MEETING WITH WOLF CREEK NUCLEAR OPERATING CORPORATION (LICENSEE)

RELATED TO WOLF CREEK GENERATING STATION

MAIN STEAM AND FEEDWATER ISOLATION SYSTEM (MSFIS) REPLACEMENT PROJECT

MEETING HELD AUGUST 2, 2007

DOCKET NO. 50-482

The MSFIS replacement project was submitted in the licensee's application dated March 14, 2007, as supplemented by letters dated April 18, May 9, and June 15, 2007. These documents are in the NRC Agencywide Documents Access and Management System (ADAMS) at ADAMS Accession Nos. ML070800193, ML071160332, ML071350247, and ML071770446)

Attached is the six-page handout from the NRC staff at the meeting:

1. Agenda from meeting notice issued July 18, 2007 for the meeting (ADAMS Accession No. ML071790007).

2. Four pages containing five questions to be addressed in the meeting that were sent to the licensee in an email dated July 25, 2007.

3. The one-page list of items still needed by the NRC staff for its review of the Wolf Creek MSFIS replacement project, which is using field programmable gate array (FPGA) components.

AGENDA

MEETING WITH WOLF CREEK NUCLEAR OPERATING CORPORATION

MODIFICATION OF MAIN STEAM AND FEEDWATER ISOLATION SYSTEM

LICENSE AMENDMENT REQUEST

AUGUST 2, 2007

- Introductions
- NRC Staff Presentation

  This addresses the NRC staff's acceptance review of the licensee's application dated March 14, 2007, as supplemented by letters dated April 18 and June 15, 2007 (Agencywide Documents Access and Management System Accession Nos. ML070800193, ML071160332, and ML071770446, respectively). The presentation will include the expected time for the NRC staff to complete its review and any additional information needed by the NRC staff to complete its review.

- Licensee Presentation

  The licensee will provide additional information regarding the complexity of the proposed modification and its actions needed to support the NRC review schedule, as necessary, including the schedule to provide the additional information. The licensee will address NRC staff's questions regarding the proposed modification and information provided in the submittals.

- Comments, Questions, and Discussion
- End of Meeting
- **Public Comments**

MAJOR PROBLEMS IDENTIFIED IN

THE MSFIS MODIFICATION LAR SUBMITTED 03/14/07 FOR WCGS

TO BE ADDRESSED BY THE LICENSEE IN THE AUGUST 2, 2007, MEETING

The following information needed from the licensee is based on the NRC staff's review of the licensee's letter dated March 14, 2007, and the supplemental letters dated April 18, May 9, and June 15, 2007, on the proposed main steam and feedwater isolation system (MSFIS) modification at Wolf Creek Generating Station (WCGS):

1. Nutherm International, the commercial grade dedication contractor, chose to use Electric Power Research Institute (EPRI) NP-5652, "Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications," as their guidelines, rather than EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications" or EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants." As a result, the dedication was by test and inspection only, and no evaluation of the quality of the design effort was made. The commercial dedication process will need to be redone, with an emphases on high quality design and lifecycle process is required in addition to the verification and validation (V&V) and test already done. The following documentation needs to be revised:

    a. MSFIS Controls Replacement Project Plan, Revision 1
    b. Nutherm International Dedication Plan WCN-9715DP, Revision 1
    c. Nutherm International Quality Assurance Plan (WCN-9175QAP), Revision 0
    d. Nutherm International dedication procedures and reports.

    Based on the above statements in the licensee's submittals, the commercial-grade dedication of the MSFIS modification project is to be done only by testing and inspection. The licensee has not provided its evaluation of the quality of the design life cycle effort for the project. The NRC position is that the licensee needs to provide this evaluation, as well as extensive validation and verification, and testing, for the NRC staff to complete its review of the application. When will this evaluation be provided to NRC?

2. The license does not appear to be planning any diversity or defense-in-depth (D3) analysis for the MSFIS modification. The license provided a document titled "Diversity and Defense-in-Depth Assessment for the Replacement MSFIS Controls" as Enclosure 41 to its June 15, 2007, letter. The conclusion of this document is that no diversity or defense-in-depth is needed since "employment of the DO-254 design guidelines by CS Innovations has resulted in a high quality design," and "the replacement MSFIS system performs at an equivalent level and in several cases provides improved performance resulting in the replacement MSFIS providing increased reliability over the existing MSFIS controls." A new diversity and defense-in-depth analysis will be required, where for each anticipated operational occurrence or postulated accident in the design basis occurring in conjunction with each single postulated common-cause failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in unacceptable consequences. The

license will need to demonstrate that sufficient diversity exists to achieve these goals, or to identify the vulnerabilities discovered and show that the corrective actions were taken, including adding a diverse system if necessary.

As discussed in the previous paragraph, the licensee does not appear to be planning any D3 analysis for the MSFIS modification. The NRC position is that the licensee needs to provide the D3 analysis for the NRC staff to complete its review of the application. When will a D3 analysis be provided to NRC?

3. Use of software tools is not considered. The NRC staff review of the submittals has found no requirement that software tools be qualified or put under configuration control. Institute of Electrical and Electronic Engineers (IEEE) standard 7-4.3.2 defines software tools in section 3.1.42: "A computer program used in the development, testing, analysis, or maintenance of a program or its documentation. Examples include comparator, cross-reference generator, decompiler, driver, editor, flowcharter, monitor, test case generator, and timing analyzer." Section 5.3.2, "Software tools," requires that "Software tools used to support software development processes and verification and validation (V&V) processes shall be controlled under configuration management," and "A test tool validation program shall be developed to provide confidence that the necessary features of the software tool function as required." There are similar requirements in RTCA DO-254/EUROCAE ED-80, "Design Assurance Guidance for Airborne Electronic Hardware." Section 11.4, "Tool Assessment and Qualification," requires that "Prior to use of a tool, a tool assessment should be performed. The results of this assessment and, if necessary, tool qualification should be recorded and maintained." The license or the vendor, CS Innovations, will need to demonstrate that the software tools were both qualified for the development of safety related systems, and that they are and will continue to be under appropriate configuration control.

   Based on the above statements, the licensee has not considered the use of software tools in the MSFIS modification. The software tools require a written assessment that these tools are qualified to perform their safety functions and are under configuration controls. The licensee has not addressed these requirements, which come the following sections of standards IEEE 7-4.3.2-2000 and DO-254 in the use of software tools: (1) Sections 3.1.42 and 5.3.2 of IEEE 7-4.3.2 and (2) Section 11.4 of DO-254. The NRC position is that the use of software controls needs to be addressed. When will the written assessment on the use of software tools be provided to NRC?

4. The standard which the licensee and the vendor chose to use to develop this system, RTCA DO-254/EUROCAE ED-80, "Design Assurance Guidance for Airborne Electronic Hardware," has not been reviewed or approved by NRC for nuclear safety related use. A comparison of the requirements between standards IEEE 7-4.3.2-2000 and DO-254 was requested and agreed to in the meeting of May 17, 2007, and provided in Enclosure 23 of the June 15, 2007, submittal. However, the comparison between the standards in Enclosure 23 is not of sufficient detail in that the comparison is only a listing by chapter or section of which DO-254 requirement goes with which IEEE 7-4.3.2-2003 requirement. Although this appears to show that DO-254 has the same requirements in IEEE 7-4.3.2-2000, this does not show that the requirements in DO-254 are equivalent to those in IEEE 7-4.3.2-2000. The NRC position is that the licensee needs to provide a more complete analysis of the requirements in the two standards for

the NRC staff to complete its review of the application. The license should provide a detailed mapping of this standard to an approved standard such as IEEE Standard 7-4.3.2, and show on a paragraph by paragraph basis what portion of RTCA DO-254/EUROCAE ED-80 has similar requirements, and why meeting that portion of RTCA DO-254/EUROCAE ED-80 will satisfy the corresponding section of the approved standard. Also, there may be sections of the approved standard which are not applicable to a FPGA design, and these should be pointed out and justified. NRC should receive the results of this task within thirty days of the formal receipt of this request, or the acceptance of the review will be retracted.

5. There appears to be a basic misunderstanding as to the nature of a field programmable gate array (FPGA)-based system. In Enclosure 7 to the licensee's June 15, 2007, letter, "Nutherm Dedication Plan for Replacement MSFIS System," the Nutherm document number WCN-9715DP, Revision 1, the statement is made that "the MSFIS system is not a digital system in the strictest definition as it is not software based,....". In Enclosure IV to the April 19, 2007, letter, "ALS [Advanced Logic System] Level-1 System Specification," Revision 1, CS Innovation document 6000-00000, states "The ALS does not utilize a microprocessor and therefore has no software component for the operation of the system. The concern for software common mode failures is eliminated by incorporating a full hardware system which only uses proven design practices and methodologies for implementation of the hardware."

The NRC staff disagrees with this position and considers the replacement MSFIS is a digital system. As is stated in IEEE Std 100-2000, "The Authoritative Dictionary of IEEE Standards Terms," the term "digital" is defined as "pertaining to quantities in the form of discrete, integral values," and a "digital device" is defined as "A device that operates on the basis of discrete numerical techniques in which the variables are represented by coded pulses or states." A FPGA system uses digital values, and is, therefore, a digital system.

Furthermore, the replacement MSFIS is a software-based system. One of the definitions of "software" in the same IEEE standard is "The programs, procedures, rules, and any associated documentation pertaining to the operation of an information processing system." The nature of an FPGA is also that the device is programed to perform its intended functions, and that programing is done using a variety of software tools. While it is true that the output of these tools is used to flash the FPGA into its intended configuration rather than being used as a program to tell a microprocessor what to do, in either case the device is subject to programing and uses software tools to achieve its design objectives, and this LAR will be reviewed on that basis.

Based on the definitions in the IEEE standards and the NRC staff's understanding of FPGA devices, it is the NRC staff position that the FPGA system proposed by the licensee is a software-based digital system, which relies on high quality software to meet its design objectives.

In the email to the licensee dated May 1, 2007, which is in Attachment 2 to the summary issued June 4, 2007, for the meeting held with the licensee on May 17, 2007, the NRC staff addressed the basic misunderstanding on the part of the licensee that the FPGA system is not a software-based digital system. The licensee addressed this in its letter

of May 9, 2007, but this misunderstanding was not discussed in the meeting held on May 17, 2007. It is the NRC position that the FPGA system is a software-based digital system and needs to rely on high quality software to meet the design safety objectives in its application for the MSFIS modification at WCGS. For the NRC staff to address this in its review of the licensee's application and conclude that the FPGA system in the MSFIS meets its safety objectives, the licensee needs to explain how the "flashing of the FPGA" would be done and controlled by the licensee to the same extent that changing the software of any information-processing system would be done and controlled. See the Question 3 above. The licensee should provide its explanation why this NRC position is not correct since this misunderstanding is seen to be preventing the NRC staff from receiving the documentation it needs to do its review of the application. Acknowledgment by the license that this FPGA-based system is a software-based digital system should be submitted within thirty days of the formal receipt of this request, or the acceptance of the review will be retracted.

Items Still Needed for Review of Wolf Creek FPGA

Item	Description (date given by Wolf Creek)	Needed By
1.	A detailed mapping of RTCA DO-254/EUROCAE ED-80 to an approved standard such as IEEE Std. 7-4.3.2.	9/20/07 ~~9/4/07~~
2.	Acknowledgment by the licensee that this is a software based digital system.	9/~~7~~ 4/07
3.	A new commercial dedication based upon high quality lifecycle processes. a. MSFIS Controls Replacement Project Plan, Revision 1 b. Nutherm International Dedication Plan WCN-9715DP, Revision 1 c. Nutherm International Quality Assurance Plan (WCN-9175QAP), Revision 0 d. Nutherm International dedication procedures and reports. Wolf Creek evaluation and acceptance or the Nutherm documentation should be provided with the documentation	11/15/07
4.	A new Diversity and Defense-in-Depth Analysis.	1/14/08
5.	Demonstration of the suitability and qualification of all software tools.	10/30/07
6.	Documentation on security requirements (RG 1.152)	1/23/08
7.	Final ALS design documentation and the Nutherm evaluation and acceptance of the final design and system architecture (available on August 17, 2007).	1/23/08
8.	Final ALS Test Plans	1/23/08
9.	The documentation of the Nutherm International review of the test plan	1/23/08
10.	Wolf Creek installation and test plans	5/12/08
11.	System Build Documentation - a detailed description of the system as it will be installed at Wolf Creek.	5/12/08
12.	factory acceptance test and test results (test will be available by July 30, 2007 and results will be available by October 5, 2007).	1/14/08
13.	Site acceptance test procedure(available by September 7, 2007).	5/12/08
14.	Installation test procedures (available October 16, 2007).	5/12/08
15.	V&V Design Analysis Report (August 31, 2007), V&V Implementation Analysis & Test Report(November 16, 2007), and V&V Validation & Test Report(unknown)	3/6/08
16.	Operations Manuals, Maintenance Manuals, Training Manuals, and repair planning documentation (All available by the end of September 2007)	4/12/08

Caveat: **It is possible that some of this information has already been submitted, and it has just not been found yet. It may also be possible that, during the course of the review, additional information is needed.**