

WOLF CREEK

NUCLEAR OPERATING CORPORATION

Matthew W. Sunseri
Vice President Operations and Plant Manager

November 16, 2007
WO 07-0028

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, WCNOG, to USNRC
 - 2) Letter dated August 8, 2007, from J. W. Lubinski, USNRC, to R. A. Muench, WCNOG
 - 3) Letter ET 07-0039, dated August 31, 2007, from T. J. Garrett, WCNOG, to USNRC
 - 4) Letter ET 07-0041, dated September 20, 2007, from T. J. Garrett, WCNOG, to USNRC

Subject: Docket No. 50-482: Response to Request for Additional Information Relating to Replacement of the Main Steam and Feedwater Isolation Valves and 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)" based on a planned modification to replace the MSIVs and associated actuators, MFIVs and associated actuators. This modification also planned replacement of the Main Steam and Feedwater Isolation System (MSFIS) controls.

On August 2, 2007, Wolf Creek Nuclear Operating Corporation (WCNOG) personnel met with the NRC staff to discuss five issues identified by the NRC associated with the review of the MSFIS controls modification. Subsequently, the NRC issued Reference 2, in which the NRC staff accepted the MSFIS controls modification license amendment request for review. This letter identified 5 issues requiring a response from WCNOG. Reference 3 provided responses to the 5 issues. With regard to issue 1, WCNOG provided in Reference 4 a difference analysis of RTCA DO-254/EUROCAE ED-80, "Design Assurance Guidance for Airborne Electronic Hardware," to Institute of Electrical and Electronics Engineers (IEEE) Std 7-4.3.2-2003, "IEEE

A001
NORR

Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." In a teleconference between NRC staff and WCNOG personnel on September 25, 2007, WCNOG agreed to provide a draft matrix of the IEEE Std 7-4.3.2-2003 requirements as they pertain to the MSFIS controls design. The draft matrix was provided by electronic mail on October 12, 2007. Enclosure I provides the Matrix of IEEE 7-4.3.2 Requirements to MSFIS Controls Design.

Enclosure I provides the proprietary WCNOG, "Matrix of IEEE 7-4.3.2 Requirements to MSFIS Controls Design," Rev. 0. Enclosure II provides the non-proprietary WCNOG, "Matrix of IEEE 7-4.3.2 Requirements to MSFIS Controls Design," Rev. 0. As Enclosure I contains information proprietary to WCNOG, it is supported by an affidavit signed by WCNOG, the owner of the information. The affidavit sets forth the basis on which the information may be withheld from public disclosure by the Commission and addresses with specificity the considerations listed in paragraph (b)(4) of 10 CFR 2.390 of the Commission's regulations. Accordingly, it is respectfully requested that the information, which is proprietary to WCNOG, be withheld from public disclosure in accordance with 10 CFR 2.390 of the Commission's regulations. This affidavit is contained in Enclosure III.

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

This letter contains no commitments. If you have any questions concerning this matter, please contact me at (620) 364-4008, or Mr. Kevin Moles, Manager Regulatory Affairs at (620) 364-4126.

Sincerely,



Matthew W. Sunseri

MWS/rlt

- Enclosures
- I - Matrix of IEEE 7-4.3.2 Requirements to MSFIS Controls Design, Rev. 0 (Proprietary)
 - II - Matrix of IEEE 7-4.3.2 Requirements to MSFIS Controls Design, Rev. 0 (Non-Proprietary)
 - III - WCNOG Affidavit for Withholding Proprietary Information from Public Disclosure

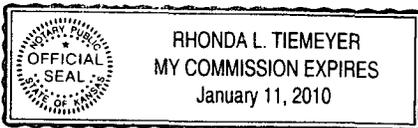
cc: E. E. Collins (NRC), w/e
T. A. Conley (KDHE), w/e (Enclosure II only)
J. N. Donohew (NRC), w/e
V. G. Gaddy (NRC), w/e
Senior Resident Inspector (NRC), w/e

STATE OF KANSAS)
) SS
COUNTY OF COFFEY)

Matthew W. Sunseri, of lawful age, being first duly sworn upon oath says that he is Vice President Operations and Plant Manager 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 MW Sunseri
Matthew W. Sunseri
Vice President Operations and Plant Manager

SUBSCRIBED and sworn to before me this 16th day of Nov., 2007.



Rhonda L. Tiemeyer
Notary Public

Expiration Date January 11, 2010

**Matrix of IEEE 7-4.3.2 Requirements to MSFIS Controls Design, Rev. 0
Non-Proprietary**

MATRIX OF IEEE 7-4.3.2 REQUIREMENTS TO MSFIS CONTROLS DESIGN

Sections 1, 2, and 3 of IEEE 7-4.3.2 are Scope, References, and Definitions and Abbreviations, respectively. They are not included in the below matrix as they are considered administrative information.

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
<p>4. Safety system design basis NOTE—See Annex A for more information about the relationship of this standard to IEEE Std 603-1998. No requirements beyond IEEE Std 603-1998 are necessary (see also Annex B).</p>	<p>4. Safety system design basis A specific basis shall be established for the design of each safety system of the nuclear power generating station. The design basis shall also be available as needed to facilitate the determination of the adequacy of the safety system, including design changes. The design basis shall be consistent with the requirements of ANSI/ANS 51.1-1983 or ANSI/ANS 52.1-1983 and shall document as a minimum: (See IEEE document for this information)</p>	<p>The main steam supply system design basis is provided in Section 10.3.1.1 of the USAR. The main feedwater system design basis is provided in Section 10.4.7 of the USAR. The main steam and feedwater isolation controls design basis is provided in Section 7.3.7 of the USAR. The design basis of the systems are not changed with the modifications to the valves and controls.</p>
<p>5. Safety system criteria The following subclauses list the safety system criteria in the order they are listed in IEEE Std 603-1998. For some criteria, there are no additional requirements beyond what is stated in IEEE Std 603-1998. For other criteria, additional requirements are described in 5.1 through 5.15.</p>		<p>None Required</p>
<p>5.1 Single-failure criterion No requirements beyond IEEE Std 603-1998 are necessary (see also Annex B).</p>	<p>5.1 Single-failure criterion The safety systems shall perform all safety functions required for a design basis event in the presence of a) Any single detectable failure within the safety systems concurrent with all identifiable but nondetectable failures. b) All failures caused by the single failure. c) All failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. The single failure could occur prior to, or at any time during, the</p>	<p>The Advanced Logic System (ALS) has been architected such that no single failure shall prevent the system from performing the safety function. CS Innovations (CSI) 6101-00006, "MSFIS Safety Assessment," provides a detailed functional failure path analysis as well as a component level failure modes and effects analysis (FMEA) to ensure the single failure criterion is met with in the ALS. Further, the System Reliability Analysis for Advance Logic System includes a FMEA which shows that the single failure criterion is met for all creditable single failures and all failures caused by the single failure. <u>References</u> CSI 6101-00006 (Enclosure 36 to ET 07-0022)] WCNOC System Reliability Analysis for Advanced Logic System (Enclosure VII to ET 07-0008)</p>

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
	<p>design basis event for which the safety system is required to function. The single-failure criterion applies to the safety systems whether control is by automatic or manual means. IEEE Std 379-1994 provides guidance on the application of the single-failure criterion. (See also [B3].) IEEE Std 7-4.3.2-1993 addresses common cause failures for digital computers.</p> <p>This criterion does not invoke coincidence (or multiple-channel) logic within a safety group; however, the application of coincidence logic may evolve from other criteria or considerations to maximize plant availability or reliability. An evaluation has been performed and documented in other standards to show that certain fluid system failures need not be considered in the application of this criterion [B3]. The performance of a probabilistic assessment of the safety systems may be used to demonstrate that certain postulated failures need not be considered in the application of the criterion. A probabilistic assessment is intended to eliminate consideration of events and failures that are not credible; it shall not be used in lieu of the single-failure criterion. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis.</p> <p>Where reasonable indication exists that a design that meets the single-failure criterion may not satisfy all the reliability</p>	

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
	<p>requirements specified in Clause 4, item i) of the design basis, a probabilistic assessment of the safety system shall be performed. The assessment shall not be limited to single failures. If the assessment shows that the design basis requirements are not met, design features shall be provided or corrective modifications shall be made to ensure that the system meets the specified reliability requirements.</p>	
<p>5.2 Completion of protective action No requirements beyond IEEE Std 603-1998 are necessary.</p>	<p>5.2 Completion of protective action The safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety systems to normal. This requirement shall not preclude the use of equipment protective devices identified in Clause 4, item k) of the design basis or the provision for deliberate operator interventions. Seal-in of individual channels is not required.</p>	<p>This functionality exists in the current design and will be retained in the ALS MSFIS. After a trip signal (ESFAS input or ALL CLOSE input) is received, the trip signal must first no longer be present and then operator action (OPEN switch on MCB) is required to re-open the valves.</p> <p><u>References</u> CSI 6101-00002 (Enclosure 38 to ET 07-0022)</p>
<p>5.3 Quality Hardware quality is addressed in IEEE Std 603-1998. Software quality is addressed in IEEE/EIA Std 12207.0-1996 and supporting standards. Computer development activities shall include the development of computer hardware and software. The integration of the computer hardware and software and the integration of the computer with the safety system shall be addressed in the development process.</p> <p>A typical computer system development process consists of the following life cycle processes:</p>	<p>5.3 Quality 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 (See ASME NQA-1-1994). Guidance</p>	<p>CS Innovations has established a 10 CFR 50 Appendix B Quality Assurance (QA) program. Within this program they have provided a framework for the design development process. Procedure QCP-3, "Design Control" is the top level design related procedure within the CS Innovations QA program. This top level procedure describes the high level development process steps. QCP-3 references a lower tier procedure, 9002-00033, "Hardware Design Development Procedure," for more details of the design development process.</p> <p>Procedure 9002-00033 provides a more detailed discussion of the design development process. It provides a flowchart of the overall process beginning with the customer requirements to the final product or system under development. Procedure 9002-00033 references three lower tier procedures</p>

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
<ul style="list-style-type: none"> - Creating the conceptual design of the system, translation of the concepts into specific system requirements - Using the requirements to develop a detailed system design - Implementing the design into hardware and software functions - Testing the functions to assure the requirements have been correctly implemented - Installing the system and performing site acceptance testing - Operating and maintaining the system - Retiring the system <p>In addition to the requirements of IEEE Std 603-1998, the following activities necessitate additional requirements that are necessary to meet the quality criterion:</p> <ul style="list-style-type: none"> - Software development - Qualification of existing commercial computers (see 5.4.2) - Use of software tools - Verification and validation - Configuration management - Risk Management 	<p>on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993.</p>	<p>for specifics regarding the electrical wiring, board design and development, and FPGA design and development.</p> <p>Procedure 9002-00034, "Electrical Wiring Design Development Procedure," procedure 9002-00035, "Board Design Development Procedure," and procedure 9002-00036, "FPGA Design Development Procedure," each provide a detailed flow chart and descriptions of the activities within the respective design flows.</p> <p><u>References</u> CSI QCP-3 (Enclosure 33 to ET 07-0022) CSI 9002-00033 (Enclosure 39 to ET 07-0022) CSI 9002-00034 (Enclosure 39 to ET 07-0022) CSI 9002-00035 (Enclosure 39 to ET 07-0022) CSI 9002-00036 (Enclosure 39 to ET 07-0022)</p>
<p>5.3.1 Software development Computer software shall be developed, modified, or accepted in accordance with an approved software quality assurance (QA) plan consistent with the requirements of IEEE/EIA 12207.0-1996. The software QA plan shall address all software that is resident on the computer at run time (i.e., application software, network software, interfaces, operating systems, and diagnostics). Guidance for developing software QA plans can be found in IEC 60880 (1986-09) [B4] and IEEE Std 730™-1998 [B8].</p>	<p>N/A</p>	<p>A review of CS Innovations 6101-00009, "MSFIS Quality Assurance Plan," determined that the MSFIS Quality Assurance (QA) Plan is consistent with the requirements of IEEE/EIA 12207.0-1996. The CS Innovations MSFIS QA Plan has been tailored to the replacement MSFIS Controls project in accordance with paragraph 1.3 of IEEE/EIA 12207.0-1996.</p> <p><u>References</u> CSI 6101-00009 (Enclosure 39 to ET 07-0022)</p>

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
<p>5.3.1.1 Software quality metrics The use of software quality metrics shall be considered throughout the software life cycle to assess whether software quality requirements are being met. When software quality metrics are used, the following life cycle phase characteristics should be considered:</p> <ul style="list-style-type: none"> - Correctness/Completeness (Requirements phase) - Compliance with requirements (Design phase) - Compliance with design (Implementation phase) - Functional compliance with requirements (Test and Integration phase) - On-site functional compliance with requirements (Installation and Checkout phase) - Performance history (Operation and Maintenance phase) <p>The basis for the metrics selected to evaluate software quality characteristics should be included in the software development documentation. IEEE Std 1061™-1998 [B11] provides a methodology for the application of software quality metrics.</p>	<p>N/A</p>	<p>CS Innovations 6101-00009, "MSFIS Quality Assurance Plan," includes requirements for defect tracking and process improvement, and the CS Innovations 6101-00008, "MSFIS V&V Plan," includes the life cycle phase characteristics identified in IEEE 7-4.3.2, with the exception of performance history. Performance history is maintained by the WCNOC maintenance program.</p> <p><u>References</u> CSI 6101-00009 (Enclosure 39 to ET 07-0022) CSI 6101-00008 (Enclosure 27 to ET 07-0022)</p>

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
<p>5.3.2 Software tools Software tools used to support software development processes and verification and validation (V&V) processes shall be controlled under configuration management.</p> <p>One or both of the following methods shall be used to confirm the software tools are suitable for use:</p> <p>a) A test tool validation program shall be developed to provide confidence that the necessary features of the software tool function as required.</p> <p>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.</p> <p>Tool operating experience may be used to provide additional confidence in the suitability of a tool, particularly when evaluating the potential for undetected defects.</p>		<p>CS Innovations utilizes several software tools to achieve the final design of the ALS. These software tools are critical aspects to ensure the final ALS hardware meets the intended design objectives.</p> <p>Tools selected for a particular project are controlled by configuration management. Specifically, the tools utilized in the development life cycle for a particular project are configuration controlled and maintained with all files associated with that project.</p> <p>CS Innovations performs a tool assessment and qualification to ensure that the tool(s) are capable of performing the particular design or verification activity to an acceptable level of confidence. Tool assessment and qualification has two fundamental aspects: 1) ensures the proper tool is used for a particular activity in the development of the ALS, and 2) identifies how the output of a particular tool is independently assessed within the V&V Activities. Tool assessment and qualification is described in CS Innovations 6000-00010 "ALS Design Tools," Chapter 2. Tool assessment and qualification satisfy the methods described in IEEE 7-4.3.2, Section 5.3.2, to confirm the software tools are suitable for use.</p> <p>Tool operating experience has also been utilized for determining software tool suitability. CS Innovations 6000-00010, "ALS Design Tools," discusses the experience with the software tools being utilized.</p> <p><u>References</u> CSI 6000-00010 (Enclosure III to ET 07-0039) CSI 6101-00005 (Enclosure 31 to ET 07-0022)</p>

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
<p>5.3.3 Verification and validation NOTE—See IEEE Std 1012-1998 and IEEE Std 1012a™-1998 [B10] for more information about software V&V.</p> <p>V&V is an extension of the program management and systems engineering team activities. V&V is used to identify objective data and conclusions (i.e., proactive feedback) about digital system quality, performance, and development process compliance throughout the system life cycle. Feedback consists of anomaly reports, performance improvements, and quality improvements regarding the expected operating conditions across the full spectrum of the system and its interfaces.</p> <p>V&V processes are used to determine whether the development products of an activity conform to the requirements of that activity, and whether the system performs according to its intended use and user needs. This determination of suitability includes assessment, analysis, evaluation, review, inspection, and testing of products and processes.</p> <p>This standard adopts the IEEE Std 1012-1998 terminology of process, activity and task, in which software V&V processes are subdivided into activities, which are further subdivided into tasks. The term V&V effort is used to reference this framework of V&V processes, activities, and tasks.</p> <p>V&V processes shall address the computer hardware and software, integration of the digital system components, and the interaction of the resulting computer system with the nuclear power plant.</p> <p>The V&V activities and tasks shall include system testing of the final integrated hardware, software, firmware, and interfaces.</p> <p>The software V&V effort shall be performed in accordance with IEEE Std 1012-1998. The IEEE Std 1012-1998 V&V requirements for the highest integrity level (level 4) apply to systems developed using this standard (i.e., IEEE Std 7-4.3.2™). See IEEE Std 1012-1998 Annex B for a definition of integrity level 4 software.</p>		<p>CS Innovations employs a V&V process for developing ALS based applications as described in 6101-00008, "MSFIS V&V Plan." CS Innovations implements a top level V&V plan for a particular application utilizing the ALS. The purpose of the V&V plan is to establish a consistent method for providing V&V sufficient to ensure safety and risk mitigation for the successful deployment of the system. For ALS based applications the V&V activities are performed as part of the ongoing development and manufacturing process to facilitate the timely detection of errors. The V&V activities are also performed to analyze and test the system with respect to the hardware interfaces, customer interfaces, and the safety related functionality.</p> <p>CS Innovations also performs ALS specific V&V activities that are independent of the replacement MSFIS Controls application V&V activities. ALS specific V&V activities are encompassed within the various procedures that deal with the design development process. This includes procedures such as 9002-00033, "Hardware Design Development Procedure," 9002-00034, "Electrical Wiring Design Development Procedure," 9002-00035, "Board Design Development Procedure," and 9002-00036, "FPGA Design Development Procedure."</p> <p>CS Innovations requires specific design reviews during each phase of the project. The design review requirements are specified in procedures 9002-00024, "Electrical Wiring Design Review Procedure," 9002-00025, "Board Design Review Procedure," and 9002-00026, "FPGA Design Review Procedure." The required reviews are summarized as follows:</p>

c,d

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position	c,d
		<p><u>References</u> CSI 6101-00008 (Enclosure 27 to ET 07-0022) CSI 9002-00036 (Enclosure 39 to ET 07-0022) CSI 6000-00008 (Enclosure 28 to ET 07-0022) CSI 9002-00034 (Enclosure 39 to ET 07-0022) CSI 9002-00035 (Enclosure 39 to ET 07-0022)</p>	

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
<p>5.3.4 Independent V&V (IV&V) requirements The previous section addresses the V&V activities to be performed. This section defines the levels of independence required for the V&V effort. IV&V activities are defined by three parameters: technical independence, managerial independence, and financial independence. These parameters are described in Annex C of IEEE Std 1012-1998.</p> <p>The development activities and tests shall be verified and validated by individuals or groups with appropriate technical competence, other than those who developed the original design.</p> <p>Oversight of the IV&V effort shall be vested in an organization separate from the development and program management organizations. The V&V effort shall independently select</p> <ol style="list-style-type: none"> a) The segments of the software and system to be analyzed and tested, b) The V&V techniques, and c) The technical issues and problems upon which to act. <p>The V&V effort shall be allocated resources that are independent of the development resources.</p> <p>See Annex C of IEEE Std 1012-1998 for additional guidance.</p>		<p>The CS Innovations V&V team is responsible for the V&V performance of all phases of the system life cycle. The V&V organization performs reviews, audits, tests and analysis in addition to normal design reviews performed within the CS Innovations organization. The V&V team is responsible for the organization of the V&V activities, as well as creating the V&V plan for a particular project. Given the fact that CS Innovations is a small company, they have chosen to head the V&V team with the president of the company. This ensures maximum familiarization with the design principles, features of the ALS, customer requirements, etc. Although this does not constitute independence between financial interests and the V&V effort, it does emphasize the focus on the V&V effort. Independence of the financial interests was not deemed necessary given the president of the company has a high interest in the V&V conducted in the best possible manner, and that the final product outcome be of the highest quality possible.</p> <p>To ensure the V&V effort is a value added aspect of the overall process the V&V team is staffed with members familiar with all processes used within CS Innovations from design, to manufacturing, to final test procedures and execution of the test equipment. This ensures a complete independent understanding of the system, without support from the design team for interpretations of the functionality of the system and the results of testing.</p> <p><u>References</u> CSI 6101-00008 (Enclosure 27 ET 07-0022)</p>
<p>5.3.5 Software configuration management Software configuration management shall be performed in accordance with IEEE Std 1042-1987. IEEE Std 828™-1998 [B9] provides guidance for the development of software configuration management plans.</p> <p>The minimum set of activities shall address the following:</p> <ol style="list-style-type: none"> a) Identification and control of all software designs and code b) Identification and control of all software design functional data (e.g., data templates and data bases) c) Identification and control of all software design interfaces d) Control of all software design changes e) Control of software documentation (user, operating, and maintenance documentation) 	N/A	<p>CS Innovations 6101-00005, "MSFIS Configuration Management Plan," is based on IEEE Std 828 and the guidance in IEEE Std 1042. The Configuration Management (CM) Plan identifies the configuration items that are under configuration management, provides detailed requirements and responsibilities for the change process, and defines the baselining process. The CM Plan also includes detailed requirements for document and software identification, release, archiving and audits.</p> <p><u>Reference</u> CSI 6101-00005 (Enclosure 31 to ET 07-0022)</p>

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
<p>f) Control of software vendor development activities for the supplied safety system software g) Control and retrieval of qualification information associated with software designs and code h) Software configuration audits i) Status accounting</p> <p>Some of these functions or documents may be performed or controlled by other QA activities. In this case, the software configuration management plan shall describe the division of responsibility.</p> <p>A software baseline shall be established at appropriate points in the software life cycle process to synchronize engineering and documentation activities. Approved changes that are created subsequent to a baseline shall be added to the baseline.</p> <p>The labeling of the software for configuration control shall include unique identification of each configuration item, and revision and/or date time stamps for each configuration item.</p> <p>Changes to the software/firmware shall be formally documented and approved consistent with the software configuration management plan. The documentation shall include the reason for the change, identification of the affected software/firmware, and the impact of the change on the system. Additionally, the documentation should include the plan for implementing the change in the system (e.g., immediately implementing the change, or scheduling the change for a future version).</p>		

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
<p>5.3.6 Software project risk management Software project risk management is a tool for problem prevention: identifying potential problems, assessing their impact, and determining which potential problems must be addressed to assure that software quality goals are achieved. Risk management shall be performed at all levels of the digital system project to provide adequate coverage for each potential problem area. Software project risks may include technical, schedule, or resource-related risks that could compromise software quality goals, and thereby affect the ability of the safety computer system to perform safety related functions. Software project risk management differs from hazard analysis, as defined in 3.1.31, in that hazard analysis is focused solely on the technical aspects of system failure mechanisms.</p>	<p>N/A</p>	<p>Risk management is addressed by CS Innovations 6101-00008, "MSFIS V&V Plan," in conjunction with procedure QCP-16, "Corrective Action." The Plan specifies the V&V activities which shall be completed at each phase of the life cycle and the corresponding task iteration and audit policies.</p> <p><u>References</u> CSI 6101-00008 (Enclosure 27 to ET 07-0022) CSI QCP-16 (Enclosure33 to ET 07-0022)</p>
<p>5.4 Equipment qualification In addition to the equipment qualification criteria provided by IEEE Std 603-1998, the requirements listed in 5.4.1 and 5.4.2 are necessary to qualify digital computers for use in safety systems.</p>		
<p>5.4.1 Computer system testing Computer system qualification testing (see 3.1.36) shall be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, shall be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the CPU, inputs and outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing shall demonstrate that the performance requirements related to safety functions have been met.</p>		<p>Qualification testing was performed on the ALS equipment per the requirements in WCNOC Specification J-105A. The qualification testing was completed with a full ALS rack, including all circuit cards installed, as well as the assembly panel. The ALS rack was configured with the complete functionality being the production system to be installed at Wolf Creek Generating Station for the MSFIS Controls. This logic included all diagnostics and self test capabilities of the ALS. The equipment was functionally tested before each test and after the completion of each test. During the qualification testing the equipment was actuated to perform the safety related function while all diagnostics and self-test capabilities were functioning. The qualification testing proved that the equipment was capable of accomplishing all safety functions and that the safety function was not impaired due to the self-test, diagnostics, or other features of the system not directly required to accomplish the safety function.</p> <p><u>References</u> WCNOC Specification J-105A(Q) (Enclosure I to ET 07-0008) NI WCN-9715R, Rev. 0 (Enclosure VI to ET 07-0008)</p>
<p>5.4.2 Qualification of existing commercial computers NOTE—See Annex C for more information about commercial grade item dedication.</p>		<p>The replacement MSFIS Controls have been developed by CS Innovations. The replacement MSFIS Controls is based on the ALS. CS Innovations has developed the ALS for safety critical applications across multiple industries, with a particular focus on the nuclear industry. At the time the replacement MSFIS Controls project began, CS Innovations was considered by WCNOC as</p>

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
<p>The qualification process shall be accomplished by evaluating the hardware and software design using the criteria of this standard. Acceptance shall be based upon evidence that the digital system or component, including hardware, software, firmware, and interfaces, can perform its required functions. The acceptance and its basis shall be documented and maintained with the qualification documentation.</p> <p>In those cases in which traditional qualification processes cannot be applied, an alternative approach to verify a component is acceptable for use in a safety-related application is commercial grade dedication. The objective of commercial grade dedication is to verify that the item being dedicated is equivalent in quality to equipment developed under a 10 CFR 50 Appendix B program [B16].</p> <p>The dedication process for the computer shall entail identification of the physical, performance, and development process requirements necessary to provide adequate confidence that the proposed digital system or component can achieve the safety function. The dedication process shall apply to the computer hardware, software, and firmware that are required to accomplish the safety function. The dedication process for software and firmware shall, whenever possible, include an evaluation of the design process. There may be some instances in which a design process cannot be evaluated as part of the dedication process. For example, the organization performing the evaluation may not have access to the design process information for a microprocessor chip to be used in the safety system. In this case, it would not be possible to perform an evaluation to support the dedication. Because the dedication process involves all aspects of life cycle processes and manufacturing quality, commercial grade item dedication should be limited to items that are relatively simple in function relative to their intended use.</p> <p>Commercial grade item dedication involves preliminary phase and detailed phase activities. These phase activities are described in 5.4.2.1 through 5.4.2.2.</p>		<p>a commercial supplier. CS Innovations indicated their intention to develop a 10 CFR 50 Appendix B program during the execution of the replacement MSFIS Controls project. However, due to the fact CS Innovations was considered by WCNOC to be a commercial supplier at the beginning of the project, a third party qualifier and dedicator was contracted by WCNOC to provide adequate confidence that the ALS based replacement MSFIS Controls could achieve the required safety function. Nutherm International was contracted by WCNOC to fulfill the role as the third party qualifier and dedicator.</p> <p>CS Innovations has continued developing their 10 CFR 50 Appendix B Program throughout the execution of the replacement MSFIS Controls Project. WCNOC performed a 10 CFR 50 Appendix B audit of the CS Innovations program in September 2007. The results of the WCNOC audit found the CS Innovations Appendix B program to be satisfactory. The audit identified four administrative findings which did not effect the actual hardware developed under the program. Therefore, WCNOC has added CS Innovations to the approved supplier list for safety-related equipment. Subsequent orders from WCNOC to CS Innovations may be safety-related orders, in this case a third party qualifier and dedicator will not be necessary.</p> <p>Nutherm International has provided the 1) qualification and 2) dedication services for the replacement MSFIS Controls Project.</p> <p>1) The qualification of the equipment has been completed per WCNOC requirements as identified in specification J-105A(Q). The qualification plan and qualification results are provided in Nutherm International documents WCN-9715P, "Nutherm Qualification Plan," Rev.1, and WCN-9715R, "Nutherm Qualification Report," Rev.0. As discussed in the response to 7-4.3.2 – 2003, Section 5.4.1, the equipment was exercising all portions of the functionality required to accomplish the safety functions as well as all functionality of the built-in self-testing, diagnostics, and other functionality not directly required to accomplish the safety function.</p> <p>2) The Nutherm International dedication process has identified the physical, performance, and dependability characteristics necessary to provide adequate confidence that the proposed digital system can achieve the safety function.</p> <p>The physical characteristics are those characteristics of the item which deals with its construction, materials, shape, form and fit, etc. The ALS physical characteristics have been compared with the qualified equipment to ensure similarity. Any differences have been noted and evaluated for impact on qualification by the Nutherm Engineering Department.</p> <p>The performance characteristics of the ALS are the operational critical characteristics as determined by a technical evaluation. The performance characteristics have been verified through testing and analysis. The performance testing verifies proper operation of the system and compliance</p>

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
		<p>with the WCNOC specification J-105A. Nutherm International will perform a detailed test procedure, TPS-9064, "Final Acceptance Testing for Main Steam Feedwater Isolation System (MSFIS) Rack," to verify the performance aspects of the replacement MSFIS Controls.</p> <p>The dependability characteristics of the ALS focuses on items such as reliability and built-in quality. The dependability of a digital system is strongly influenced by the development process and the personnel involved in the design, development, verification, and validation of the digital equipment. The ALS is considered a software-based digital system which depends on high quality software utilized in the development to ensure the intended design objective is achieved. However, the system does not contain, nor rely on, software or firmware for the execution of the system. Given the fact that the ALS is software-based digital system, as described above, the dependability aspects of the ALS are critical to ensure adequate confidence that the ALS can achieve the safety function. The Nutherm International Final Dedication Report will provide the final results and conclusions regarding the dedication process employed.</p> <p><u>References</u> WCNOC Specification J-105A(Q) (Enclosure I to ET 07-0008) NI WCN-9715R, Rev. 0 (Enclosure VI to ET 07-0008)</p>
<p>5.5 System integrity In addition to the system integrity criteria provided by IEEE Std 603-1998, the following are necessary to achieve system integrity in digital equipment for use in safety systems:</p> <ul style="list-style-type: none"> — Design for computer integrity — Design for test and calibration — Fault detection and self-diagnostics 		

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
<p>5.5.1 Design for computer integrity The computer shall be designed to perform its safety function when subjected to conditions, external or internal, that have significant potential for defeating the safety function. For example, input and output processing failures, precision or roundoff problems, improper recovery actions, electrical input voltage and frequency fluctuations, and maximum credible number of coincident signal changes.</p> <p>If the system requirements identify a safety system preferred failure mode, failures of the computer shall not preclude the safety system from being placed in that mode. Performance of computer system restart operations shall not result in the safety system being inhibited from performing its function.</p>		

c,d

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position	c,d
<p>5.5.2 Design for test and calibration Test and calibration functions shall not adversely affect the ability of the computer to perform its safety function. Appropriate bypass of one redundant channel is not considered an adverse effect in this context. It shall be verified that the test and calibration functions do not affect computer functions that are not included in a calibration change (e.g., setpoint change).</p> <p>V&V, configuration management, and QA shall be required for test and calibration functions on separate computers (e.g., test and calibration computer) that provide the sole verification of test and calibration data. V&V, configuration management, and QA shall be required when the test and calibration function is inherent to the computer that is part of the safety system.</p> <p>V&V, configuration management, and QA are not required when the test and calibration function is resident on a separate computer and does not provide the sole verification of test and calibration data for the computer that is part of the safety system.</p>		<p>The on-line test capabilities of the ALS are fully contained within the ALS system, thus no separate test systems are required.</p> <p>The ALS does not implement setpoints, e.g., calibration settings for specific trip points, for the replacement MSFIS Controls. Therefore specific concerns regarding the calibration and changing of setpoints do not apply.</p> <p><u>References</u> CSI 6000-00000 (Enclosure 37 to ET 07-0022)</p>	<p>c,d</p> <p>c,d</p>

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position	c,d
<p>5.5.3 Fault detection and self-diagnostics Computer systems can experience partial failures that can degrade the capabilities of the computer system, but may not be immediately detectable by the system. Self-diagnostics are one means that can be used to assist in detecting these failures. Fault detection and self-diagnostics requirements are addressed in this subclause.</p> <p>The reliability requirements of the safety system shall be used to establish the need for self-diagnostics. Self diagnostics are not required for systems in which failures can be detected by alternate means in a timely manner. If self-diagnostics are incorporated into the system requirements, these functions shall be subject to the same V&V processes as the safety system functions.</p> <p>If reliability requirements warrant self-diagnostics, then computer programs shall incorporate functions to detect and report computer system faults and failures in a timely manner. Conversely, self-diagnostic functions shall not adversely affect the ability of the computer system to perform its safety function, or cause spurious actuations of the safety function. A typical set of self-diagnostic functions includes the following:</p> <ul style="list-style-type: none"> — Memory functionality and integrity tests (e.g., PROM checksum and RAM tests) — Computer system instruction set (e.g., calculation tests) — Computer peripheral hardware tests (e.g., watchdog timers and keyboards) — Computer architecture support hardware (e.g., address lines and shared memory interfaces) — Communication link diagnostics (e.g., CRC checks) <p>Infrequent communication link failures that do not result in a system failure or a lack of system functionality do not require reporting.</p> <p>When self-diagnostics are applied, the following self-diagnostic features shall be incorporated into the system design:</p> <ol style="list-style-type: none"> a) Self-diagnostics during computer system startup b) Periodic self-diagnostics while the computer system is operating c) Self-diagnostic test failure reporting 		<p><u>References</u></p> <p>CSI 6000-00000 (Enclosure 37 to ET 07-0022) Sections; 2.1, 2.7.1, 2.7.3, 7.4</p>	

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
<p>5.6 Independence In addition to the requirements of IEEE Std 603-1998, data communication between safety channels or between safety and nonsafety systems shall not inhibit the performance of the safety function.</p> <p>IEEE Std 603-1998 requires that safety functions be separated from nonsafety functions such that the nonsafety functions cannot prevent the safety system from performing its intended functions. In digital systems, safety and nonsafety software may reside on the same computer and use the same computer resources.</p> <p>Either of the following approaches is acceptable to address the previous issues:</p> <p>a) Barrier requirements shall be identified to provide adequate confidence that the nonsafety functions cannot interfere with performance of the safety functions of the software or firmware. The barriers shall be designed in accordance with the requirements of this standard. The nonsafety software is not required to meet these requirements.</p> <p>b) If barriers between the safety software and nonsafety software are not implemented, the nonsafety software functions shall be developed in accordance with the requirements of this standard.</p> <p>Guidance for establishing communication independence is provided in Annex E.</p>	<p>5.6 Independence</p> <p>5.6.1 Between redundant portions of a safety system Redundant portions of a safety system provided for a safety function shall be independent of, and physically separated from, each other to the degree necessary to retain the capability of accomplishing the safety function during and following any design basis event requiring that safety function.</p> <p>5.6.2 Between safety systems and effects of design basis event Safety system equipment required to mitigate the consequences of a specific design basis event shall be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability of meeting the requirements of this standard. Equipment qualification in accordance with 5.4 is one method that can be used to meet this requirement.</p> <p>5.6.3 Between safety systems and other systems The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in Clause 4, item h) of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.</p> <p>5.6.3.1 Interconnected equipment a) <i>Classification.</i> Equipment that is used for both safety and nonsafety functions shall be classified as part of the safety systems. Isolation devices used to effect a safety system</p>	<p>The ALS MSFIS will be installed in the existing Group 1 and Group 4 cabinets, maintaining the current safety group separations. New switches installed on the MCB to control both trains include physical barriers which meet the requirements of IEEE Std 384-1992.</p> <p>The ALS MSFIS equipment has been seismically qualified by the Appendix B supplier, Nutherm International.</p> <p>There are no changes from the existing MSFIS design.</p>

c,d

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
	<p>boundary shall be classified as part of the safety system.</p> <p>b) <i>Isolation</i>. No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.</p> <p>5.6.3.2 Equipment in proximity</p> <p>a) <i>Separation</i>. Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems capability to accomplish their safety functions in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384-1992. (See [B1].)</p> <p>b) <i>Barrier</i>. Physical barriers used to effect a safety system boundary shall meet the requirements of 5.3, 5.4 and 5.5 for the applicable conditions specified in Clause 4, items g) and h) of the design basis.</p>	<p>There are no changes from the existing MSFIS design.</p>

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
	<p>5.6.3.3 Effects of a single random failure Where a single random failure in a nonsafety system can result in a design basis event, and also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. See IEEE Std 379-1994 for the application of this requirement.</p> <p>5.6.4 Detailed criteria IEEE Std 384-1992 provides detailed criteria for the independence of Class 1E equipment and circuits [B1]. IEEE Std 7-4.3.2-1993 provides guidance on the application of this criteria for the separation and isolation of the data processing functions of interconnected computers.</p>	<p>There are no changes from the existing MSFIS design.</p> <p>As described above, the IEEE Std 7-4.3.2-1993 requirements have been applied to the ASU service and test connection.</p> <p><u>References</u> CSI 6000-00000 (Enclosure 37 to ET 07-0022) NI WCN-9715R, Rev. 0 (Enclosure VI to ET 07-0008)</p>

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
<p>5.7 Capability for test and calibration No requirements beyond IEEE Std 603-1998 are necessary.</p>	<p>5.7 Capability for testing and calibration Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. Testing of Class 1E systems shall be in accordance with the requirements of IEEE Std 338-1987. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station. In this case:</p> <ul style="list-style-type: none"> - Appropriate justification shall be provided (e.g., demonstration that no practical design exists), - Acceptable reliability of equipment operation shall be otherwise demonstrated, and - The capability shall be provided while the generating station is shut down. 	<p>The ALS includes the capability for a maintenance bypass function. The replacement MSFIS Controls implementation provides a maintenance bypass for each of the Main Steam Isolation Valve (MSIV) and Main Feedwater Isolation Valve (MFIV). When a single train is in bypass, the opposite train maintains the capability to perform the MSFIS safety function (also see the position associated with Section 5.3.2).</p>
<p>5.8 Information displays No requirements beyond IEEE Std 603-1998 are necessary.</p>	<p>5.8.1 Displays for manually controlled actions</p> <p>The display instrumentation provided for manually controlled actions for which no automatic control is provided and the display instrumentation required for the safety systems to accomplish their safety functions shall be part of the safety</p>	<p>There are no changes from the existing MSFIS design.</p>

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
	<p>systems and shall meet the requirements of IEEE Std 497-1981 [B10]. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator.</p> <p>5.8.2 System status indication</p> <p>Display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status. This information shall include indication and identification of protective actions of the sense and command features and execute features. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. The display instrumentation provided for safety system status indication need not be part of the safety systems.</p> <p>5.8.3 Indication of bypasses</p> <p>If the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room.</p> <p>a) This display instrumentation need not be part of the safety systems. b) This indication shall be automatically actuated if the bypass or inoperative condition is expected to occur more</p>	<p>The ALS MSFIS includes a "Summary Trouble Alarm" for each train on the MCB. This alarm will activate on any system fault.</p> <p>The ALS MSFIS includes a STATUS indicator for each train on the MCB. This will indicate if any valve is in bypass mode.</p>

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
	<p>frequently than once a year, and is expected to occur when the affected system is required to be operable.</p> <p>c) The capability shall exist in the control room to manually activate this display indication.</p> <p>5.8.4 Location</p> <p>Information displays shall be located accessible to the operator. Information displays provided for manually controlled protective actions shall be visible from the location of the controls used to affect the actions.</p>	<p>The Summary Trouble Alarm and Status indicators are located on the MCB alarm and status panels in the same locations as the existing system.</p> <p><u>References</u> CSI 6000-00000 (Enclosure 37 to ET 07-0022)</p>
<p>5.9 Control of access No requirements beyond IEEE Std 603-1998 are necessary.</p>	<p>5.9 Control of access The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.</p>	<p>Physical access is controlled by plant security. Administrative controls limit access when the ASU is connected.</p>
<p>5.10 Repair No requirements beyond IEEE Std 603-1998 are necessary.</p>	<p>5.10 Repair The safety systems shall be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.</p>	<p>The ALS MSFIS contains extensive on-line continuous self-test, failure detection and isolation, and off-line diagnostic aids.</p>
<p>5.11 Identification To provide assurance that the required computer system hardware and software are installed in the appropriate system configuration, the following identification requirements specific to software systems shall be met: a) Firmware and software identification shall be used to assure the correct software is installed in the correct hardware component.</p>	<p>5.11 Identification In order to provide assurance that the requirements given in this standard can be applied during the design, construction, maintenance, and operation of the plant, the following</p>	

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
<p>b) Means shall be included in the software such that the identification may be retrieved from the firmware using software maintenance tools.</p> <p>c) Physical identification requirements of the digital computer system hardware shall be in accordance with the identification requirements in IEEE Std 603-1998.</p>	<p>requirements shall be met:</p> <p>a) Safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std 384-1992 and IEEE Std 420-1982.</p> <p>b) Components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification.</p> <p>c) Identification of safety system equipment shall be distinguishable from any identifying markings placed on equipment for other purposes (e.g., identification of fire protection equipment, phase identification of power cables).</p> <p>d) Identification of safety system equipment and its divisional assignment shall not require frequent use of reference material.</p> <p>e) The associated documentation shall be distinctly identified in accordance with the requirements of IEEE Std 494-1974 [B9].</p> <p>f) The versions of computer hardware, programs, and software shall be distinctly identified in accordance with IEEE Std 7-4.3.2-1993.</p>	<p>No changes to existing safety group identification (cabinet nameplates and color-coded wiring).</p> <p>There are no changes from the existing MSFIS design.</p> <p>There are no changes from the existing MSFIS design.</p> <p>There are no changes from the existing MSFIS design.</p> <p>There are no changes from the existing MSFIS design.</p>

c,d

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
<p>5.12 Auxiliary features No requirements beyond IEEE Std 603-1998 are necessary.</p>	<p>5.12 Auxiliary features Auxiliary supporting features shall meet all requirements of <i>this standard</i>.</p> <p>Other auxiliary features that perform a function that is not required for the safety systems to accomplish their safety functions, and are part of the safety systems by association (i.e., not isolated from the safety system) shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. Examples of these other auxiliary features are shown in Figure 3 and an illustration of the application of this criteria is contained in Annex A.</p>	<p>As one element of the Engineered Safety Features Actuation System (ESFAS), the ALS MSFIS does not contain any auxiliary features as defined here. The complete ALS MSFIS has been designed to meet this standard.</p>
<p>5.13 Multi-unit stations No requirements beyond IEEE Std 603-1998 are necessary.</p>	<p>5.13 Multi-unit stations The sharing of structures, systems, and components between units at multi-unit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired. Guidance on the sharing of electrical power systems between units is contained in IEEE Std 308-1991. Guidance on the application of the single failure criterion to shared systems is contained in IEEE Std 379-1994.</p>	<p>This is not applicable as WCGS is a single unit facility.</p>

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
<p>5.14 Human factor considerations No requirements beyond IEEE Std 603-1998 are necessary.</p>	<p>5.14 Human factor considerations Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023-1988.</p>	<p>Human factor considerations were a major design goal of the ALS MSFIS project. All operator information is available on the front panels. Controls and indicators are clearly labeled and grouped and show the state of the system for efficient evaluation of system status.</p>
<p>5.15 Reliability NOTE—See Annex F for more information about the reliability criterion.</p> <p>In addition to the requirements of IEEE Std 603-1998, when reliability goals are identified, the proof of meeting the goals shall include the software. The method for determining reliability may include combinations of analysis, field experience, or testing. Software error recording and trending may be used in combination with analysis, field experience, or testing.</p>	<p>5.15 Reliability For those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis. Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993.</p>	<p>The quantitative reliability goal established for the ALS MSFIS was to exceed the two year mean time between failure (MTBF) of the existing MSFIS equipment. A System Reliability Analysis (SRA) was performed in accordance with IEEE Std 352-1987 and IEEE Std 577-1976. The SRA shows that the reliability goal has been far exceeded.</p> <p><u>References</u> WCNOC System Reliability Analysis for Advanced Logic System (Enclosure VII to ET 07-0008)</p>
<p>6. Sense and command features—functional and design requirements No requirements beyond IEEE Std 603-1998 are necessary.</p>	<p>6. Sense and command features—functional and design requirements In addition to the functional and design requirements in Clause 5, the requirements listed in 6.1 through 6.8 shall apply to the sense and command features.</p> <p>6.1 Automatic control Means shall be provided to automatically initiate and control all protective actions except as</p>	<p>This requirement is not applicable to the extent that the MSFIS does not automatically initiate protective actions, however as an element of the ESFAS, the MSFIS provides automatic MSIV and MFIV closure, without operator</p>

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
	<p>justified in Clause 4, item e). The safety system design shall be such that the operator is not required to take any action prior to the time and plant conditions specified in Clause 4, item e) following the onset of each design basis event. At the option of the safety system designer, means may be provided to automatically initiate and control those protective actions of Clause 4, item e).</p> <p>6.2 Manual control Means shall be provided in the control room to</p> <p>a) Implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1.</p> <p>b) Implement manual initiation and control of the protective actions identified in Clause 4, item e) that have not been selected for automatic control under 6.1. The displays provided for these actions shall meet the requirements of 5.8.1.</p> <p>c) Implement the manual actions necessary to maintain safe conditions after the protective actions are completed as specified in Clause 4, item j). The information provided to the operators, the actions required of these operators, and the quantity and location of associated displays and controls shall be appropriate for</p>	<p>intervention, when commanded via the ESFAS trip input.</p> <p>Main Control Board (MCB) MSFIS control functions are provided (essentially unchanged from the existing system) which meet this requirement.</p>

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
	<p>the time period within which the actions shall be accomplished and the number of available qualified operators. Such displays and controls shall be located in areas that are accessible, located in an environment suitable for the operator, and suitably arranged for operator surveillance and action.</p> <p>6.3 Interaction between the sense and command features and other systems</p> <p>6.3.1 Requirements Where a single credible event, including all direct and consequential results of that event, can cause a non- safety system action that results in a condition requiring protective action, and can concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, one of the following requirements shall be met:</p> <p>a) Alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design basis. Alternate channels shall be selected from the following:</p> <ol style="list-style-type: none"> 1) Channels that sense a set of variables different from the principal channels. 2) Channels that use equipment different from that of the principal channels to 	<p>No change from the existing system of two trains of MSFIS.</p>

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
	<p>sense the same variable.</p> <p>3) Channels that sense a set of variables different from those of the principal channels using equipment different from that of the principal channels.</p> <p>4) Both the principal and alternate channels shall be part of the sense and command features.</p> <p>b) Equipment not subject to failure caused by the same single credible event shall be provided to detect the event and limit the consequences to a value specified by the design bases. Such equipment is considered a part of the safety system. See Figure 5 for a decision chart for applying the requirements of this clause.</p> <p>6.3.2 Provisions Provisions shall be included so that the requirements in 6.3.1 can be met in conjunction with the requirements of 6.7 if a channel is in maintenance bypass. These provisions include reducing the required coincidence, defeating the non-safety system signals taken from the redundant channels, or initiating a protective action from the bypassed channel.</p> <p>6.4 Derivation of system inputs To the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis.</p>	<p>No change from the existing system. Only one train of MSFIS is required to close a valve.</p> <p>No change from the existing system. Each train of ALS MSFIS utilizes independent inputs from switches on the MCB and valve position instrumentation on the valve actuators.</p>

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
	<p>6.5 Capability for testing and calibration</p> <p>6.5.1 Checking the operational availability Means shall be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation. This may be accomplished in various ways; for example:</p> <ul style="list-style-type: none"> a) By perturbing the monitored variable, b) Within the constraints of 6.6, by introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable, or c) By cross-checking between channels that bear a known relationship to each other and that have read- outs available. <p>6.5.2 Assuring the operational availability One of the following means shall be provided for assuring the operational availability of each sense and command feature required during the post-accident period:</p> <ul style="list-style-type: none"> a) Checking the operational availability of sensors by use of the methods described in 6.5.1. b) Specifying equipment that is stable and the period of time it retains its calibration during the post- accident time period. 	<p>ALS MSFIS continuous self-test functions include all of the MSFIS inputs and the existing manual system test capabilities are retained. This includes complete testing of the safety function from the ESFAS input to the valve actuation outputs.</p> <p>ALS MSFIS provides continuous self-test features and extensive redundancy within each train. Failures are annunciated in the Control Room.</p>

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
	<p>6.6 Operating bypasses Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:</p> <ul style="list-style-type: none"> a) Remove the appropriate active operating bypass(es). b) Restore plant conditions so that permissive conditions once again exist. c) Initiate the appropriate safety function(s). <p>6.7 Maintenance bypass Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features should continue to meet the requirements of 5.1 and 6.3. NOTE—For portions of the sense and command features that cannot meet the requirements of 5.1 and 6.3 when in maintenance bypass, acceptable reliability of equipment operation shall be demonstrated (e.g., that the period allowed for removal from service for maintenance bypass is sufficiently short, or additional measures are taken, or both, to ensure there is no significant detrimental effect on overall</p>	<p>This requirement is not applicable. The ALS MSFIS does not include any operating bypass functions.</p> <p>If one train of ALS MSFIS is in maintenance bypass, the other train retains the capability to perform the safety function. Administrative controls prevent both trains from being in bypass simultaneously.</p>

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
	<p>sense and command feature availability).</p> <p>6.8 Setpoints The allowance for uncertainties between the process analytical limit documented in Clause 4, item d) and the device setpoint shall be determined using a documented methodology. Refer to ANSI/ISA S67.04-1994.</p> <p>Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required. The devices used to prevent improper use of less restrictive setpoints shall be part of the sense and command features.</p>	<p>This requirement is not applicable to ALS MSFIS. There are no analog inputs or setpoints.</p>
<p>7. Execute features—functional and design requirements No requirements beyond IEEE Std 603-1998 are necessary.</p>	<p>In addition to the functional and design requirements in Clause 5, the requirements listed in 7.1 through 7.5 shall apply to the execute features.</p> <p>7.1 Automatic control Capability shall be incorporated in the execute features to receive and act upon automatic control signals from the sense and command features consistent with Clause 4, item d) of the design basis.</p> <p>7.2 Manual control If manual control of any actuated component in the execute features is provided, the</p>	<p>There are no changes from the existing MSFIS design.</p> <p>There are no changes from the existing MSFIS design. The ALS MSFIS inputs are prioritized in the logic, with the ESFAS "ALL CLOSE" input having the highest priority.</p>

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
	<p>additional design features in the execute features necessary to accomplish such manual control shall not defeat the requirements of 5.1 and 6.2. Capability shall be provided in the execute features to receive and act upon manual control signals from the sense and command features consistent with the design basis.</p> <p>7.3 Completion of protective action The design of the execute features shall be such that, once initiated, the protective actions of the execute features shall go to completion. This requirement shall not preclude the use of equipment protective devices identified in Clause 4, item k) of the design basis or the provision for deliberate operator interventions. When the sense and command features reset, the execute features shall not automatically return to normal; they shall require separate, deliberate operator action to be returned to normal. After the initial protective action has gone to completion, the execute features may require manual control or automatic control (i.e., cycling) of specific equipment to maintain completion of the safety function.</p> <p>7.4 Operating bypass Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions</p>	<p>Following receipt of an ESFAS close signal, an MSIV or MFIV cannot be opened until the ESFAS signal is no longer present. This is consistent with the logic of the existing system.</p> <p>This requirement is not applicable. The ALS MSFIS does not include any operating bypass functions.</p>

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
	<p>change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:</p> <ul style="list-style-type: none"> a) Remove the appropriate active operating bypass(es). b) Restore plant conditions so that permissive conditions once again exist. c) Initiate the appropriate safety function(s). <p>7.5 Maintenance bypass The capability of a safety system to accomplish its safety function shall be retained while execute features equipment is in maintenance bypass. Portions of the execute features with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (i.e., reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.</p>	<p>If one train of ALS MSFIS is in maintenance bypass, the other train retains the capability to perform the safety function. Administrative controls prevent both trains from being in bypass simultaneously.</p>

NON-PROPRIETARY

IEEE 7-4.3.2-2003 Requirements	IEEE 603-1998	WCNOC Position
<p>8. Power source requirements No requirements beyond IEEE Std 603-1998 are necessary.</p>	<p>8.1 Electrical power sources Those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems. Specific criteria unique to the Class 1E power systems are given in IEEE Std 308-1991.</p> <p>8.2 Non-electrical power sources Non-electrical power sources, such as control-air systems, bottled-gas systems, and hydraulic systems, required to provide the power to the safety systems are a portion of the safety systems and shall provide power consistent with the requirements of this standard. Specific criteria unique to non-electrical power sources are outside the scope of this standard and can be found in other standards.11 [B4, B5]</p> <p>8.3 Maintenance bypass The capability of the safety systems to accomplish their safety functions shall be retained while power sources are in maintenance bypass. Portions of the power sources with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (i.e., reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.</p>	<p>There are no changes from the existing MSFIS design.</p> <p>This requirement is not applicable.</p> <p>If one train of the NK DC bus feeding the MSFIS is in a maintenance bypass, the other MSFIS train retains the capability to perform the safety function. Administrative controls prevent both trains from being in bypass simultaneously.</p>

Enclosure III to WO 07-0028

WCNOC Affidavit for Withholding Proprietary Information from Public Disclosure

- (1) I am Vice President Operations and Plant Manager, Wolf Creek Nuclear Operating Corporation (WCNOC), and as such, I have been specifically delegated the function of reviewing the proprietary information sought to be withheld from public disclosure in WCNOC's submittal of the Matrix of IEEE 7-4.3.2 Requirements to MSFIS Controls Design, and am authorized to apply for its withholding on behalf of WCNOC.
- (2) I am making this Affidavit in conformance with the provisions of 10 CFR Section 2.390 of the Commission's regulations and in conjunction with WCNOC letter WO 07-0028 which includes the Matrix of IEEE 7-4.3.2 Requirements to MSFIS Controls Design accompanying this Affidavit.
- (3) I have personal knowledge of the criteria and procedures utilized by WCNOC in designating information as a trade secret, privileged or as confidential commercial or financial information.
- (4) Pursuant to the provisions of paragraph (b)(4) of Section 2.390 of the Commission's regulations, the following is furnished for consideration by the Commission in determining whether the information sought to be withheld from public disclosure should be withheld.
 - (i) The information sought to be withheld from public disclosure is owned and has been held in confidence by WCNOC.
 - (ii) The information is of a type customarily held in confidence by other organizations and not customarily disclosed to the public. Based on a review of 10 CFR 2.390, the information is held in confidence if it falls in one or more of several types, the release of which might result in the loss of an existing or potential competitive advantage, as follows:
 - (a) The information reveals the distinguishing aspects of a process (or component, structure, tool, method, etc.) where prevention of its use by any other company without license from WCNOC constitutes a competitive economic advantage over other companies.
 - (b) It consists of supporting data, including test data, relative to a process (or component, structure, tool, method, etc.), the application of which data secures a competitive economic advantage, e.g., by optimization or improved marketability.
 - (c) Its use by another company would reduce its expenditure of resources or improve its competitive position in the design, assurance of quality, or licensing a similar product.
 - (d) It is not the property of WCNOC, but must be treated as proprietary by WCNOC according to agreements with the owners of the information.

There are sound reasons behind the WCNOC position which include the following:

- (a) It is information which is marketable in many ways.

- (b) Use by other companies would put WCNOC at a competitive disadvantage by reducing their expenditure of resources at our expense.
 - (c) Each component of proprietary information pertinent to a particular competitive advantage is potentially as valuable as the total competitive advantage. If other companies acquire components of proprietary information, any one component may be the key to the entire puzzle, thereby depriving WCNOC of a competitive advantage.
- (iii) The information is being transmitted to the Commission in confidence and, under the provisions of 10 CFR Section 2.390, it is to be received in confidence by the Commission.
 - (iv) The information sought to be protected is not available in public sources or available information has not been previously employed in the same original manner or method to the best of our knowledge and belief.
 - (v) The proprietary information sought to be withheld in this submittal is the Matrix of IEEE 7-4.3.2 Requirements to MSFIS Controls Design.

The subject information could only be duplicated by competitors if they were to invest time and effort equivalent to that invested by WCNOC provided they have the requisite talent and experience.

Public disclosure of this information is likely to cause substantial harm to the competitive position of WCNOC because it would simplify design and evaluation tasks without requiring a commensurate investment of time and effort.