Nuclear Innovation
North America LLC
4000 Avenue F, Suite A
Bay City, Texas 77414

February 23, 2011
U7-C-NINA-NRC-110031

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 No. 52-012 and 52-013
Submittal of I&C Information

Reference: Letter from Scott Head to Document Control Desk, "Submittal of I&C Information," dated January 19, 2011, U7-C-STP-NRC-110013 (ML110250367)

In the referenced letter, STP Nuclear Operating Company (STPNOC) submitted proposed Appendix 7DS to Part 2, Tier 2 of the South Texas Project Units 3 and 4 (STP 3 & 4) Combined License Application (COLA).

In response to discussions with the Advisory Committee on Reactor Safeguards Advanced Boiling Water Reactor Subcommittee meeting on February 8, 2011, Nuclear Innovation North America (NINA) submits a revision to Appendix 7DS, as shown in the attachment.

This change to Appendix 7DS, Digital Instrumentation and Control Design Verification for Safety-Related Systems, will be made to STP 3 & 4 COLA, Part 2, Tier 2, in a future revision.

There are no commitments in this letter.

If there are any questions regarding this submittal, please contact me at (361) 972-7136, or Bill Mookhoek at (361) 972-7274.

D091
NRO

STI 32829370

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

Executed on 2/23/11

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

jwc

Attachment: as stated

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.
Inspection Unit Manager
Texas Department of State Health Services
P. O. Box 149347
Austin, Texas 78714-9347

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

*Adrian Muniz
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852

(electronic copy)

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

Steve Winn
Joseph Kiwak
Jamey Seely
Eli Smith
Nuclear Innovation North America

Peter G. Nemeth
Crain, Caton and James, P.C.

Richard Peña
Kevin Pollo
L. D. Blaylock
CPS Energy

STP 3&4 COLA, Part 2, Tier 2, Appendix 7DS, Digital Instrumentation and Control Design Verification for Safety-Related Systems, was submitted to the NRC in letter U7-C-STP-NRC-110013 dated January 19, 2011. Subsection 7DS.1.3 is revised as shown below in gray highlight and will be incorporated in a future revision.

7DS.1.3 Determinism

The response time requirement for each NMS and RTIS safety-related function is determined by the Safety Analysis. The response time must be predictable and repeatable to be considered deterministic. The response time for all NMS and RTIS safety functions is deterministic. A description of the FPGA platforms that make the NMS and RTIS response deterministic is provided below.

The FPGA-based system designs use multiple FPGAs on some modules. To enhance testability and reduce undesirable circuit behavior, the basic architecture within each FPGA is a clocked sequential circuit, with periodic synchronizing registers within the FPGAs. Each FPGA only starts processing data when data is transferred into that FPGA, and sends data to the next FPGA or module when processing is complete. Thus, the functions in a given module execute in sequence that is inherently deterministic based on the clocked sequence. The first FPGA completes its function, and then provides data to the next FPGA. When that FPGA completes its function, it provides data to the next FPGA. In addition, when all signal processing FPGAs have finished passing data to the next, the signal processing watchdog timer on the module resets and restarts timing. The watchdog timer is hardware-based and is diverse from the FPGA circuits on each module. {Failure of a signal processing FPGA to complete and pass data to the next FPGA will result in all subsequent FPGAs on that module failing to start. If this occurs in the FPGAs that implement the signal processing and thus the safety functions, the module is marked as failed, the watchdog timer times out, resulting in the tripped division, and an alarm is provided to the operator. Two tripped divisions will result in a reactor scram via the two-out-of-four voting arrangement. The watchdog timer on each module is designed to be fully testable.}[7]

Because FPGAs are arrays of logic cells and registers, each cell connected in series adds defined delay to the logic circuit. {As a result, the logic within each FPGA is designed, verified, and validated to ensure operation within timing constraints under expected operating conditions. The clocked synchronous design is used within each FPGA to avoid timing errors and to ensure timing constraints are satisfied. For synchronous design, changes of state within the FPGA occur only at selected times, controlled by a timing signal. The logic within each FPGA is designed to ensure that the design provides adequate shaping on the inputs to the FPGA to providing sufficient slew on the signal edges.}[8]

{To avoid timing errors within FPGAs, analysis and simulation are performed during the design process. This two-part process includes static timing analysis and dynamic

timing simulation. Static timing analysis demonstrates that the setup and hold times on each path within the FPGA design are within predetermined parameters. Software tools used to perform the static timing analysis also are used to evaluate the propagation delay to each element in the code to confirm each timing path in the code is within predetermined paramaters. Also, a diverse set of dynamic simulation software tools are used to validate the design, using predetermined, accurate propagation delays, which are set based on the chosen cells and paths within the routed FPGA. These analyses provide data to the designer to verify that appropriate logic implementation has been achieved, eliminating any potential concerns regarding signal races, signal setup and hold times, and clock skew. A report is generated for implementation including safety analyses.}[10]

{The communication protocols used in the FPGA platforms are deterministic because they are pre-defined, fixed length, fixed format, and generated at specific times in the FPGA logic execution. The communication links that perform safety functions include data and time out error checking to ensure determinism. All detected errors are alarmed. The communication protocols and logic in the communication receivers include self-diagnostics that will generate module failure signals upon detection of communication failures, alerting operators.}[7, 16, 18]

In summary, the FPGA-based, safety-related NMS and RTIS are deterministic. The FPGA platform does not utilize any non-deterministic data communication, non-deterministic computation, interrupts, multitasking, dynamic scheduling, or event driven design. The logic design of the FPGA circuits is fixed and clocked. {The response times for the system elements, including architecture, communications (including timing and loading) and processing elements are tested to verify that the systems' performance characteristics are consistent with the safety requirements established in the design basis for these systems. The analyses are performed to satisfy the design timing requirements set forth in Clause 4.10 of IEEE-603. A report is generated to demonstrate the adequacy of the timing analysis.}[10]