the start-up range. The SRNM receives inputs from hard wired detectors distributed throughout the reactor core. The SRNM detects the high flux trip condition and provides hardwired signals to the RTIS's voter logic for reactor trip determination.

In each NMS division, the APRM, OPRM, and SRNMs provide isolated data links to an ELCS communications interface, ELCS provides the information on a one way fiber optic communication link to the safety displays in the main control room.

For each of the four NMS divisions, the NMS communicates to the non-safety related PICS through separate communication interfaces in the LPRM, APRM, and SRNM units. The communication interfaces consist of one way fiber optic communication links that provides fixed data sets from a safety division to the non-safety PICS. The communication interface is designed to prevent any data transmission from the non-safety PICS to the NMS. The fiber optic cable provides electrical isolation. The Transmit module provides functional isolation.

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 non-safety related core monitor function of the PICS, the NMS division desired to receive the information must be bypassed by the control room operator, placed in an inoperative status, and a key lock switch on that NMS division must be enabled to request and allow the data transfer. Only a limited data set in a predefined format will be accepted by the

NMS. Before the data can be used by the NMS, manual verification and acceptance at the NMS human-system interface is required.

The Multi-channel Rod Withdrawal Block Monitor (MRBM) is a non-safety portion of the NMS. The APRM in each NMS division communicates to two MRBMs with one way fiber optic communication links that provide fixed data sets from the safety division to the non-safety side. MRBM communicates by a one way fiber optic communication link that provides fixed data sets from the non-safety MRBM to the non-safety PICS.

Non-Safety Related Systems

Feedwater Control (FWC), Recirculation Flow Control (RFC), Automatic Power Regulator (APR), Rod Control and Information System (RCIS), Automatic Thermal Limit Monitoring (ATLM), Rod Worth Minimizer (RWM) and the turbine Electrohydaulic Control (EHC) are non-safety related systems that use similar microprocessor based platforms. These systems have dedicated networks which provide two-way Ethernet-type communication links with PICS.

Other Packaged System

Various systems will be purchased from other vendors. Communications with those systems will use the same isolation and cyber security methods as used for the systems listed above.

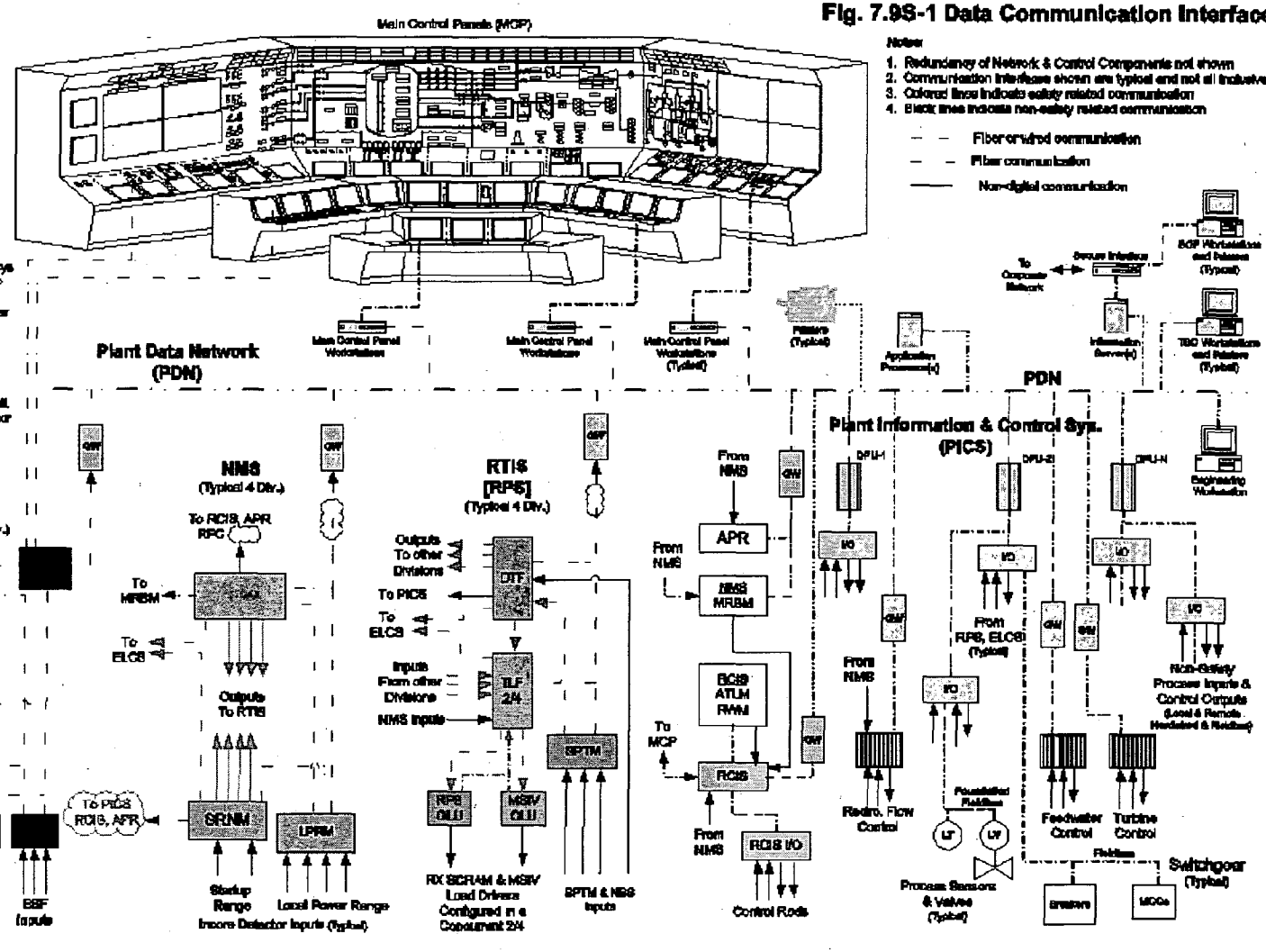
The STP 3&4 COLA, Subsection 7.9S.2.2 and Figure 7.9S-1, Data Communication Interfaces, will be revised as shown below in a future revision.

Fig. 7.9S-1 Data Communication Interfaces

Legend:
APR – Auto Power Regulator
APRM – Average Power Range Monitor
ATLM – Auto. Thermal Limit Monitor
CI – Communications Interface
DPU – Digital Processing Unit
DTF – Digital Trip Function
ELCS – ESF Logic & Control System
EOF – Emergency Operations Facility
ESF – Engineered Safety Functions
GW – Gateway
I/O – Plant Input & Output Units
LT – Level Transmitter
LV – Level Control Valve
MCC – Motor Control Centers
MCP – Main Control Panel
MRBM – Multichannel Rod Block
MTP – Maintenance & Test Panel
NMS – Neutron Monitoring System
NBS – Nuclear Boiler System
OLU – Output Logic Unit
PDN – Plant Data Network
PICS – Plant Information & Control Sys
RCIS – Rod Control & Info. Sys.
RDLC – Remote Digital Logic Controller
RFC – Recirculation Flow Control
RPS – Reactor Protection System
RTIS – Reactor Trip & Isolation Sys.
RWM – Rod Worth Minimizer
SLF – Safety Logic Functions
SPTM – Suppression Pool Temp. Monit.
SRNM – Startup Range Neutron Monitor
TLF – Trip Logic Function
TSC – Technical Support Center

Notes:
1. Redundancy of Network & Control Components not shown
2. Communication Interfaces shown are typical and not all inclusive
3. Colored lines indicate safety related communication
4. Black lines indicate non-safety related communication

Fiber or wired communication
Fiber communication
Non-digital communication



RAI 07.09-2

QUESTION:

Departure STD DEP T1 3.4-1 describes the deviation of safety-related instrumentation and controls (I&C) architecture from the certified ABWR DCD. Provide sufficient information in COLA FSAR Tier 2 Section 7.9S on how the isolation is implemented for both the communication interface (CI) modules and gateways. In addition, a safety related CI module is used on Figure 7.9S-1 for NMS and RTIS systems to communicate to the corresponding gateways, but there is no CI for ELCS system. Provide sufficient information on how the communication interface function is addressed for the safety related ELCS system.

RESPONSE:

The communication interfaces and implementation of isolation for the Reactor Trip and Isolation System (RTIS), the Neutron Monitoring System (NMS), and the Engineered Safety Features Logic and Control System (ELCS) are discussed in FSAR Subsections 7.9S.2.3, 7.9S.2.4, 7.9S.2.5.3, 7.9S.2.5.7, and 7.9S.2.5.11. These topics are discussed in more detail in the RAI 07.09-1 response, which also addresses with more information the safety related communication interface function for ELCS.

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

RAI 07.09-3

QUESTION:

STP COLA took Departure STD DEP T1 3.4-1 on the data communication system from the generic ABWR DCD. This proposed data communication system will be fiber optic based. Both the fiber optic cable and its components such as terminations, field splices, and connectors are critical to provide communication, electrical and communication isolation for the safety related systems. Provide sufficient equipment qualification information in the COL application for the fiber optic cable components.

RESPONSE:

The qualification of all safety-related instrumentation and control (I&C) equipment is within the scope of the STP 3&4 Inspections, Tests, Analyses and Acceptance Criteria (ITAAC). Specifically, ABWR DCD, Tier 1, Table 3.4 Item 14, ITAAC Design Commitment states, "Qualification of safety-related I&C equipment is implemented by a program that assures this equipment is able to complete its safety-related function under the environmental conditions that exist up to and including the time the equipment has finished performing that function." A review that the safety-related I&C equipment has been environmentally qualified is part of the ITAAC acceptance criteria. Tier 1, Table 3.4, Item 12 includes the ITAAC for electromagnetic compatibility qualification. No departures related to these ITAACs have been taken in the STP 3&4 COLA.

The hardware qualification process will demonstrate that the system meets the STPNOC requirements for Electromagnetic Compatibility (EMC) and Equipment Qualification (EQ). These requirements will be made available for NRC Staff review through the DAC process of COLA Part 2, Tier 1, Section 3.4, Table 3.4 Items 12 and 14. STPNOC Letter U7-C-STP-NRC-090059 provides a schedule for when these documents will be available for NRC Staff review.

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

RAI 07.09-4

QUESTION:

In Departure STD DEP T1 3.4-1, STPNOC took a deviation on data communication systems from the certified ABWR DCD. COLA FSAR Section 7.9S.3.1 states that network gateways are safety related, but Figure 7.9S-1 shows that the gateways are not safety related. Clarify this inconsistency.

RESPONSE:

The safety-related aspects of communication from a safety system to a non-safety system are communications isolation and electrical isolation. These two elements are implemented in the safety system. In COLA Part 2, Tier 2, Figure 7.9S-1, they are shown correctly as being accomplished in the communications interfaces for Reactor Trip and Isolation System (RTIS) and Neutron Monitoring System (NMS), and in the Maintenance and Test Panel (MTP) for the Engineered Safety Features Logic and Control System (ELCS).

The gateways described in COLA Part 2, Tier 2, Subsection 7.9S.3.1 are non-safety related.

STP 3&4 COLA Rev. 2, Part 2, Tier 2, Subsection 7.9S.3.1 will be revised as follows for clarification in a future revision.

7.9S.3.1 Plant Data Network (PDN) Functions

The PDN provides a plant wide, highly reliable, high speed data communication network for plant control, monitoring, and other related operational needs.

The PDN is nonsafety-related and supports the collection and distribution of data for multiple systems using a layered network design. A control layer is designated for systems and information that directly impact plant operation. The PDN has other communication layers that support other selected nonsafety-related functions.

The control network supports data communication between:

- Process I/O units, controllers, engineering workstations
- Network monitoring, historical data storage units, control building workstations
- Main control room panel displays and workstations that support the operator interfaces
- Printers
- ~~Safety-related network~~ Network gateways that support the one-way acquisition of data from the safety systems for plant data historian recording and for use on nonsafety displays.

RAI 07.09-5

QUESTION:

STP COLA took Departure STD DEP T1 3.4-1 from the generic ABWR DCD to use new data communication systems. The new data communication system proposed in the COLA is different from the system used in the ABWR DCD. Provide sufficient information to address system design analysis and the criteria in SRP Section 7.9 and BTP 7-21.

RESPONSE:

As stated in STPNOC letter U7-C-STP-NRC-090009, dated February 9, 2009, Enclosure 4d, the departures for RTIS/NMS and ELCS do not impact compliance to BTP 7-21. Also as discussed in STPNOC's response to RAI 14.03.05-4, 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 analysis will be utilized to determine the acceptance criteria for the validation tests that will demonstrate that the systems are deterministic.

STP 3&4 COLA Part 2, Tier 2, Subsection 7.9S.2.5, Design Basis Information, contains information related to IEEE Standards, Branch Technical Positions, and Regulatory Guides as discussed in SRP 7.9, Data Communication Systems. The major design considerations listed in SRP 7.9 are discussed in COLA Part 2, Tier 2, Subsection 7.9S.2.5 or other referenced subsections.

For the certified ABWR DCD, data communication was reviewed and in the Final Safety Evaluation Report (FSER) NUREG-1503 Volume 1, Section 7.9, regarding the level of design detail and the commitment to meet the listed industry standards, the Staff in their final evaluation concluded that "Verification that the I&C system design conforms with this commitment will be accomplished during the ITAAC phase." In their letter U7-C-STP-NRC-090009, dated February 9, 2009, Enclosures 2a, 2b, & 2c, STPNOC has committed to more current versions of standards than those listed in the reference ABWR DCD.

The final basis for the above conclusion was the staff's accepting the level of detail provided in Appendix 7A, as augmented by Appendices 7B and 7C, which further address digital I&C system design issues, including defense-in-depth. STPNOC also has updated the Appendix 7A responses with respect to the instrumentation platforms which implement the reference ABWR DCD safety and functional design requirements.

In conclusion, the Staff stated "Based on the review of the information provided in the SSAR (Appendices 7A, 7B, and 7C) and in related CDM, the staff considers that issues regarding standards and criteria for digital equipment, raised by the LRB Appendix B questions, have been adequately addressed."

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

RAI 07.09-6

QUESTION:

Departure T1 3.4-1 in STP COLA made the final selection of platforms to use configurable logic devices for neutron monitoring system (NMS) and reactor trip and isolation system (RTIS). Since the topical report for the new platform will not be included as part of the COL application, provide sufficient information in the COL application on how the following technical items are addressed in the new platform-based NMS and RTIS system design to meet the safety and reliability requirements: timing, delay, race conditions, gate skew, power dissipation, partitioning, maintainability, testability, tool usage and qualification, environmental, and fabrication associated with the underlying technologies to be used.

RESPONSE:

As described in the response to RAI 07.01-1, STPNOC plans to make technical report(s) on Toshiba's Non-rewritable Field Programmable Gate Array (NRW-FPGA) based platforms for Neutron Monitoring System (NMS) and Reactor Trip and Isolation System (RTIS) available for NRC Staff review through the Design Acceptance Criteria (DAC) closure process. The technical report(s) will address COLA Part 2, Tier 1, Section 3.4, Table 3.4 Items 7 through 10, 12 and 14. The technical items such as timing, delay, race conditions, gate skew, power dissipation, partitioning, maintainability, testability, tool usage and qualification, environmental, and fabrication will be specifically addressed in sufficient detail for STPNOC and NRC Staff acceptance. STPNOC Letter U7-C-STP-NRC-090059 provides a schedule for when these documents will be available for NRC Staff review.

A summary of how the NMS and RTIS FPGA-based platforms address each technical item is provided below.

FPGA Logic Design:

To address timing delays, race conditions, clock skew, power dissipation, and partitioning, Toshiba has implemented rules for the design of FPGA-based systems. The following paragraphs provide a brief description of the design rules implemented for the design of FPGAs.

Because FPGAs are arrays of logic cells and registers, each cell connected in series adds delay. As a result, it might not be possible to meet timing constraints on a critical path with too many cells connected in series. To ensure that timing constraints can be met, clocked synchronous design is used to avoid timing errors. For synchronous design, changes of state occur only at selected times, controlled by a clock signal. Also, the logic is designed to ensure that the design provides adequate shaping on the inputs to the FPGA to avoid slew edge rates.

To minimize risks associated with timing, analysis and simulation are performed during the design process. This two-part process includes static timing analysis and dynamic timing simulation. Static timing analysis evaluates the setup and hold times on each path within the FPGA design. The software tool evaluates the propagation delay to each element in the code in order to determine each timing path in the code. Also, a simulator is used to validate the design with dynamic simulation, using accurate propagation delays.

Because clock skew is a key factor in setup and hold time verification of registers, designers verify clock skew during synthesis and simulation of the FPGA.

Tool Usage and Qualification:

Software tools are used to design and implement the logic in the FPGA. The development of FPGA-based system follows a process similar to that used in a software lifecycle. The FPGA logic lifecycle is analogous to a software lifecycle and includes the normal features and design outputs of the software lifecycle, including design documentation, verification and validation (V&V) records, software safety analyses, change control, and configuration management. This modified software lifecycle approach meets STPNOC's requirements for software life cycle.

Maintainability and Testability:

The FPGA modules may require replacement to remove latent errors, to address revised requirements, or to accommodate modifications in the operating environment. Because FPGAs are one-time programmable devices, after an FPGA-based product is completed, no changes to the system logic are possible without replacing the module where the FPGA is installed. Any changes to the system must be made under strict change-control procedures.

The new FPGAs are tested by the manufacturer and then installed and tested at the plant.

The FPGA-based system testability includes self-diagnostic functions that continuously verify proper FPGA and communications performance and provide outputs used to alert the operator. Other maintenance and testing includes:

- Users Manual contains recommendations for maintenance.
- Maintenance procedures will be written with the guidance from the Users Manual.
- Gain adjustment as described in the response to RAI 07.01-1 is performed on a frequency specified in the Technical Specification.
- The surveillance testing is used to detect failures to lower the risk of occurrence of any problem that could adversely affect plant operation or safety.

Environmental:

The hardware qualification process will demonstrate that the system meets the STPNOC requirements for Electromagnetic Compatibility (EMC) and Equipment Qualification (EQ). These requirements will be made available for NRC Staff review through the DAC process of COLA Part 2, Tier 1, Section 3.4, Table 3.4 Items 12 and 14. STPNOC Letter U7-C-STP-NRC-090059 provides a schedule for when these documents will be available for NRC Staff review.

Fabrication:

The fabrication process is described in detail in the technical reports to be made available for NRC Staff review through the DAC process.

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

RAI 07.09-7

QUESTION:

Departure STD DEP T1 3.4-1, Safety-Related I&C Architecture, proposed a new data communication technology in the COLA. Therefore, include all specific functions related to the new communication technology in the COLA, for example, test and inspection for redundancy function at the component level (power supplies module, interface module, processor, etc.), network communication speed, and load capability.

RESPONSE:

STPNOC's response to RAI 07.09-1 provides additional information primarily focused on interfaces among the various platforms for the STP 3&4 safety-related systems communication to the nonsafety-related systems.

The safety-related and nonsafety-related functions are given in COLA Part 2, Tier 1, Subsection 2.7.5 and COLA Part 2, Tier 2, Subsection 7.9S.2. Tier 1, Table 2.7.5 provides a definition of the ITAAC for the Data Communications ECFs and NECFs. This ITAAC is considered sufficient for testing and acceptance of the data communications systems.

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

RAI 07-1

QUESTION:

COLA FSAR Tier 1 Section 2.2.7 has been annotated with departure number STD DEP T1 2.2-1. However, the staff is unable to find any changes in this section that may have resulted from departure STD DEP T1 2.2-1. Verify the applicability of departure STD DEP T1 2.2-1 to COLA FSAR Tier 1 Section 2.2.7.

RESPONSE:

STD DEP T1 2.2-1 does not make any changes to COLA Tier 1 Section 2.2.7. That annotation should have been removed in COLA Revision 2.

The departure number reference in Section 2.2.7 will be deleted as shown below:

~~STD DEP T1 2.2-1~~

RAI 07-2

QUESTION:

Based on COLA FSAR Tier 1 departure STD T1 3.4-1, process computer system (PCS) was replaced with plant computer functions (PCFs). Design Description provided for the PCFs in COLA FSAR Tier 1, Section 2.2.11 is inconsistent with the system description provided in COLA FSAR Tier 2, Section 7.7.1.5. 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 staff requests STPNOC to resolve these inconsistencies.

RESPONSE:

Details will be added to COLA Tier 2 Subsection 7.7.1.5, "Plant Computer Functions (PCF) – Instrumentation and Controls" to resolve the inconsistencies between this subsection and COLA FSAR Tier 1, Section 2.2.11.

The following paragraphs will be added to COLA Tier 2 Subsection 7.7.1.5, "Plant Computer Functions (PCF) – Instrumentation and Controls" as the first information after *(1) System Identification:*

(1) System Identification

The Plant Computer Functions (PCF) are a set of control, monitoring, and data calculation functions that are implemented on digital central processing units and associated peripheral equipment provided by the Plant Information and Control System (PICS). Redundant processors are used for functions that are important to plant operation. The PCF are classified as non-safety related.

The PCF perform local power range monitor (LPRM) calibrations and calculations of fuel operating thermal limits data, which is provided to the automated thermal limit monitor (ATLM) function of the Rod Control & Information System (RCIS) for the purpose of updating rod block setpoints.

The PCF also include top-level controller functions which monitor the overall plant conditions, issue control commands and adjust setpoints of lower level controllers to support automation of normal plant startup, shutdown, and power range operations. In the event that abnormal conditions develop in the plant during operations in the automatic mode, these functions automatically revert to the manual mode of operation.

The ~~PCS includes~~ PCF include *two subsystems, the Performance Monitoring and Control Subsystem (PMCS) and the Power Generation Control Subsystem (PGCS). Between them, the two subsystems perform the process monitoring and control and the calculations that are necessary for the effective evaluation of normal and emergency power plant operation. The ~~PCS is~~* PCF are *designed for high reliability utilizing redundant, network combined processing equipment which is capable of processing data, servicing subsystems, providing supervisory control over digital control systems and presenting data to the user.*

RAI 07-3

QUESTION:

In Design Description for COLA FSAR Tier 1 Section 2.2.7, "Reactor Protection System," applicant deleted the description of interfaces between 1) the RPS and MSIV closure signals; and 2) RPS and Suppression Pool Temperature trip. These changes are based on departure STD DEP T1 3.4-1. However, the Departure Report does not provide any justification for these changes. Provide justification for these changes.

RESPONSE:

Changes in the Design Description provided in STP 3&4 COLA Tier 1 Section 2.2.7 reflect the new Non-Rewriteable Field Programmable Gate Array (FPGA) based platforms. The interfaces between 1) the Reactor Protection System (RPS) and Main Steam Isolation Valve (MSIV) closure signals; and 2) RPS and Suppression Pool Temperature trip were not deleted in STD DEP T1 3.4-1, although some text dealing with those interfaces was deleted from paragraph 4 for clarity. Both of those interfaces are shown on Figure 2.2.7a as noted in paragraph 1 and further detailed below.

The interface between the RPS and MSIV closure signals is listed as "(7) Main Steamline Isolation [NBS]" in the text.

The interface between the RPS and Suppression Pool Temperature trip is listed as "(9) High Suppression Pool Average Temperature [SPTM]" in the text.

No COLA Change is required with this RAI response.

RAI 07-4

QUESTION:

In Design Description for COLA FSAR Tier 1 Section 2.2.7, "Reactor Protection System," applicant added a new paragraph "The OLU and LDs are implemented with non-microprocessor-based equipment. The remaining RPS functions are primarily implemented with microprocessor-based equipment configurable logic devices." Statements made in the paragraph are inconsistent with the changes described for STD DEP T1 3.4-1 in the Departure Report. The staff requests STPNOC to resolve these inconsistencies.

RESPONSE:

There was a word processing error that did not remove words which were to be replaced by "configurable logic devices."

The added paragraph in FSAR, Tier 1, Subsection 2.2.7 will be changed as shown below:

> The OLU and LDs are implemented with non-microprocessor-based equipment. The remaining RPS functions are primarily implemented with ~~microprocessor-based equipment~~ configurable logic devices.

RAI 07-7

QUESTION:

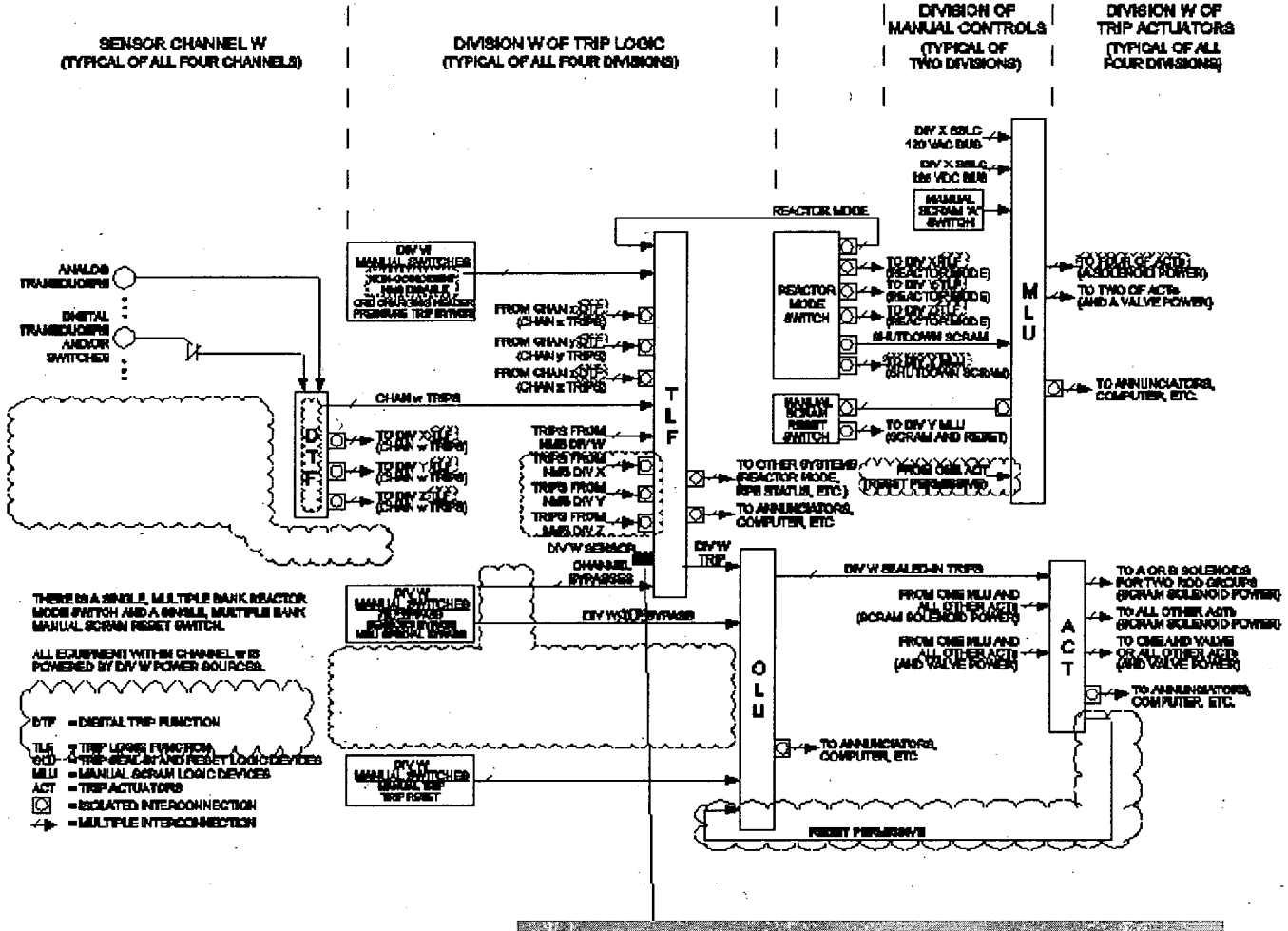
Based on STD DEP T1 3.4-1, the applicant added a sentence in COLA FSAR Tier 1 subsection A(3) of Section 3.4 stating, "The TLF also receives input directly from the Neutron Monitoring System and manual control switches." Whereas, according to the COLA FSAR Tier 2, Figure 7.2-2, the Trip Logic Function (TLF) also receives direct input from the sensor channel(s) of corresponding division. Provide the design description of the sensor channel(s) with direct input to the TLF, and evaluate the impact on Figure 3.4b.

RESPONSE:

STP 3&4 COLA Revision 2, Tier 1 Figure 3.4b shows a simplified arrangement of the safety system logic for one division. Note 2A of the figure indicates that the inputs for Neutron Monitoring System (NMS) are not shown. This is consistent with the level of information in Tier 1 Figure 3.4b of the reference ABWR DCD.

There are no sensor channels with direct inputs into the Trip Logic Function (TLF) of the Reactor Trip and Isolation System (RTIS). This is consistent with the descriptions in Tier 1 Subsection 2.2.7 and Tier 2 Subsection 7.2.1.1.4.1. The COLA Part 2, Tier 2, Figure 7.2-2 is not correct; the arrow showing Division W sensor input to the TLF will be removed. The "Div W Sensor" text applies to the Channel Bypass text below it. That arrow will be "Div W Sensor Channel Bypass."

A markup of COLA Part 2, Tier 2, Figure 7.2-2 is provided with this RAI response and will be included in a future COLA revision.



The change made in the red cloud was to delete the erroneous arrow to TLF. It is not the Div W Sensor alone that goes to the TLF. It is the Div W Sensor Channel Bypasses that go from the Div W Manual Switches to the TLF.

RAI 07-8

QUESTION:

Based on STD DEP T1 3.4-1, the applicant has deleted from COLA FSAR Tier 1 subsection A(5) of Section 3.4 the design concept of each division containing two engineered safety features (ESF) processing channels each containing a pair of SLU. The Departure Report fails to provide any justification for making this change in the design concept. Provide adequate justification for this change in design concept.

RESPONSE:

STP 3&4 COLA Part 7, departure STD DEP T1 3.4-1 Description, Item (2) "Elimination of unnecessary inadvertent actuation prevention logic and equipment" was previously addressed in the RAI 07.03-1 response. This response provided expanded bases for limiting the application of the dual redundant Safety System Logic Functions (SLFs), which replace the Safety System Logic Units (SLUs). It also provided bases for retention of two forms of dual redundancy in certain cases along with an expanded justification for item (2) of this departure. In addition, this response identified which functions did not require this logic feature and the justification bases for each function.

STP 3&4 COLA Part 2, Tier 1 Subsection 3.4.1 (changed back to Subsection 3.4.A) under "The ELCS portion of SSLC ..." Item (3) has a paragraph that captures the related Tier 1 requirements as:

> "The SLF logic for ECCS functions (i.e. initiation of Reactor Core Isolation Cooling, High Pressure Core Flooder, Low Pressure Core Flooder or Automatic Depressurization) is implemented using redundant processing channels. The redundant channels receive the same input data from the DTF, manual control switch inputs and contact closures and perform the same trip decision logic. A majority of the redundant processors must agree for initiation of the function to occur, in order to assure that failure of a single electronic module will not result in inadvertent coolant injection into the core or inadvertent depressurization. The final majority vote of the system initiation signals is accomplished with non-microprocessor based equipment in the logic or with a separate actuation of system valves and pumps, where both are required to initiate coolant injection."

Also, STP 3&4 COLA, Part 2, Tier 2 will be updated with a new Section 7.1S.2 as described in STPNOC's RAI 07-6 response. The related and supporting Tier 2 requirements are in new Subsection 7.1S.2.1 as:

> "As shown in 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."

And later it states:

> "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."

The above referenced RAI responses and related Tier 1 content and proposed Tier 2 additional content provide the information and resolution to this RAI.

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

RAI 07-9

QUESTION:

Based on STD DEP T1 3.4-1, the applicant has added design description for ESF Logic & Control System (ELCS) portion of Safety System Logic & Control (SSLC) in COLA FSAR Tier 1 subsection A(3) of Section 3.4. Some of the added statements are vague, e.g., A majority of redundant processors must agree …., … logic for some isolation and supporting ESF functions …, Other ELCS functions are implemented using redundancy …., etc. With these types of statements, inspection/verification of associate ITAAC would be impossible. Provide specific design details that outline the ESF functions and their need for redundant or non-redundant processing channels. Criteria for selecting the ESF functions that do not require redundant processing channels should also be provided.

RESPONSE:

In STPNOC's response to RAI 07-6, an addition to the COLA Part 2, Tier 2 Section 7.1S.2 was presented. In that COLA addition, the redundant SLF processing channels and the two-out-of-two voting of the channels was described. Also in response to RAI 07.03-1, a list of Functions for which there was a modification of the 2-out-of-2 voting was provided. This response also provided the Bases for limiting the application of dual redundant SLFs.

Additional information is provided below regarding design criteria for ESF functions.

SLF redundancy is categorized into the following four cases. The concept for categorization is described in COLA Part 2, Tier 1, Subsection 3.4.1, Item (3) under ELCS discussion as follows.

1. A majority of the redundant processors must agree for initiation of the function to occur, in order to assure that failure of a single electronic module will not result in inadvertent coolant injection into the core or inadvertent depressurization. The final majority vote of the system initiation signals is accomplished with non-microprocessor based equipment in the logic or with a separate actuation of system valves and pumps, where both are required to initiate coolant injection.
2. The SLF logic for some isolation and supporting ESF functions are also implemented using redundant channels where such implementation increases the operator response time to avoid plant operational impact following postulated failure in the control equipment. In these cases, an operator bypass that reduces the logic to a single channel may be utilized where such logic reduces the risk of unnecessary adverse plant operational impact.
3. Other ELCS functions are implemented using redundancy where such logic provides overall plant operating or maintenance benefits.
4. Non-redundancy in processing channels.

Case 1 is applied to ECCS (i. e. RCIC, HPCF, LPFL, or ADS). This structure is described in COLA Part 2, Tier 2, Chapter 16, Figures B 3.3.1.4-2, B 3.3.1.4-3 or B 3.3.1.4-4.

Case 2 is mainly applied to equipment that is normally in operation and does not have redundancy of equipment (example: RCW isolation valve of non-safety loads). This structure is described in COLA Part 2, Tier 2, Chapter 16, Figure B 3.3.1.4-5.

Case 3 is applied when equipment malfunction does not impact plant operation. However, the logic redundancy benefits plant operation or maintenance. Applicable equipment for case (3) is determined during detailed design. COLA Part 2, Tier 2, Chapter 16, Figure B 3.3.1.4-2 or Figure B 3.3.1.4-5 is applied to the structures.

Case 4 is applied when equipment malfunction does not impact plant operation as in case 3, and failure to take action does not affect system functions. The major equipment applied is shown in the response to RAI 07.03-1. This structure is described in COLA Part 2, Tier 2, Chapter 16, Figure B 3.3.1.4-1.

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

RAI 07-10

QUESTION:

Based on STD DEP T1 3.4-1, the applicant has revised design description for ELCS portion of SSLC in COLA FSAR Tier 1 subsection A(4) of Section 3.4. The first sentence in the subsection appears to be incomplete, which simply states "local inputs." Also the applicant added a statement that states, "ELCS logic and controls are implemented through three divisions corresponding to the three divisions of controlled equipment." This statement is in contradiction with design details provided in various other parts of the COL application, which imply that there are four divisions of ELCS. Complete the missing information, and resolve the stated conflicting information.

RESPONSE:

The STP 3&4 COLA text "local inputs" will be deleted as shown in COLA Part 2, Tier 1 Subsection 3.4.A. Additional text also will provide clarification about the four divisions of I&C control functions communicating status to the three divisions of ESF actuated equipment.

Other ELCS functions are implemented using redundancy where such logic provides overall plant operating or maintenance benefits.

~~5. (6)For reactor trip or MSIV closure if a 2--out-of-4 trip condition of sensors is satisfied, all four divisions' trip outputs produce a simultaneous coincident trip signal (e.g., reactor trip) and transmit the signal through hardwired connections (and isolators where necessary) to load drivers that control the protective action of the actuators. The load drivers 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.~~

~~(7)For ESF functions, the trip signals in three divisions are transmitted by the Essential Multiplexing System to the RMUs~~ ~~local inputs~~~~. where a final 2--outof-2 logic comparison is made prior to distribution of the control signals to the final actuators. ESF outputs do not exist in Division IV.~~ As described above, 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. No ESF actuated equipment exists in Division IV. The final SLF actuation outputs are distributed to the final system actuated equipment ~~control elements~~ through the RDLC remote I/O devices. ~~ELCS logic and controls are implemented through three divisions corresponding to the three divisions of controlled equipment.~~

RAI 07-11

QUESTION:

Based on STD DEP T1 3.4-1, the applicant had renumbered the subsections of Tier 1 COLA FSAR Section 3.4, i.e., subsection 'A' to '3.4.1', 'B' to '3.4.2', and 'C' to '3.4.3'. In the STPNOC letter U7-C-STP-NRC-090009, dated February 9, 2009, the applicant reverted back the subsection numbering from '3.4.1' to 'A' and '3.4.3' to 'C'. However, the applicant did not revert back numbering of the subsection '3.4.2' to 'B'. Parts of the COLA FSAR Tier 1 document still make references to subsection 'B'. The NRC staff requests STPNOC to resolve this conflict.

RESPONSE:

To be consistent with the ABWR DCD, numbering of Section 3.4 subsections has been changed back to alpha designations.

Section 3.4 subsections have been changed back to alpha designations, as shown below:

~~*3.4.1*~~ A ***Safety System Logic and Control***

~~*3.4.2*~~ ***B I & C Development and Qualification Processes***

~~*3.4.3*~~ C ***Diversity and Defense-in-Depth Considerations***

RAI 07.07-7

QUESTION:

The NRC Staff has identified a possible "typo" in Tier 2 departure STD DEP 7.7-1 wording. The STP 3 and 4 COLA Part 7, "Departure Report", for STD DEP 7.7-1, explained that a clarification was needed to indicate that the flushing to prevent the build-up of non-condensable gases was only needed for those instrument lines with a condensing chamber. STD DEP 7.7-1,"RPV Water Level Instrumentation, adds a sentence to ABWR DCD, Section 7.7.1.1, item (6) that states, "This applies to (a) through (e) above". However, "(e)" is for the Reactor Well Water Level Range. Since this range is: 1) used to monitor the reactor water level when the reactor vessel head is removed, 2) the reactor system is flooded during refueling with a calibration at 0 MPag and 48.9 degrees C, and 3) the lower point uses the RPV tap below the top of the active fuel while the upper point is far above the RPV. The NRC Staff determined that the "e" may be a "typo" type error and should actually be a "d". Correct this apparent "typo", if in fact this Reactor Well Water Level Range water level instrument actually does not have a condensing chamber and "d" was actually intended.

RESPONSE:

Only water level instruments (a) through (d) of ABWR DCD, Tier 2 Subsection 7.7.1.1 (6) require the Control Rod Drive water for flushing of the instrument line to prevent the build-up of non-condensable gases in the condensing chamber.

COLA Part 2, Tier 2 Subsection 7.7.1.1 (6) after item (e), has been revised as shown below:

(e) Reactor Well Water Level Range

The concern that non-condensable gasses may build-up in the water column in the reactor vessel reference leg water level instrument lines, i.e., the reactor vessel instrument lines at the elevation near the main steam line nozzles, has been addressed by continually flushing these instrument lines with water supplied by the Control Rod Drive (CRD) System for those instrument lines with a condensing chamber. This applies to (a) through ~~(e)~~(d) above.

RAI 07.07-8

QUESTION:

The NRC Staff has identified a possible "typo" in the "Description" wording of departure STD DEP 7.7-18. STP 3 & 4 identified departure STD DEP 7.7-18 as involving changes to technical specifications (TS) and thus requiring prior NRC approval. In TS Bases B 3.10.3, "LCO", the departures "STD DEP 7.7-18" and "STD DEP 16.3-24" are listed (above the word "LCO") as the departures that describe the change, but the departure "Description" for "STD DEP 7.7-18" refers to changes in B.3.10.3, "Background" and "Applicable Safety Analysis." There are no changes at all in the "Applicable Safety Analysis" leading to the possibility that "Applicable Safety Analysis" was actually intended to be "LCO." Further the departure "Description" of STD DEP 7.7-18 does not sufficiently identify the change that exist under "LCO" so the NRC Staff can complete the review of STD DEP 7.7-18. Provide a resolution on the concern described above.

RESPONSE:

The typo is not in the COLA Part 7, Section 2.2, "Description" wording for departure STD DEP 7.7-18. The typo is in the COLA Part 2, Tier 2, Subsection 16B.3.10.3 Bases markup of TS 3.10.3 Applicable Safety Analysis, in which the words "Rod Test Switch" were inadvertently removed rather than shown lined out in Rev 2. STD DEP 7.7-18 affects TS 3.9.3 Bases Background, TS 3.10.3 Bases Background and Applicable Safety Analysis, TS 3.10.4 Bases Background and Applicable Safety Analysis, and TS 3.10.5 Bases Background and Applicable Safety Analysis, in which "Rod Test Switch" is replaced by "RCIS scram test mode."

The TS 3.10.3 Bases LCO section is not affected by STD DEP 7.7-18. It is only affected by STD DEP 16.3-24, which removes the reference to LCO 3.10.4, Control Rod Withdrawal-Cold Shutdown, because LCO 3.10.4 does not apply in this situation; and therefore, is not an accurate reference for this section.

STP 3&4 COLA Part 2, Tier 2, Subsection 16B.3.10.3 will be changed in a future revision as shown below, with gray shading showing the changes.

B 3.10 SPECIAL OPERATIONS

B 3.10.3 Control Rod Withdrawal – Hot Shutdown

BASES

The information in this section of the reference ABWR DCD, including all subsections, is incorporated by reference with the following departures.

STD DEP 7.7-18
STD DEP 16.3-24

BACKGROUND

The purpose of this MODE 3 Special Operations LCO is to permit the withdrawal of a single control rod, or control rod pair, for testing while in hot shutdown, by imposing certain restrictions. In MODE 3, the reactor mode switch is in the shutdown position, and all control rods are inserted and blocked from withdrawal. Many systems and functions are not required in these conditions, due to other installed interlocks that are actuated when the reactor mode switch is in the shutdown position. However, circumstances will arise while in MODE 3 that present the need to withdraw a single control rod, or control rod pair, for various tests (e.g., friction tests, scram timing, and coupling integrity checks). These single control rod, or control rod pair, withdrawals are normally accomplished by selecting the refuel position for the reactor mode switch. A control rod pair (those associated by a shared CRD hydraulic control unit) may be withdrawn by utilizing the ~~Rod Test Switch~~ RCIS scram test mode which "gangs" the two rods together for rod position and control purposes. This Special Operations LCO provides the appropriate additional controls to allow a single control rod, or control rod pair, withdrawal in MODE 3.

APPLICABLE SAFETY ANALYSES

With the reactor mode switch in the refuel position, the analyses for control rod withdrawal during refueling are applicable and, provided the assumptions of these analyses are satisfied in MODE 3, these analyses will bound the consequences of an accident. Explicit safety analyses (Ref. 1) demonstrate that the functioning of the refueling interlocks and adequate SDM will preclude unacceptable reactivity excursions.

Refueling interlocks restrict the movement of control rods to reinforce operational procedures that prevent the reactor from becoming critical. These interlocks prevent the withdrawal of more than one control rod or control rod pair. Under these conditions, the core will always be shut down even with the highest worth control rod pair withdrawn if adequate SDM exists.

Control rod pairs have been established for each control rod drive hydraulic control unit (except for the one rod which has its own accumulator). These pairs are selected and analyzed so that adequate shutdown margin is maintained with any control rod pair fully withdrawn. When the ~~rod test switch~~ RCIS scram test mode is used and GANG mode is selected for the RCIS, the selected rod pair is substituted for a single rod within the appropriate logic in order to satisfy the refuel mode rod-out interlock. The rod pair may then be withdrawn simultaneously.

~~STD DEP 7.7-18~~
STD DEP 16.3-24

LCO

As described in LCO 3.0.7, compliance with this Special Operations LCO is optional. Operation in MODE 3 with the reactor mode switch in the refuel position can be performed in accordance with other Special Operations LCO (i.e., LCO 3.10.2, "Reactor Mode Switch Interlock Testing," ~~and LCO 3.10.4,"Control Rod Withdrawal – Cold Shutdown"~~) without meeting this Special Operations LCO or its ACTIONS. However, if a single control rod, or control rod pair, withdrawal is desired in MODE 3, controls consistent with those required during refueling must be implemented and this Special Operations LCO applied. The refueling interlocks of LCO 3.9.2, "Refuel Position Rod-Out Interlock," required by this Special Operations LCO, will ensure that only one control rod, or control rod pair, can be withdrawn.

RAI 07.07-9

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 "Description" describes a change to the TS Bases for Subsection B 3.9.4. However, the "Evaluation Summary" discusses the TS Bases for B 3.4.3. This appears to be a "typo" type error that needs to be corrected. Correct this apparent "typo" error.

RESPONSE:

STP 3&4 COLA, Part 7, Section 2.2, STD DEP 7.7-10, Evaluation Summary, has been corrected as follows:

Evaluation Summary

~~Special circumstance (iv) applies in that the departure represents a net benefit to the public health and safety by providing additional interface and feedback check on rod position and control functions. It also better integrates the control rod interface with overall control room human factors design.~~

~~This exemption is not inconsistent with the Atomic Energy Act or any other statute and therefore is authorized by law. As discussed above, the design change represents an improvement and therefore will not present an undue risk to the public health and safety. The design change does not relate to security and does not otherwise pertain to the common defense and security.~~

This proposed change does not affect Tier 1 or Tier 2* information, however it does affect the bases of Technical Specification ~~3.4.3~~ 3.9.4 and therefore requires prior NRC approval. This proposed change was evaluated per Section VIII.C.4 of Appendix A to 10CFR part 52 and:

1. This proposed change is not inconsistent with the Atomic Energy Act or any other statute and therefore is authorized by law. This proposed change consists only of rewording for clarification and editorial correction with no change to the meaning or intent of the original bases of Technical Specification ~~3.4.3~~ 3.9.4, and therefore will not present an undue risk to the public health and safety. This proposed change does not pertain to the common defense and security.

The STP 3&4 COLA, Part 2, Tier 2 Technical Specification Bases 3.9.4 reference departure was corrected in COLA Revision 3 as follows:

B 3.9 REFUELING OPERATIONS

B 3.9.4 Control Rod Position Indication

BASES

The information in this section of the reference ABWR DCD, including all subsections, is incorporated by reference with the following departure.

STD DEP 7.7~~-18~~ -10