REQUEST FOR ADDITIONAL INFORMATION
ON OCONEE UNITS 1,2, AND 3 LICENSE AMENDMENT REQUEST
REACTOR PROTECTIVE SYSTEM /ENGINEERED SAFEGUARDS PROTECTION SYSTEM
DIGITAL UPGRADE

1. Please provide the following documentation:

A. Design requirements and design basis for the RPS/ESPS TXS system as it will be installed at Oconee. This should include a detailed system description with system architecture and system specification for the planned TXS and any subsystems

B. Procurement Specification. If this does not include specific hardware and software specifications, please provide them.

C. Oconee Software Management plan

D. Oconee Software Quality Assurance Plan and any procedures specific to this system.

E. Oconee Configuration Management Manual, including the Software Configuration Management Plan

F. The Oconee Safety analyses

G. Oconee Nuclear Station, Unit 3 RPS/ESF Controls Upgrade, Software V&V Plan, Document 51-5024087-00.

H. Oconee Software Development plan and related life-cycle documentation, if any applications software is being developed by the licensee. If applications software is being developed by the Framatome, please provide the following software life-cycle documents in accordance with Section 5.1.2 of EMF-2110

i. Requirements Definition
ii. Technical Design Specification.
iii. Detailed Design Specification.
iv. Implementation Specification.
v. Integration Plan.
vi. Test Plan

I. The documentation and plans which the licensee will determine that the RPS/ESPS system software meets the requirements. This would normally include:

i. Software Design Review.
ii. Source Code Review
iii. Software Verification and Validation Plan
iv. Verification and Validation Report

J. Factory Acceptance Test (FAT) and the ONS Site Acceptance Test (SAT), and any other test documentation which will be used.

K. Oconee User Instruction Manual and an explanation of what training will be provided to control room operators, I&C maintenance personnel and plant engineering.

L. The RPS/ESPS specification compliance matrix.

M. The updated ONS UFSAR Chapter 15, Accident Analyses. This analysis should include an accident analysis which assumes that a common mode software failure renders unavailable all safety-related functions which are performed by the Teleperm XS RPS/ESPS system. If manual actions is credited, show what indications the operators would have which are not dependant on the Teleperm XS RPS/ESPS system.

N. The Human Factors Review.

O. The Failure Modes and Effects Analysis (FMEA), including not only significant failure modes but all failure modes.

P. Siemens (FANP) Report, 66-5015893, "TXS Supplemental Equipment Qualification, Summary Test Report" and TÜV test report, 968/K 109.00/02 dated September 13, 2002.

Q. The RPS/ESPS System Instrument Setpoint Calculations and Instrument Accuracy Uncertainty Calculations. If the Oconee setpoint methodology is derived from ISA 67.4, please state which methodology is used. Has the setpoint methodology been reviewed and approved by NRC? If so, please provide the appropriate reference documents.

R. The output from the RETRANS tool, and the analysis comparing this output to the design data base.

2. List All functions currently performed by the existing RPS and ESPS. Indicate which of these functions will now be performed by the TXS.

3. List all hardware modules and software components which will be used in the Teleperm XS RPS/ESPS system, including the revision level. Are any of these revision levels of either hardware and software different from those previously reviewed and approved by NRC?

4. The submittal identified several differences between the TXS system approved by the NRC and the system proposed for installation at Oconee, principally the SVE CPU module and the communications modules. Please provide the following information:

A. Exact description of the changes, including changes to support chip sets, printed circuit board artwork, and software changes. Software change descriptions should include changes to the basic input/output system (BIOS) for the different processor.

B. The environmental test data which verified the new equipment qualifications, including temperature, humidity, radiation, seismic, and electromagnetic qualifications.

C. Test data showing that the existing software did not require modification, or if modifications were required, a description of those software changes and how the changes were tested.

D. Page 3-48 of EMF-2110 states that a ISTec/TÜV-Nord issued a certificate for the CP486. Has a similar certificate been issued for the new SVE CPU? If so, please provide that certificate.

5. List the online continuous self-testing and diagnostic functions. Do these differ or add to the diagnostic functions reviewed in the original TXS SER?

6. Section 4.9 of topical report EMF-2110 states “Signal transmission between redundant class 1E channels may be required for availability or reliability reasons. If required it will be performed by serial fiber optic Profibusses in an end to end configuration.” Since the February 14, 2005, submittal states that the TXS sets exchange their process data via point-to-point fiber-optic data links and that by comparison (Data Validation) between the redundant values, outlying signals are rejected and the optimum representative signal is selected, it would appear that this feature used in the Oconee RPS/ESFS application. How is the requirement for channel independence maintained? Please describe in detail all communications and data exchange between channels.

7. The February 14, 2005, submittal states that “the new RPS system will enhance the RPS/Operator Aid Computer (OAC) interface. The TELEPERM-OAC gateway will make additional information available to the OAC on RPS process variables and equipment status.” Please provide details on this enhancement, listing what additional information will be available, and all software and hardware changes to the TXS system required for these changes. In addition, please show how isolation is maintained. Please describe in detail all communications and data exchange between the safety-related RPS/ESPS TXS system and any non-safety system. How does this meet the Standard Review Plan section 7.9 requirement that the communications systems “does not present an electronic path by which unauthorized personnel can change plant software or display erroneous plant status information to the operators” and “Such connections should be one-way communication paths.”

8. Please explain how the use of dual port RAM as a interface maintain the requirement for independence? Is the safety side input port write only, or the non-safety output port read only? How does this prevent cyber intrusion and maintain security of the system.

9. The February 14, 2005, submittal states, in section K, that “The digital upgrade of the RPS and ESPS will not have a significant impact on the Oconee PRA results.” Please provide information on how this determination was reached, including the data used to make this determination. This should be justified keeping in mind that a single hardware failure will disable one channel of all RPS and ESPS functions in which the TXS is used, and one common mode failure could eliminate all RPS and ESPS functions in which the TXS is used.

10. The February 14, 2005 submittal, in section K, refers to “The expected high reliability of the digital actuation systems.” What is the value of this expected high reliability, and how was it determined? How was software reliability calculated, and how was this software reliability included in the expected high reliability value?

11. In the safety evaluation for EPRI TR-102323, the NRC staff concluded that “TR-102323 provide an acceptable method for assessing the qualification of digital equipment to the nuclear plant EM environment without the need for plant specific EMI surveys if the plant specific EM environment is confirmed to be similar to that identified in TR-102323". Please show how it was determined that the EM environment at Oconee was similar to that identified in TR-102323.

12. The February 14, 2005, submittal states that TXS equipment qualification criteria bound the plant specific qualification levels for the applicable locations at ONS. Please provide the worst case plant specific accident environmental conditions for the locations where the TXS equipment will be located.

13. The February 14, 2005, submittal, in response to plant specific requirement 9, stated that "The Oconee AMSAC and DSS systems' attributes have been evaluated for diversity between them and the TXS based RPS/ESPS for the categories of Design Diversity, Human Diversity, Equipment Diversity, Software Diversity, Functional Diversity, and Signal Diversity." Please provide that analysis.

14. The submittal, in response to plant specific requirement 12, stated that a plant specific risk informed D-in-D&D assessment to justify eliminating the need to install the diverse LPI actuation in early 2005. Please provide that assessment, keeping in mind that NRC has neither reviewed or approved the EPRI report 1002835, "Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital Upgrades."

15. The submittal, in response to plant specific requirement 14, stated: "The power supplies will be commercially dedicated and qualified by Framatome ANP for this ONS safety related, Quality Condition 1 application". Please provide the test plans, procedures and reports.

16. The submittal, in response to plant specific requirement 14, stated: "The TXS communication from the safety I&C system to the non-safety plant information system is done via the Monitoring and Service Interface (MSI)". Please describe this communications link, and the manner is which it maintains isolation? Is this a communications path a broadcast type one-way communication path used without handshaking or acknowledgment signals? If the communications is not a broadcast, please explain the cyber security provisions used by the Teleperm XS RPS/ESPS system.

17. How is access control for the TXS cabinets maintained? Who controls the keys? Please provide a proposed access list, or the access list for physical access to the existing cabinets.

18. Please discuss the response time requirements for the RPS and ESPS functions. What is the expected worst case response time for the Teleperm XS systems as it will be installed at Oconee, and how will that response time be tested? This should include a discussion of the microprocessor cycle times, sampling rates, and testing procedures.

19. What provisions for repair parts has been made? How many spare boards and modules will be delivered with the system? For what period of time has Framatome guaranteed that additional parts of the same revision level as the original be available? If parts are received with a different revision level, how will they be evaluated, and under what conditions will NRC approval be required?

20. Please show how and where the software under configuration management is stored, and who is the software librarian is.

21. Please discuss what provisions have been made for the repair and maintenance of components, PC boards and software.

22. Who will modify software if errors are discovered? How will those modifications be tested, both by the organization making the changes and by the licensee?

23. Will all documentation, training manuals, software listings, screen data and error massages be in English? Where is the application specific software being developed and tested?

24. In attachment 3, figure 1, there are two cabinets labeled "Status (Cab 8)" and "Status (Cab

9)". Please describe the functions performed by each. What hardware and software will be used in these functions, and how will each be qualified?

25. In the same figure 1, the fifth bullet states "One RPS computer ("RPS-E") providing information to the control board and the Integrated Control System (ICS) and implementing the functions of the TXS Monitoring and Service Interface (MSI)." Please describe RPS-E fully, including function, hardware, software, interconnects, and qualification.

26. In figure 2 there is an input described as "RPS Input Channel E". Please state where this input is from, and what function it performs.

27. Please show how the Teleperm XS RPS/ESPS system as installed at Oconee will comply with the following sections of IEEE Std. 603-1991 (as required by 10 CFR 50.55a). If this information is already contained in sufficient detail in the February 14, 2005 submittal, please reference the section of the submittal where the information is discussed.

Section 4.1	identification of the design basis events
Section 4.4	identification of variables monitored
Section 4.5	minimum criteria for manual initiation and control of protective actions
Section 4.6	identification of the minimum number and location of sensors
Section 4.4	identification of the analytical limit associated with each variable.
Section 4.7	range of transient and steady-state conditions
Section 4.8	identification of conditions having the potential for causing functional degradation of safety system performance
Section 4.9	identification of the methods used to determine reliability of the safety system design
Section 5.1	Single-Failure Criterion
Section 5.2	Completion of Protective Action
Section 5.3	Quality
Section 5.4	Equipment Qualification
Section 5.5	System Integrity
Section 5.6	Independence • Physical independence. • Electrical independence. • Communications independence.
Section 5.7	Capability for Test and Calibration
Section 5.8	Information Displays
Section 5.9	Control of Access
Section 5.10	Repair
Section 5.11	Identification
Section 5.12	Auxiliary Features
Section 5.13	Multi-Unit Stations
Section 5.14	Human Factors Considerations
Section 5.15	Reliability
Sections 6.1 and 7.1	Automatic Control
Sections 6.2 and 7.2	Manual Control
Section 6.3	Interaction Between the Sense and Command Features and Other Systems
Section 7.3	Completion of Protective Action
Section 6.4	Derivation of System Inputs
Section 6.5	Capability for Testing and Calibration

Sections 6.6 and 7.4	Operating Bypasses
Sections 6.7 and 7.5	Maintenance Bypass
Section 6.8	Setpoints
Section 8	Power Source Requirements