WOLF CREEK
NUCLEAR OPERATING CORPORATION

Terry J. Garrett
Vice President, Engineering

May 9, 2007
ET 07-0013

U. S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555

Reference: 1) Letter ET 07-0004, dated March 14, 2007, from T. J. Garrett, WCNOC, to USNRC

2) Letter ET 07-0008, dated April 18, 2007, from T. J. Garrett, WCNOC, to USNRC

Subject: Docket No. 50-482: Response to Request for Additional Information Relating to Replacement of the Main Steam and Feedwater Isolation System Controls

Gentlemen:

Reference 1 provided a license amendment request that proposed revisions to Technical Specification (TS) 3.3.2, "Engineered Safety Feature Actuation System (ESFAS) Instrumentation," TS 3.7.2, "Main Steam Isolation Valves (MSIVs)," and TS 3.7.3, "Main Feedwater Isolation Valves (MFIVs)." The Reference proposed changes to these specifications based on a planned modification to replace the MSIVs and associated actuators, MFIVs and associated actuators, and replacement of the Main Steam and Feedwater Isolation System (MSFIS) controls. Reference 2 provided supplemental information requested by the NRC during a teleconference call on April 3, 2007.

The NRC provided by electronic mail on May 1, 2007, a request for additional information needed for the NRC staff to begin its review of the proposed changes to the MSFIS controls. The Attachment provides responses to the five items identified by the NRC.

The supplemental information provided in the Enclosures does not impact the conclusions of the No Significant Hazards Consideration provided in Reference 1. In accordance with 10 CFR 50.91, a copy of the submittal is being provided to the designated Kansas State official.

A001

This letter contains no commitments. If you have any questions concerning this matter, please contact me at (620) 364-4084, or Mr. Kevin Moles at (620) 364-4126.

Sincerely,

Terry J. Garrett

TJG/rlt

Attachment

cc: T. A. Conley (KDHE), w/a
J. N. Donohew (NRC), w/a
V. G. Gaddy (NRC), w/a
B. S. Mallett (NRC), w/a
Senior Resident Inspector (NRC), w/a

STATE OF KANSAS)
) SS
COUNTY OF COFFEY)

Terry J. Garrett, of lawful age, being first duly sworn upon oath says that he is Vice President Engineering of Wolf Creek Nuclear Operating Corporation; that he has read the foregoing document and knows the contents thereof; that he has executed the same for and on behalf of said Corporation with full power and authority to do so; and that the facts therein stated are true and correct to the best of his knowledge, information and belief.

By _____
Terry J. Garrett
Vice President Engineering

SUBSCRIBED and sworn to before me this 9th day of May, 2007.

_____
Notary Public

NOTARY PUBLIC STATE OF KANSAS
CINDY NOVINGER
My Appt. Exp. 7/8/10

Expiration Date 7/8/10

RESPONSE TO NRC REQUEST FOR ADDITIONAL INFORMAION

The NRC provided by electronic mail on May 1, 2007, a request for additional information (italicized text) needed for the NRC staff to begin its review of the proposed changes to the Main Steam and Feedwater Isolation System (MSFIS) controls. Responses to the request for additional information are provided below.

The Wolf Creek Nuclear Operating Corporation (WCNOC) provided information in its submittals dated March 14 and April 18, 2007, on its proposed upgrade of the engineered safety feature actuation system (ESFAS) main steam and feedwater isolation system (MSFIS) using field programmable gate array (FPGA) technology.

In the submittals, there appears to be a basic misunderstanding as to the nature of a FPGA based system. In "Nutherm Dedication Plan for Replacement MSFIS System," Nutherm document number WCN-9715DP, the statement is made that "the MSFIS system is not a digital system in the strictest definition as it is not software based,....". ALS Level-1 System Specification, 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."

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 uses digital values, and is therefore a digital 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 a FPGA is also that the device is programed [programmed] *to perform its intended functions, and that programing* [programming] *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* [programming] *and uses software tools to achieve its design objectives. Therefore, the licensee would be as capable of changing the FPGA (i.e., by re-flashing the FPGA with new instructions) as it would be capable of changing any information processing system based on software by changing the software. How this "flashing the FPGA" would be done and controlled by the licensee must be explained to the same extent that changing the software of an information processing system would be done and controlled.*

Based on the definitions in the IEEE standards and the staff's understanding of FPGA devices, the staff concluded that the FPGA system proposed by the licensee is a digital system and needs to rely on high quality software to meet its design objectives.

Response:

The modification to the Main Steam and Feedwater Isolation System (MSFIS) is implemented using the Advanced Logic System (ALS). The ALS is a rack-based digital hardware system consisting of several circuit cards, which contain both analog and digital devices. In the ALS design, all of the functions have been allocated to hardware. Each circuit card in the ALS is controlled by a field programmable gate array (FPGA), there are no processors, microcontrollers, central processing unit (CPU) elements or microcode. None of the FPGAs contain any processor cores or any type of arithmetic logic unit (ALU), in fact, the design could be implemented using just logic chips such as 7400 series OR-gates, AND-gates, latches, etc. The FPGA logic design is accomplished by using a Hardware Description Language (HDL), and the basic design element is the finite state machine, which eliminates the need for any processors or application software. The particular FPGA implemented in the ALS utilizes basic unconnected logic elements which are then interconnected using flash memory programming to configure the device, similar to the wiring on a printed circuit board (PCB).

WCNOC believes that there are similarities between this type of hardware design and a programmable logic controller (PLC) or digital computer-based instrumentation and control (I&C) system. Therefore, where applicable the guidance of Regulatory Guide 1.152 "Criteria for Use of Computers in Safety Systems of Nuclear Power Generating Stations" Revision 2 and IEEE 7-4.3.2-2003 "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" has been utilized. For example, the following IEEE 7-4.3.2 guidance was utilized in developing a Verification and Validation (V&V) Plan, Configuration Management Plan, Requirements Traceability Matrix, System Reliability Analysis, Failure Modes and Effects Analysis, and electromagnetic compatibility (EMC) qualification. However, not all of the IEEE standard for software-based systems is appropriate to the ALS. This is supported by the Federal Aviation Administration guidance document RTCA DO-254/EUROCAE ED-80, "Design Assurance Guidance for Airborne Electronic Hardware," (endorsed by FAA AC 20-152), which states, in part:

> HDL design representations use coded text based techniques that are similar in appearance to those used for software representations. This similarity in appearance can mislead one to attempt to use software verification methods directly on the design representation of HDL or other equivalent hardware specification languages.

Although WCNOC has structured the V&V Plan for this modification on applicable elements of IEEE 7-4.3.2, there is no specific guidance within the IEEE standard for a hardware-only logic system based on FPGAs. RTCA DO-254/EUROCAE ED-80, "Design Assurance Guidance for Airborne Electronic Hardware" applies specifically to hardware-only logic systems based on FPGAs. It was developed because safety critical flight equipment vendors were attempting to use RTCA DO-178/EUROCAE ED-12, "Software Considerations in Airborne Systems and Equipment Certification," a software standard similar to IEEE 7-4.3.2, for these hardware systems (which are common in flight controls) and the resulting Quality Assurance requirements and procedures were inappropriate.

The FPGA is specifically configured to meet the logic requirements of the application. Once the logic design is completed and has been fully tested the FPGA is locked such that they can only be modified by an entity that maintains the necessary tools to configure the FPGA. The system is delivered to WCGS as a fixed digital hardware system. WCNOC does not maintain the

capability onsite to modify the logic design in the FPGAs. A subsequent modification to the logic of the system would require WCNOC to contract with an entity with the necessary tools to program FPGAs. Any subsequent modification to the FPGA logic design would also require a design change to the MSFIS using the WCNOC Appendix B design control process and procedures.

Software tools are used in the FPGA logic development process, as well as in the circuit design, board design, and build processes. These software tools are controlled by a configuration management process maintained by the controls vendor (CS Innovations). The software tools utilized in this modification were chosen and confirmed suitable for use by the controls vendor using the following criteria: 1) implementing V&V activities which detect possible defects in the software tools; 2) a review of operating experience of the software tools; and 3) corrective action program(s) implemented by the software tools vendor.

The ALS is a digital system as described in IEEE 100-2000, "Authoritative Dictionary of IEEE Standards Terms," as well as the existing MSFIS currently installed at WCGS is considered a digital system. The ALS is not considered to be a digital computer-based I&C system. The MSFIS controls to be delivered to WCGS are comprised of fixed hardware devices. The development of the system does utilize software tools as discussed above, however those tools are subject to V&V activities to ensure defects are not injected into the design. The FPGA software tools are utilized as tools for implementing the hardware design in the same way as the software tools are used for developing the PCB or a discrete logic design.

Upon its review of the licensee's application submittals dated March 14 and April 18, 2007, the NRC staff has determined that there are the following 5 points of deficiency in the information provided. This is information needed for the NRC staff to begin its review of the proposed MSFIS upgrade.

1. Appendix B Compliance

Section IV, on "Procurement Document Control," of Appendix B, 10 CFR Part 50, states:

> *Measures shall be established to assure that applicable regulatory requirements, design bases, and other requirements which are necessary to assure adequate quality are suitably included or referenced in the documents for procurement of material, equipment, and services, whether purchased by the applicant or by its contractors or subcontractors. To the extent necessary, procurement documents shall require contractors or subcontractors to provide a quality assurance program consistent with the pertinent provisions of this appendix.*

EPRI report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, discusses the commercial grade use of complex digital systems in section 6.4. The example given is for the dedication of programmable logic controllers, but the level of complexity and the processes required is similar. The discussion on identification and verification of critical characteristics states:

> *"In this case the commercial grade vendor survey is a central part of the dedication. The survey requires extensive interaction with the PLC vendor. Initial contact is made and*

information obtained to prepare for the survey. Then a one-week visit (typical for a relatively complex device like this one) is made to the manufacturer's site where the bulk of the survey information is collected and evaluation performed. This includes evaluation of the vendor's QA program, digital system development process, verification and validation practices, configuration management program, and problem reporting procedures. In addition, a detailed critical design review of the PLC hardware and software architecture is performed, including evaluation of real-time task processing and robustness of failure management provisions."

Based upon the information provided, EICB could not determine how the proposed FPGA's were dedicated for safety related use. Wolf Creek and their vendor, CS Innovations chose to use a highly complex FPGA, the Actel ProASICplus APA600, which has 600,000 system gates, 128K onboard memory, 21,504 registers, and an I/O capacity of 356.

The licensee has provided two documents, "Nutherm Qualification Report for CS Innovations Replacement MSFIS System," Nutherm document number WCN-9715R, and "Nutherm Dedication Plan for Replacement MSFIS System," Nutherm document number WCN-9715DP. The qualifications report discusses only the physical qualification of the FPGA, such as temperature, seismic, and EMI, but does not discuss the quality of design and fabrication of the actual FPGA. The second document, the Nutherm Dedication Plan, requires a commercial grade dedication process, but the licensee did not provide documentation of what was done. For example, there is no indication in the documentation provided that a vendor survey was conducted when selecting the Actel ProASICplus APA600 for use in this system, or that any commercial grade dedication was done. Based on the requirements in 10 CFR Appendix B and EPRI report TR-106439, the staff would have expected to see documentation of a vendor survey, with an analysis of the Actel quality control and any existing documentation of previous qualifications of the Actel ProASICplus APA600. Without this information, the staff is unable to determine if the Actel ProASICplus APA600 is a suitable device to use in this application.

Response:

WCNOC is procuring the modifications to the MSFIS controls in accordance with the appropriate commercial grade dedication processes. Nutherm International has been contracted by WCNOC as the 10 CFR 50 Appendix B supplier of the safety related MSFIS controls. Nutherm International will deliver the MSFIS controls to WCNOC as a Class 1E safety related system. CS Innovations is the commercial grade vendor responsible for the design of the ALS and subsequent MSFIS controls as a commercial grade system. Nutherm International's responsibility is to qualify the design and the system as well as dedicate the MSFIS controls delivered to WCGS. Nutherm International has reviewed design documentation and activities of CS Innovations' level of design and build quality in the initial design. During commercial grade survey activities, Nutherm International is performing several specific items including, but not limited to: 1) review of the process by which the individual system components were selected with a detailed review of the Actel FPGA; 2) review of the CS Innovations' V&V activities implemented for the design of the system as well as the V&V activities to detect possible defects in the software tools; and 3) review of CS Innovations' quality assurance and configuration management process.

2. *Acceptable Method Per Regulatory Guide 1.152*

Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems Of Nuclear Power Plants," endorses IEEE 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as a method that the staff has found acceptable for complying with the Commission's regulations for promoting high functional reliability, design quality, and cyber-security. IEEE 7-4.3.2 cites the used [use] *of verification and validation as necessary to meet quality requirements.*

The licensee, in the original submittal of March 14, 2007, provided the Wolf Creek MSFIS System Verification and Validation Plan. The licensee did not provide the V&V plans for the design contractor, CS Innovation; the qualification contractor, Nutherm; or the V&V consultant. None of the V&V plan outputs were provided. Without this information, the staff is unable to determine what V&V was actually done, whether this level of V&V is adequate, or if the V&V was done correctly.

Response:

CS Innovations is performing V&V activities during the design and development of ALS and the MSFIS controls consistent with the guidance in RTCA DO-254/EUROCAE ED-80, "Design Assurance Guidance for Airborne Electronic Hardware." Nutherm International, as the Appendix B supplier, is performing commercial grade surveys of the activities of CS innovations to verify and validate that CS Innovations is designing and developing the MSFIS controls in accordance with the plant specifications for a Class 1E safety related system. As the commercial grade surveys are still in process, the results of the V&V activities have not been finalized in the Nutherm International final dedication report. WCNOC has contracted with Baseline Engineering to provide oversight V&V activities of the entire modification as described in Enclosure IV to letter ET 07-0004 dated March 14, 2007.

3. *IEEE 7-4.3.2, section 5.3.2, Compliance*

IEEE 7-4.3.2, section 5.3.2, "Software Tools," states that a) a test tool validation program shall be developed to provide confidence that the necessary features of the software tool function as required, or that b) the software tool shall be used in a manner such that defects not detected by the software tool will be detected by V&V activities.

The licensee has provided a list of software tools used in the development of the proposed FPGA[.] The list includes:

> *FPGA design tool: Libero Integrated Design Environment Version 7.1sp2" for Windows XP platform.*
>
> *Simulation Tool: ModelSim 6.1b Actel Edition produced by Mentor Graphics*
>
> *Synthesis Tool: Synplify 8.5F Actel Edition produced by Synplicity*
>
> *Place-and-Route Tool: Actel Designer Version 7.2.3.2*

Programming (Flashing) Tool: Actel FlashPro Version 7.1.0.13 together with FlashPro LITE programming adaptor

Schematic Capture Tool: Altium Designer Version 6.6.7903

PCB Layout Tool: Altium Designer Version 6.6.7903

Gerber Analysis Tool: Altium Designer Version 6.6.7903

Analog Circuit Simulation Tool: SIMetrix Circuit Simulation Version

There is no indication in the documentation provided how the criteria contained in IEEE 7-4.3.2, section 5.3.2 were met. In addition, there is no documentation on how those software tools were dedicated for safety related use in a nuclear power plant.

Response:

The activities employed by CS Innovations that are consistent with the guidance described in IEEE 7-4.3.2, Section 5.3.2 will be discussed in Nutherm International's final dedication report. As described above, the software tools utilized by CS Innovations are used in a manner such that defects not detected by the software tools will be detected by V&V activities. In addition, Nutherm International is in the process of a commercial grade survey of the software tools vendor, which includes but is not limited to a survey of the corrective action program employed by the tools vendor as well as operating history of the tools.

4. IEEE 603-1991 Compliance

10 CFR 50.55.a(h) requires compliance with IEEE 603-1991. This standard, in section 5.3, "Quality," requires that components and modules "shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program." 10 CFR Appendix B requires a "quality assurance program to be applied to the design, fabrication, construction, and testing of the structures, systems, and components of the facility." It also states that "the applicant may delegate to others, such as contractors, agents, or consultants, the work of establishing and executing the quality assurance program, or any part thereof, but shall retain responsibility therefor."

The licensee provided the Wolf Creek "MSFIS Quality Assurance Plan" and the "MSFIS Configuration Management Plan," but these plans show how the quality assurance and configuration management will be conducted after the completed FPGA is accepted by the licensee. Neither of these documents discuss the quality assurance and configuration management methods used by the system developer, CS Innovation, during the design and implementation phases of the life cycle. Based on the information submitted, EICB could not determine if an 10 CFR 50 Appendix B quality assurance program was used during the design process, or if any quality control was used.

Response:

As discussed in the response to Question 1, Nutherm International is reviewing CS Innovations' quality assurance and configuration management processes as part of the commercial grade survey activities.

5. *Acceptable Method Per Branch Technical Position 14*

The Standard Review Plan, NUREG-0800, Chapter 7, Branch Technical Position 14 (BTP-14), "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," shows an acceptable method for the software development process to meet the quality requirements of 10 CFR 50 Appendix B. A number of documents are to be reviewed by NRC staff to meet the review criteria of BTP 14. Enclosure 1 to this memorandum lists these documents, the Wolf Creek comment or commitment, and the EICB analysis of that comment or commitment. EICB finds that a number of documents which should have been prepared at this point in the design process are not yet available. Overall, the incomplete nature of the documentation does not provide a record for review by NRC that demonstrates that CS Innovation is using a high quality design process, or that Wolf Creek has been monitoring their contractor to assure this required high quality. In addition, Wolf Creek has stated that since the FPGA is not a software based system, a number of these documents are not required. In fact, the FPGA relies on software for one-time programing [programming] *by flashing a particular pattern of links rather than repeatedly providing instructions for a microprocessor. This type of device is just as program driven as a microprocessor device, including that the FPGA chosen by Wolf Creek is re-programable* [re-programmable], *similar to the reprogramming capability of microprocessor based systems, by re-flashing the FPGA. Accordingly, the staff needs to review the process that was used to develop the FPGA flash list to evaluate the adequacy of the FPGA programing* [programming].

Response:

The ALS is not considered to be a digital computer-based I&C system. The MSFIS controls to be delivered to WCGS are comprised of fixed hardware devices. The development of the system does utilize software tools as discussed above, however those tools are subject to V&V activities to ensure defects are not injected into the design. The FPGA software tools are utilized as tools for implementing the hardware design in the same way as the software tools are used for developing the PCB or a discrete logic design.

As discussed above, the FPGA is specifically configured to meet the logic requirements of the application. Once the logic design is completed and has been fully tested the FPGA is locked such that they can only be modified by an entity that maintains the necessary tools to configure the FPGA. Section 3.6.11 in Enclosure 1 to WCNOC letter ET 07-0004, identified that the ALS boards are Flash-Locked once they are configured in the production test. The system is delivered to WCGS as a fixed digital hardware system. WCNOC does not maintain the capability onsite to modify the logic design in the FPGAs. A subsequent modification to the logic of the system would require WCNOC to contract with an entity with the necessary tools to program FPGAs. Any subsequent modification to the FPGA logic design would also require a design change to the MSFIS using the WCNOC Appendix B design control process and procedures.

Nutherm International has reviewed design documentation and activities of CS Innovations' level of design and build quality in the initial design. During commercial grade survey activities, Nutherm International is performing several specific items including, but not limited to: 1) review of the process by which the individual system components were selected with a detailed review of the Actel FPGA; 2) review of the CS Innovations' V&V activities implemented for the design of the system as well as the V&V activities to detect possible defects in the software tools; and 3) review of CS Innovations' quality assurance and configuration management process. Documentation of the above activities will be provided in the final dedication report from Nutherm International.