December 20, 2005

TO: Allen G. Howe, Chief
Instrumentation and Controls Branch
Division of Engineering

FROM: Paul J. Loeser **/RA/**
Michael E. Waterman **/RA/**
Instrumentation and Controls Branch

SUBJECT: TRIP REPORT FOR STAFF VISIT TO FRAMATOME ANP OFFICES IN ALPHARETTA, GA, NOVEMBER 14-18, 2005 TO REVIEW THE RPS/ESPS DIGITAL UPGRADE FOR OCONEE NUCLEAR STATION (TACs MC5895/5896/5897)

NRC Staff from the Instrumentation and Controls Branch, Division of Engineering, visited the Framatome (FANP) offices in Alpharetta, GA, November 14-18, 2005. The purpose of the visit was to review development of a digital reactor protection system (RPS) and Engineered Safety Features Actuation System (ESFAS) proposed by Duke Energy Corporation (the licensee) for installation in Oconee Nuclear Station, Unit 1 (ONS-1). The staff addressed system aspects and software development activities. Table 1 summarizes the review topics addressed by the staff. Table 2 lists the materials reviewed by the staff during the visit to facilitate staff understanding of the TXS safety system development process and the design of the RPS and ESFAS safety system. The following discussion summarizes the staff's activities and preliminary conclusions.

I. Software Review Activities

The staff reviewed current revisions of the software requirements specification (SRS) and the software design description (SDD), and the interrelationship between the SRS, SDD, and the requirements traceability matrix (RTM).

The staff reviewed the SRS. Some requirements data were located in other documents; for example, accuracy requirements were stated in the SDD and the Functional Requirements Specification (FRS); however, the location of this data was consistent, and therefore, appropriately documented. The licensee stated that parameter values specific to ONS-1 will be incorporated into the RPS/ESFAS after the licensee completes a setpoint analysis for the system. Until then, the parameter values used in the system will be generic values not representative of a particular plant.

The staff reviewed task descriptions and text in the draft SDD and found the SDD to be organized consistent with the TXS process for transcribing design details into TXS components. The SDD will be rebaselined in December or January. The staff will conduct more detailed reviews of the SDD products after the design is baselined. A thorough knowledge of the TXS system development process is required to derive all the information from the SDD. Hardware

issues such as timing analyses are located in other documentation, such as outputs from the SPACE tool on CPU loading.

The RTM appears to be at least one revision behind the SRS and SDD revisions. This may be due to the process by which the SRS and SDD are integrated into the requirements traceability system. The SRS and SDD are updated such that the specific requirements and associated design element identifiers are integrated into the text of the SRS and SDD. This integration process, consequently, lags the issue date of the revised documents. A baseline of the requirements and design is expected to be created in either December or January. A more detailed reviewed of specific requirements will be performed after the baseline is generated.

The staff reviewed the draft V&V plan with the understanding that a final plan would be reviewed in the future. A revision of the ONS-1 RPS/ESFAS V&V Plan is being prepared by FANP. The staff worked with the FANP staff member responsible for V&V on this project to understand the process by which V&V is performed by the FANP system development team. The staff also reviewed sample V&V documentation and V&V problem reports in various states of implementation and review to evaluate the consistency by which V&V activities are followed and documented.

The V&V person assigned to this project appears to have a sufficient degree of technical independence - the degree of independence will be further verified in a subsequent review. The adequacy of the V&V process will be verified in subsequent staff reviews. A potential issue may be the staffing level for the V&V process, in that it appears that only one person is responsible for reviewing all development products. This may impact the timeliness of V&V feedback relative to system development activities. The vendor indicated that there may be two more staff positions planned for this activity, although the timetable for the increased staffing is not known.

The staff reviewed the use of the SIVAT validation tool and process. FANP demonstrated the SIVAT process and provided samples of SIVAT tests and outputs. Dr. Stefan Richter of FANP also provided additional information on the use of SIVAT for system validation both during the development process and during site acceptance testing. The staff will further review the use of the SIVAT tool capabilities and SIVAT products in a subsequent review.

The staff reviewed configuration management processes. The software is maintained in a configuration management library. Since the development process has not been completed, a future review will devote more resources to this aspect of the software quality assurance process. The staff reviewed a small sample of configuration management documentation and confirmed that system development documentation has been maintained under configuration management control.

III. Hardware Review Activities

The staff reviewed cabinet drawings, traced wiring through the drawings and documentation, and will continue this part of the review using cabinet 5 and cabinet 6 design drawings.

Additionally, the staff discussed several topics with Dr. Richter. These discussions addressed:

a. Dual port memory configuration
b. Interchannel communications
c. Communications within the safety system and between the safety system, the service unit, and the gateway.
d. Use of the service unit during normal operations, parameterization, testing, etc.
e. Security issues regarding system access through the service unit. The use of a portable notebook for system operations will be reviewed. The security of the notebook will be discussed in a future review.

The discussions clarified issues regarding system security features and safety issues concerning separation and independence between channels.

IV. Schedule Considerations

FANP intends to provide a baseline of the RPS/ESFAS design by January 5, 2005. Additionally, FANP will provide a change list to preclude the review of all products after the baseline is competed and during subsequent development efforts. Some discussions between FANP, the licensee, and the staff may be needed to determine what constitutes significant changes requiring additional review.

V. Outstanding Issues

a. The staff, FANP, and the licensee discussed the use of interchannel communications in the proposed RPS/ESFAS design. The licensee may seek relief from existing regulatory requirements and determine whether a TS change would be required to address specific actions to take when signal in one or more channels are faulted or fail.

b. The staff, FANP, and the licensee discussed the use of TXS service unit and whether the service unit should be disconnected all the time, isolated, or be configured as proposed. This issue will require further staff review.

c. The staff, FANP, and the licensee discussed combining RPS and ESFAS functions together as a single software program. This issue has been discussed at length for several meetings without resolution. Since this combination of systems has not been seen in past systems, the staff is dealing with the safety concerns and regulatory precedence in line with approving this design. Regarding the combination of RPS and ESFAS functions, the complexity of the system is such that the interaction of the systems must be thoroughly reviewed to arrive at a level of assurance that this architecture is safe. Additionally, the review and safety evaluation report must be structured such that every other similar application combining systems on the same processor are reviewed to the same level of detail. The implications of a combined system versus a separate system must be understood. The licensee asked whether there was some process by which the staff and the licensee could work together to resolve

this issue. The staff and technical reviewers will continue to work toward a resolution of this issue, however, at this point there is no assurance on whether or not the design will be acceptable.

d. The licensee is not sure how the defense-in-depth and diversity (D3) issue factors into the design review. The D3 analysis provided by the licensee addresses uncertainty. The licensee inquired whether the D3 analysis could be used to justify the common processor approach.

e. Given the proposed architecture of the RPS/ESFAS, and assuming the architecture could be approved, the staff may be required to perform an exhaustive review of each unique requirement in the proposed system to reach a sufficient level of assurance that the system is safe. Unique requirements are those requirements that are restated for each channel, such that confirming a requirement has been implemented appropriately in one channel, the staff can conclude the requirement is implemented safely in each channel. In the future the staff should require that digital systems be completed with sufficient lead time to allow more complete review, such as that performed using coverage testing (e.g., fault injection testing). SIVAT may be an appropriate tool for performing this testing, although this has not been confirmed yet.

f. A resolution to the issue regarding isolation of the safety system from non-safety systems using a port tap has been proposed. The staff requires further information regarding details on the communication isolation port tap proposed for this system.

g. The licensee stated that reactor trip functions proposed for future implementation will be removed from the trip system logic until the trip functions have been approved by the NRC for all three ONS units.

h. The licensee will provide details regarding the ESF Override function at a later date.

i. Lead/lag algorithms in the trip logic for future digital signal processing to remove noise may be acceptable; however control of the lead/lag parameter values must be implemented as part of the licensing basis of the plant.

j. The trip reset issue is resolved provided the trip reset only affects the trip logic portion of the safety system. That is, no safety components actuated by the RPS/ESFAS trip logic are to be affected by the reset action.

VI. Summary

The staff found that FANP and the licensee have not completed development of the ONS-1 RPS/ESFAS. Consequently, subsequent reviews of the system development products will be required before the staff can conclude with reasonable assurance that the RPS/ESFAS has been developed with an appropriate level of quality and safety. From its limited review, the staff did not identify any issues with the software development. The staff notes that many of the processes are in draft form or under revision. Therefore additional review will be needed to evaluate the software development process. Outstanding issues regarding interchannel communications, independence of RPS and ESFAS functions, and isolation of the safety systems from non-safety systems must still be resolved.

VI. Summary

The staff found that FANP and the licensee have not completed development of the ONS-1 RPS/ESFAS. Consequently, subsequent reviews of the system development products will be required before the staff can conclude with reasonable assurance that the RPS/ESFAS has been developed with an appropriate level of quality and safety. From its limited review, the staff did not identify any issues with the software development. The staff notes that many of the processes are in draft form or under revision. Therefore additional review will be needed to evaluate the software development process. Outstanding issues regarding interchannel communications, independence of RPS and ESFAS functions, and isolation of the safety systems from non-safety systems must still be resolved.

DISTRIBUTION:

MMayfield LOlshan EMarinos

ADAMS/ACCESSION NO.: ML053540359

OFFICE	NRR:DE:EICB	NRR:DE:EICB	SECY:DE:EICB	BC:DE:EICB
NAME	MWaterman	PLoeser	KSteven	AHowe
DATE	12/19/05	12/19/05	12/20/05	12/19/05

OFFICIAL RECORD COPY

Table 1. RPS/ESFAS Review Topics

System Review	
System Issues	Schematics, drawing and wiring diagrams Data Flow Signal flow Reset functions New Trip Functions
V&V activities	Documentation review Operating system modifications Tool usage
Isolation issues	TXS to plant computer via gateway TXS to service unit interchannel connections dual port RAM
Configuration Control	Documentation review Operating system modifications Duke/Oconee interactions Naming conventions
Software Review	
Requirements	Software Requirements Specification Requirements Safety Analysis V&V Requirements Analysis Report CM Requirements Report
Design	Hardware & Software Architecture Design Specification Design Safety Analysis V&V Design Analysis Report CM Design Report
Implementation	Code Listings Code Safety Analysis V&V Implementation Analysis and Test Report CM Implementation Report
Validation	Validation Safety Analysis V&V Validation Analysis and Test Report CM Validation Report

ATTACHMENT

Table 2. Information Reviewed During the Audit

Document Title	Doc. No.	Abstract
ONS Unit 1 - RPS & ESFAS System Functional Description, Rev 2.	OSC-8623 11/02/05	The purpose of this document is to provide a high-level description of the RPS and ESFAS inputs, functions, algorithms, and outputs.
Clarification of Accuracy Specification for TELEPERM XS Modules SAA1, SNV1, and S466	51-9004194-000	This report provides clarification of the accuracy and uncertainty specifications for the TXS SAA1 analog signal module, the SNV1 standard signal multiplier, and the S466 analog input module as provided in the user manual associated with each module. This report also correlates the various error terms specified for each module to the uncertainty terms described in ISA RP67.04.02-2000, “Recommend Practice - Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation.”
Software Requirements Specification, ONS-1 RPS/ESF Software Requirements Specification (QA1)	51-5045380-00	This document provides the software requirements for the new Reactor Protection System (RPS), Engineered Safety Feature Actuation System (ESFAS), related Monitoring & Service Interface (MSI) computer, and TXS Gateway replacement and upgrade for the Oconee Nuclear Station.
Software Requirements Specification, ONS-1 RPS/ESF Software Requirements Specification (QA1)	51-5045380-02	This document provides the software requirements for the new Reactor Protection System (RPS), Engineered Safety Feature Actuation System (ESFAS), related Monitoring & Service Interface (MSI) computer, and TXS Gateway replacement and upgrade for the Oconee Nuclear Station.

ONS-1, 2, &3 RPS/ESF Controls Upgrade, Design Specification for Key Locks and Key Switches	51-5045379-00	This document specifies the design requirements for the cabinet-internal key locks and key switches for the Plant Protection System. For each of the key switches, the function, the implementation and the requirements concerning the key lock are described.
Oconee Nuclear Station, Units 1, 2, & 3 RPS/ESF Controls Upgrade ID Coding Concept	51-5058134-02	The ONS RPS/ESF ID coding provides a standardized method of naming equipment, diagrams and signals for the purpose of continuity in identification during the project development process. The overall system architecture of the project is described in /2/ and /3/. This document defines the rules for the assignment of ID codes to: • I&C equipment • I&C diagrams • I&C signals This document forms an essential design input for "Software Requirement Specification" document.
Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Software Requirements Review Report	51-5066516-01	This document provides information about the conduct and results of the Software Requirements Review for the Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade project. The review was performed to verify that the functional requirements of the customer's source documents and the project proposal document are correctly implemented into the application software requirements document of the TELEPERM XS (TXS) control system.

Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Software Design Description	51-5065423-01	The SDD describes the structure of the RPS/ESPS system and translates the SRS requirements into a description of the software structure, software components, interfaces, and data necessary for the implementation phase. The SDD format is structured to support implementation of the SRS requirements in the SPACE system.
SIVAT LSELS Specifications, Job 4310002, Outputs: EFHV0037	Test Case L010400A	
SPACE Diagram - SSPS SIS A, Callaway Plant	USA143, SISK0600A12	
SIVAT-TXS Simulation Based Validation Tool, Version 1.4.0	TXS-1047-76-V2.0/01.04	
TELEPERM XS Product Information 2005/26		New Release 3.0.7A of the TXS Software under LINUX
Single Item Notice, Open Item O1.0423, 11/14/2005, VV Tracking Number D-39		
Single Item Notice, Open Item O1.0214, 8/2/2005, VV Tracking Number B-35		
Oconee Unit 1: RPS and ESFAS Replacement Project Open Item Form, “HW Typicals for CRD UV Test Jacks,” Doc Step 3.12	51-5052833-01	
Oconee Unit 1: RPS and ESFAS Replacement Project Open Item Form, “Method to Test CRD Breaker - Under Voltage UV,” Doc Step 13.2.2	32-5061401-01 (FRS)	
Oconee Unit 1: RPS and ESFAS Replacement Project Open Item Form, “HDS Typical R05 - Missing Information,” Doc Step 3.7	HDS 51-5052833-01	

Oconee Unit 1: RPS and ESFAS Replacement Project Open Item Form, “ESF actuation IEEE 603 clarification,” Doc Step General - attached 3.15.16.7 for example	15-5045380-01 (SRS)	
E-mail from Peter J. Berry to Paul Mangano, et al., “ONS Review Comments,” with attachments, “SSP KDW Comments.pdf; 51-5058452-001 MHM Comments Software Safe Plan.pdf”	dated 10/24/2005, 2:29 PM	
ONS 1, 2, & 3 RPS/ESF Controls Upgrade Hardware Design Solutions	51-5052833-01	
ONS 1, 2, & 3 RPS/ESF Controls Upgrade, Design Specification for Key Locks and Key Switches	51-5045379-00	
Oconee Nuclear Station TXS RPS/ESPS Replacement System Cabinet Design: 1PPSCA0006	38-5069822-00	
Oconee Nuclear Station TXS RPS/ESPS Replacement System Cabinet Design: 1PPSCA0005	38-5069821-00	
ONS-1 RPS/ESFAS Software Design Description, Engineering Information Record, Draft	51-5065423-01 (92 pages)	
Duke power Company, Oconee Nuclear Station, “Nuclear Instrumentation RPS Removal from and Return to Service for Channels A, B, C and D, Rev. 031, ETQS No. RPS-Q-ENTRY”	Procedure No. IP/0/A/0305/015, Rev. 031	
Engineered Safeguards Features Actuation System (ESFAS) Replacement Project Specification	OSS-0311.00-00-0012, Rev. 2, July 13, 2005	This Specification covers procurement of a replacement Engineered Safety Features Actuation System (ESFAS) for each of the three Oconee Nuclear Units and for the Operator Training Simulator.
Oconee 1 RPS&ESFAS Requirements Traceability Matrix	11/14/2005	

Paper by Dr. Richter and J-U Wittig, “Verification and Validation Process for Safety I&C Systems”		
Slide Presentation, “Digital Safety I&C TELEPERM XS for NPPs”		
Slide Presentation, “Simulation Software SIVAT”		
Slide Presentation, “TELEPERM XS Communication”		
Slide Presentation, “Communication with MicroNET”		
Slide Presentation, “Profibus FDL”		
Slide Presentation, “TELEPERM XS Service Unit”		
Slide Presentation, “TELEPERM XS Software Architecture and Operation Principles for Safe and Reliable I&C System Behavior”		
FANP Report, “TELEPERM XS Simulation - Concept of Validation and Verification,”	NGLP/2004/en/0094	