Tennessee Valley Authority, 1101 Market Street, Chattanooga, Tennessee 37402

CNL-15-130

July 10, 2015

10 CFR 50.4

ATTN: Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-001

Watts Bar Nuclear Plant, Unit 2
Construction Permit No. CPPR-92
NRC Docket No. 50-391

Subject: **WATTS BAR NUCLEAR PLANT (WBN) UNIT 2 - DISTRIBUTED CONTROL SYSTEM (DCS) DATA STORM TEST PLAN**

Reference: NUREG-0847, Supplement No. 23, "Safety Evaluation Report Related to the Operation of Watts Bar Nuclear Plant, Unit 2," dated July 2011 (ML11206A499)

The purpose of this letter is to provide the Distributed Control System (DCS) Data Storm Test Plan which satisfies a verbal request from the Nuclear Regulatory Commission (NRC) staff. The completion of the Data Storm Test is the subject of Supplemental Safety Evaluation Report (SSER) 23, Appendix HH, Open Item No. 83 contained in the above reference. TVA will provide the results of the data storm test after completion of the test which is currently scheduled for August 5, 2015.

Enclosure 1 provides the DCS Data Storm Test Plan. Enclosure 2 provides the commitment to provide the test results to the NRC.

Should you have questions regarding this submittal, please contact Gordon Arent at (423) 365-2004.

Respectfully,

J. W. Shea
Vice President, Nuclear Licensing

Enclosures

cc: See Page 2

Enclosures:

1. Watts Bar Nuclear Plant, Unit 2, Distributed Control System (DCS) Data Storm Test Plan
2. List of Commitments

cc (Enclosures):

U.S. Nuclear Regulatory Commission, Region II
NRC Project Manager - Watts Bar Nuclear Plant, Unit 2
NRC Senior Resident Inspector - Watts Bar Nuclear Plant, Unit 2

ENCLOSURE 1
WATTS BAR NUCLEAR PLANT, UNIT 2
DISTRIBUTED CONTROL SYSTEM (DCS) DATA STORM TEST PLAN

PURPOSE:

The purpose of this test plan is to establish the requirements, test methodology, and acceptance criteria for the non-safety related Foxboro (Invensys) Intelligent Automation (I/A) Distributed Control System (DCS) Data Storm test. This test plan is driven by Supplemental Safety Evaluation Report (SSER) 23 of NUREG-0847 (ADAMS Accession No. ML1206A499), where Tennessee Valley Authority (TVA) was to provide the results of the DCS data storm test to the Nuclear Regulatory Commission (NRC).

DCS CONFIGURATION:

The Watts Bar Nuclear Plant (WBN) Unit 2 DCS is the control and monitoring platform for most of the Nuclear Steam Supply System (NSSS) and Balance of Plant (BOP) systems. The basic configuration of the DCS are redundant fault tolerant control processor (CP) pairs, redundant power supplies with diverse power sources, redundant communication networks, and redundant operator workstations. Redundant field-bus modules (FBM) are utilized for critical inputs and outputs. The system is designed such that the control system is not affected by the failure of a single device or component for functions important to safe plant operation. The DCS has been segmented, consisting of 15 functional groups, each with a redundant CP pair. See Table 1 below. This segmentation ensures that a failure of one CP pair, with all outputs failing high, low, or as is, maintains independence between redundant control functions and limits the effects of failures on the critical control system.

TABLE 1: FUNCTIONAL GROUPS

GROUP (CP PAIR)	PRIMARY FUNCTION
01	Steam Generator (SG) 1 Level, Feedwater (FW) Flow
02	SG 2 Level, FW Flow
03	SG 3 Level, FW Flow
04	SG 4 Level, FW Flow
05	Main Feedwater (MFW) Pump Speed Control & Steam Dump Loss of Load Interlock
06	Rod Control
07	SG 1 Power Operated Relief Valve (PORV) (Atmospheric Dump)
08	SG 2 PORV (Atmospheric Dump)
09	SG 3 PORV (Atmospheric Dump)
10	SG 4 PORV (Atmospheric Dump)
11	Condenser Steam Dump
12	Pressurizer (PZR) A [Pressure, Level, Charging, Letdown, Spray, Cold Overpressure Mitigation System (COMS)]
13	PZR B (Pressure, Level, Charging, Letdown, Spray, COMS)
14	Auxiliary Control System A
15	Auxiliary Control System B

DCS NETWORK CONFIGURATION:

The WBN Unit 2 DCS is configured with two communication links to the Integrated Computer System (ICS) using separate Network Interface Controller (NIC) hardware and subnet address from the DCS mesh network. The DCS mesh network achieves redundancy using two dedicated NIC cards in each Operator and Engineering workstation. Additionally, DCS is configured with redundant networks and hardwired analog control signal transmission between CP pairs, so that no critical control functions are totally dependent upon the network to ensure the system will continue to function if the network fails.

- DCS Network Impacts to Multiple/Common Systems:
    - There are no digital communications from DCS to any other control system or protection system. The analog inputs from the protection system are transmitted via qualified isolators as on WBN Unit 1.
    - Firewalls between the DCS and ICS limit the volume of data traffic and ensure that common cause events, such as a data storm, do not prevent DCS from performing its design function or prevent any other system from performing its design function.
- This configuration ensures DCS network failures will not propagate to other control or protective systems and result in a condition more severe than already described in Chapter 15 of the Final Safety Analysis Report.

Some communication signals are used in more than one functional group or processor pair and are transmitted to other processors by either hardwired analog connection, peer-to-peer network connection or both. No critical control function is dependent upon the network alone. Figures 1 and 2 provide a depiction of the network configuration. Table 2 below provides the switch and port configuration.

TABLE 2: DCS SWITCH AND PORT CONFIGURATION

Network Switch	Port	Control Groups
W2SW01/W2SW02	1	SG 1 Level, FW Flow
	2	SG 2 Level, FW Flow
	3	SG 3 Level, FW Flow
	4	SG 4 Level, FW Flow
	5	MFW Pump Speed Control, Main Feed Pump (MFP) Recirculation Control, SG Blowdown Control, Cold Leg Accumulator (CLA) N_2 Vent Header Control, Residual Heat Removal (RHR) Heat Exchanger (Htx) A Flow Control, Charging Header Reactor Coolant Pump (RCP) Seals
	6	Rod Control
	7	Hotwell Level Control, SG 1 PORV

TABLE 2: DCS SWITCH AND PORT CONFIGURATION (Continued)

Network Switch	Port	Control Groups
W2SW01/W2SW02 (continued)	8	RHR Htx B Flow Control, SG 2 PORV, Main Feed Pump Turbine (MFPT) Oil Htx A Temp, MFPT Oil Htx B Temp, #3 Heater Drain Tank Level/Flow, #3 Heater Drain Tank Level Bypass
	9	Hotwell Pump Discharge Header Flow, SG 3 PORV, #7 Heater Drain Tank Level, #7 Heater Drain Tank Level Bypass, Stator Cold Leg H_2O Temperature, H_2 Side Seal Oil Temperature, Air Side Seal Oil Temperature, Raw Cooling Water (RCW) Exciter Htx Temperature, RCW H_2 Htx Temperature, Main Turbine Oil Tank Temp
	10	SG 4 PORV, RHR Htx Bypass Flow
	11	Condenser Steam Dump Pressure Control, Loss of Load Interlock
	12	Primary Water Flow, Primary Water Batch, Boric Acid Flow, Boric Acid Batch, PZR Pressure, PZR Pressure Loop (LP) 1 Spray, Excess Letdown Flow
	13	Boric Acid Tank B Recirculation, Charging Flow, Letdown Pressure, Letdown Htx Outlet Temp, PZR Pressure LP 2 Spray, PZR Level, RHR Letdown, Volume Control Tank (VCT) Level
W2SW03/W2SW04	1	Auxiliary Control Room (ACR) VCT Level, ACR SG 1 PORV, ACR SG 3 PORV, ACR Excess Letdown Flow, ACR RHR Letdown, ACR Charging Header Flow, ACR RHR Htx A, ACR RHR Htx Bypass
	2	ACR Letdown Htx Temp, ACR Letdown Pressure, ACR SG 2 PORV, ACR SG 4 PORV, ACR RHR Htx B, ACR Charging Flow, ACR CLA N2 Vent

REQUIREMENTS:

TVA’s Engineering Standard Specification SS-E18.15.01, “Requirements for Digital Systems (Real-Time Data Acquisition and Control Computer Systems),” provides guidelines on testing digital systems and confirming robustness of critical design features including Data Storm testing. It is preferred that data transfer and communication routines be robust with designed in fault recovery such that loss of communications or communications overloads do not adversely affect critical design features. Although the DCS is not safety related, it provides critical plant control and monitoring functions and therefore a Data Storm (network system is overwhelmed by continuous multicast or broadcast traffic) and a loss of network, which can be caused by a Data Storm, are credible failures and thus testing is needed to confirm the ability of the DCS to sustain critical design features.

The WBN Unit 1 and Sequoyah Nuclear Plant (SQN) Unit 1 and Unit 2 have similar DCS platforms already installed and are operational. However, WBN Unit 2 impacts more systems. Although WBN Unit 1 and SQN Unit 1 and 2 demonstrated during their Factory Acceptance Test that a data storm can disable the communication networks and cause one CP of a pair to become non-functional, the control groups, however, continue to operate. The WBN Unit 2 DCS has yet to confirm that the installed configuration will sustain a data storm event without experiencing a plant upset. Therefore, TVA has committed to perform a network data storm test on the installed system prior to final commissioning.

A network data storm test will be performed with the system installed and prior to final commissioning. The test will confirm that the system will continue to function with a failed communication network without any plant upset.

ANALYSIS:

In SSER 23, Section 7.7.1.4.4.2 states that TVA provided a description of the Foxboro I/A Mesh Network, including an analysis of credited network failures. Based on its review of the analysis, the NRC concluded that a Foxboro I/A Mesh Network failure in one segment will not disable another segment. The Data Storm test results are to be analyzed to ensure CP or CP pairs sustain their design function during the data storm event. Segmentation Analysis concluded that events listed in SSER 23, Section 7.7.1.4.4.1, items (1) through (8), will not be caused by the propagation of failures. This test will document that the CP or CP pairs sustain their design function through a data storm event and thereby validates the Segmentation Analysis.

TEST METHODOLOGY:

With the WBN Unit 2 DCS installed, a network Data Storm will be generated to validate system performance. System performance will be accessed thru monitoring and trending critical attributes of each control processor including control processor loading, processor overruns and system alarms. Additionally, Input thru Output timing metrics will be monitored using external test devices on sample Field Bus Module types. The input/output monitoring will demonstrate the effect of the data storm on the processing cycle time of 200 msec and 1 sec requirements which are detailed in the purchase specification. Network Storm testing will be implemented in two phases: Loss of Network and Data Storm. Loss of network is not addressed within this testing plan as it will be performed in a separate test. The loss of network test will confirm that upon loss of network, the system's logic detects loss of peer-to-peer points and the control algorithm switches to the hardwired analog backups.

The Data Storm is initiated in two phases (Broadcast and Multicast) for up to three separate locations within the DCS network, workstation connection, CP switch connections, and the Auxiliary Control Room network switch. Figure 1 provides a depiction of the data storm generation locations.

- Broadcast Storm
    - Overwhelm the network with continuous traffic at maximum speed. This is accomplished utilizing a Packet Generator to send data (all 1s) at maximum speed onto the network with no specific address.
        - This test validates the network switch limiters.
- Multicast Storm
    - Overwhelm the network with continuous traffic at maximum speed. This is accomplished utilizing a Packet Generator to send data (all 1s) at maximum speed onto the network to a specific media access control (MAC) address.
        - This test forces the DCS to process the network data and demonstrates that CP pairs continue to function independent of the network.

ACCEPTANCE CRITERIA:

- Clause 6.3 of IEEE Standard 603-1991 is met and the propagation of failures does not take place beyond the Foxboro I/A mesh network from one segment to another. There is no effect on the Reactor Protection System.
- During a simulated data storm event, network limiter settings/functions are validated.
- During a simulated data/multicast storm, DCS sustains process control capability, and control system segmentation is maintained as detailed in SSER 23, Section 7.7.1.4.4.1, items (1) through (8) by monitoring demand signals.

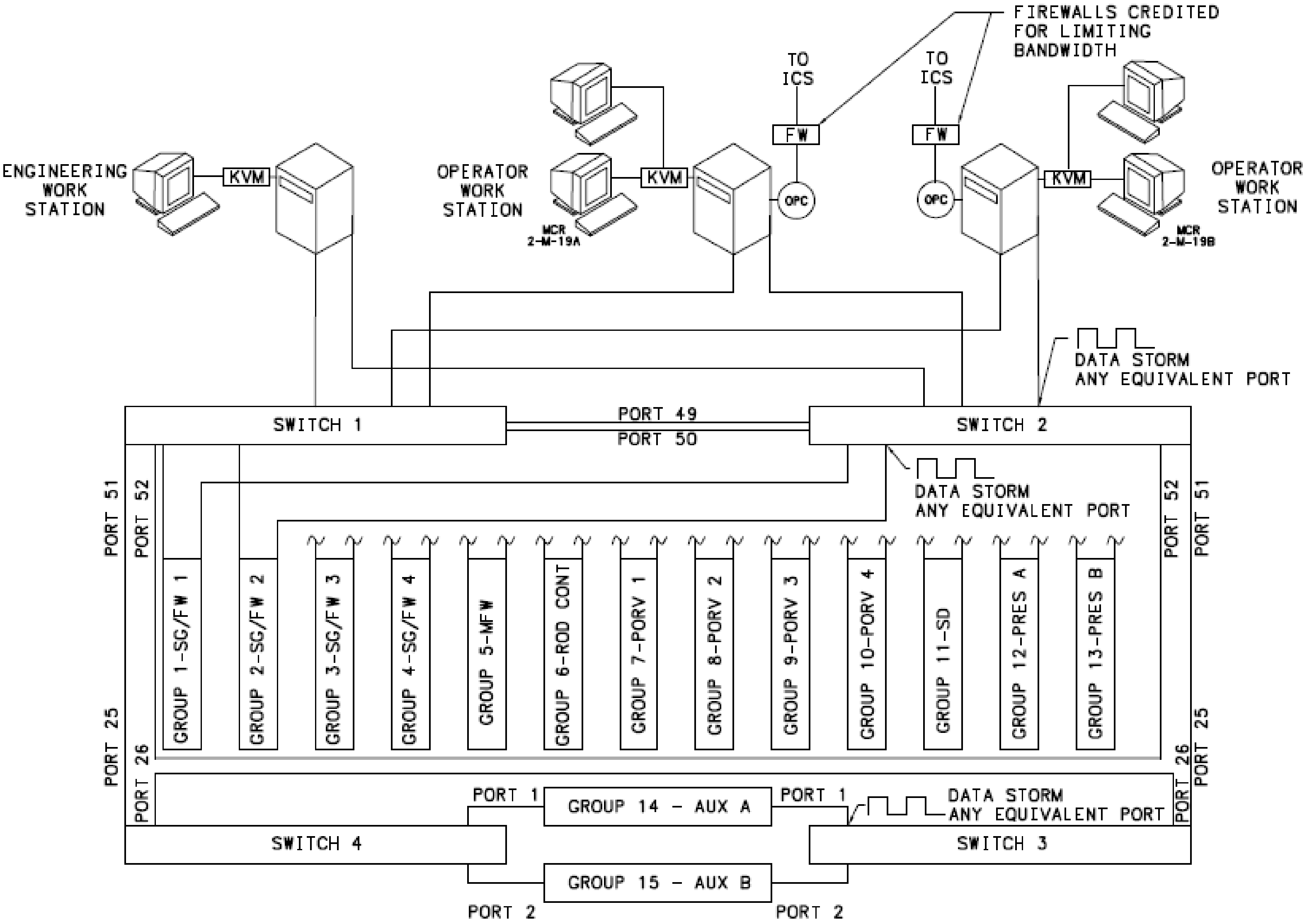

FIGURE 1: DCS NETWORK CONFIGURATION
(INFO ONLY - SOME DETAILS AND CONNECTIONS ARE NOT SHOWN)

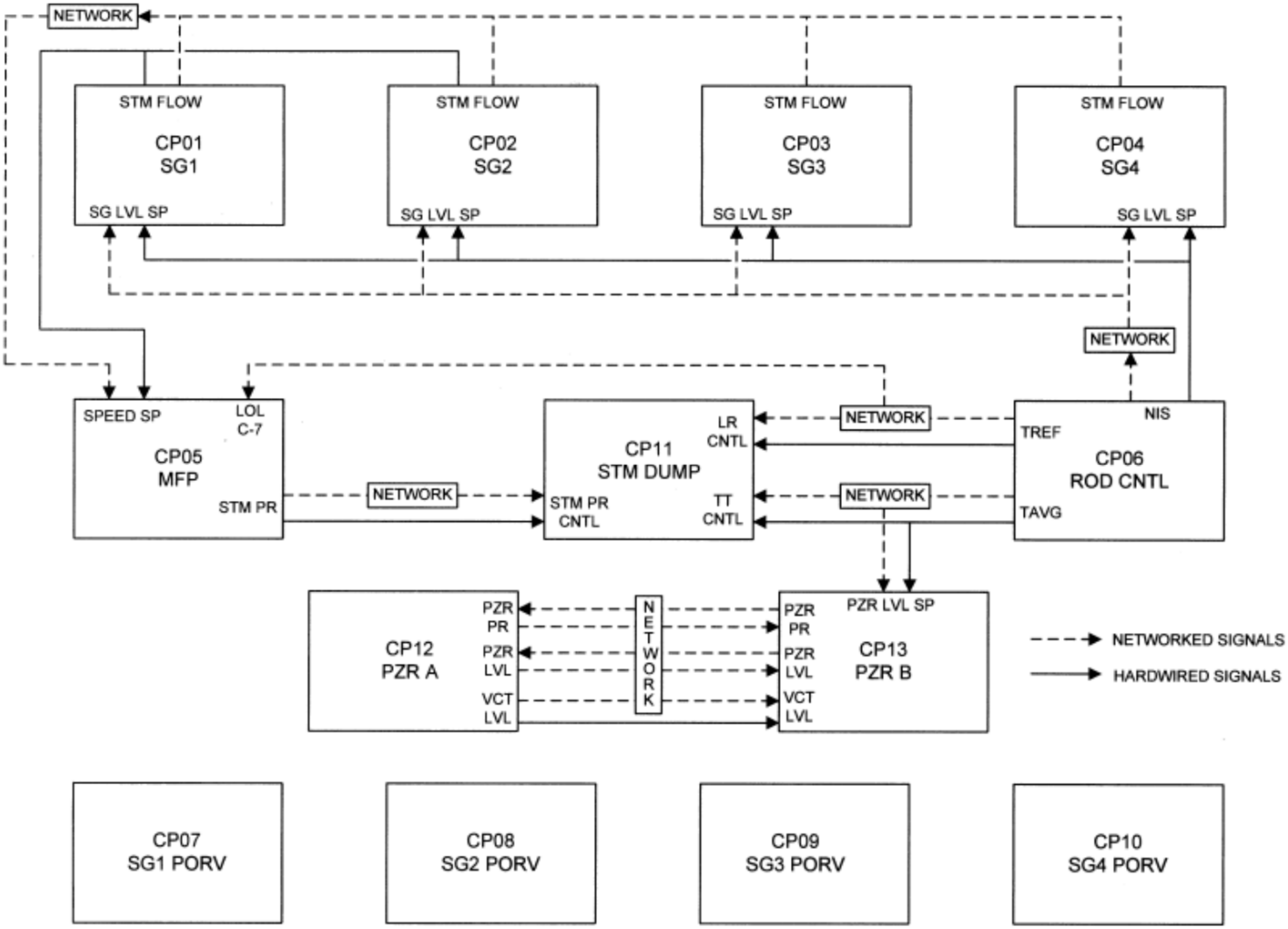

FIGURE 2: SHARED NETWORK

ENCLOSURE 2
LIST OF COMMITMENTS

1. TVA will provide the results of the data storm test after completion of the test which is currently scheduled for August 5, 2015.