



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

March 31, 2009

Mr. Rick A. Muench
President and Chief Executive Officer
Wolf Creek Nuclear Operating Corporation
Post Office Box 411
Burlington, KS 66839

SUBJECT: WOLF CREEK GENERATING STATION - ISSUANCE OF AMENDMENT RE:
MODIFICATION OF THE MAIN STEAM AND FEEDWATER ISOLATION
SYSTEM CONTROLS (TAC NO. MD4839)

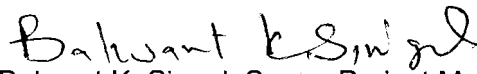
Dear Mr. Muench:

The U.S. Nuclear Regulatory Commission has issued the enclosed Amendment No. 181 to Renewed Facility Operating License No. NPF-42 for the Wolf Creek Generating Station. The amendment consists of changes to the licensing basis for the facility, in response to your application dated March 14, 2007, as supplemented by letters dated April 18, May 9, June 15, August 31, September 12 and 20, October 16, November 16, two letters dated December 14, and December 18, 2007; two letters dated January 18, January 31, February 26 and 28, March 14, April 26, May 14, June 19, and July 31, 2008; and January 16 and 29, and February 17 and 27, 2009.

The amendment revises the licensing basis for the Main Steam and Feedwater Isolation System (MSFIS) controls to incorporate field programmable gate array technology. Other related changes cited in your March 14, 2007, application were previously approved in Amendment No. 174, dated August 28, 2007, Amendment No. 175, dated March 3, 2008, Amendment No. 176, dated March 21, 2008, and Amendment No. 177, dated April 3, 2008.

A copy of our related Safety Evaluation is enclosed. The Notice of Issuance will be included in the Commission's next biweekly *Federal Register* notice.

Sincerely,


Balwant K. Singal, Senior Project Manager
Plant Licensing Branch IV
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-482

Enclosures:

1. Amendment No. 181 to NPF-42
2. Safety Evaluation

cc w/encls: Distribution via Listserv



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

WOLF CREEK NUCLEAR OPERATING CORPORATION

WOLF CREEK GENERATING STATION

DOCKET NO. 50-482

AMENDMENT TO RENEWED FACILITY OPERATING LICENSE

Amendment No. 181
License No. NPF-42

1. The Nuclear Regulatory Commission (the Commission) has found that:
 - A. The application for amendment to the Wolf Creek Generating Station (the facility) Renewed Facility Operating License No. NPF-42 filed by the Wolf Creek Nuclear Operating Corporation (the Corporation), dated March 14, 2007, as supplemented by letters dated April 18, May 9, June 15, August 31, September 12 and 20, October 16, November 16, two letters dated December 14, and December 18, 2007; two letters dated January 18, January 31, February 26 and 28, March 14, April 26, May 14, June 19, and July 31, 2008; and January 16 and 29, and February 17 and 27, 2009, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission's rules and regulations set forth in 10 CFR Chapter I;
 - B. The facility will operate in conformity with the application, as amended, the provisions of the Act, and the rules and regulations of the Commission;
 - C. There is reasonable assurance (i) that the activities authorized by this amendment can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the Commission's regulations;
 - D. The issuance of this license amendment will not be inimical to the common defense and security or to the health and safety of the public; and
 - E. The issuance of this amendment is in accordance with 10 CFR Part 51 of the Commission's regulations and all applicable requirements have been satisfied.

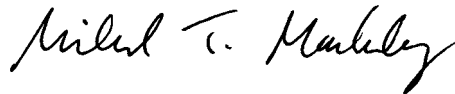
2. Accordingly, the license is amended by changes to the Technical Specifications as indicated in the attachment to this license amendment and Paragraph 2.C.(2) of Renewed Facility Operating License No. NPF-42 is hereby amended to read as follows:

(2) Technical Specifications and Environmental Protection Plan

The Technical Specifications contained in Appendix A, as revised through Amendment No. 181, and the Environmental Protection Plan contained in Appendix B, both of which are attached hereto, are hereby incorporated in the license. The Corporation shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan.

3. The license amendment is effective as of its date of issuance and shall be implemented prior to startup from Refueling Outage 17, which is to be conducted in the fall of 2009. Consistent with the requirements in 10 CFR 50.71(e), implementation shall include revision to the Updated Safety Analysis Report (USAR) to include the effects of all changes made in the facility or procedures described in the USAR and all safety analyses and evaluations performed by the licensee in support of the license amendment.

FOR THE NUCLEAR REGULATORY COMMISSION



Michael T. Markley, Chief
Plant Licensing Branch IV
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to the Renewed Facility
Operating License and
Technical Specifications

Date of Issuance: March 31, 2009

ATTACHMENT TO LICENSE AMENDMENT NO. 181

RENEWED FACILITY OPERATING LICENSE NO. NPF-42

DOCKET NO. 50-482

Replace the following page of the Renewed Facility Operating License No. NPF-42 with the attached revised page. The revised page is identified by amendment number and contains marginal lines indicating the areas of change.

Renewed Facility Operating License

REMOVE

INSERT

-4-

-4-

- (5) The Operating Corporation, pursuant to the Act and 10 CFR Parts 30, 40 and 70, to receive, possess, and use in amounts as required any byproduct, source or special nuclear material without restriction to chemical or physical form, for sample analysis or instrument calibration or associated with radioactive apparatus or components; and
 - (6) The Operating Corporation, pursuant to the Act and 10 CFR Parts 30, 40 and 70, to possess, but not separate, such byproduct and special nuclear materials as may be produced by the operation of the facility.
- C. This renewed operating license shall be deemed to contain and is subject to the conditions specified in the Commission's regulations in 10 CFR Chapter I and is subject to all applicable provisions of the Act and to the rules, regulations, and orders of the Commission, now or hereafter in effect; and is subject to the additional conditions specified or incorporated below:
- (1) Maximum Power Level

The Operating Corporation is authorized to operate the facility at reactor core power levels not in excess of 3565 megawatts thermal (100% power) in accordance with the conditions specified herein.
 - (2) Technical Specifications and Environmental Protection Plan

The Technical Specifications contained in Appendix A, as revised through Amendment No. 181, and the Environmental Protection Plan contained in Appendix B, both of which are attached hereto, are hereby incorporated in the license. The Corporation shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan.
 - (3) Antitrust Conditions

Kansas Gas & Electric Company and Kansas City Power & Light Company shall comply with the antitrust conditions delineated in Appendix C to this license.
 - (4) Environmental Qualification (Section 3.11, SSER #4, Section 3.11, SSER #5)*

Deleted per Amendment No. 141.

*The parenthetical notation following the title of many license conditions denotes the section of the supporting Safety Evaluation Report and/or its supplements wherein the license condition is discussed.

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 181 TO

RENEWED FACILITY OPERATING LICENSE NO. NPF-42

WOLF CREEK NUCLEAR OPERATING CORPORATION

WOLF CREEK GENERATING STATION

DOCKET NO. 50-482

Table of Contents

1.0	Introduction.....	- 1 -
2.0	Regulatory Evaluation.....	- 2 -
2.1	Regulatory Criteria.....	- 2 -
2.2	Precedents	- 3 -
3.0	Technical Evaluation	- 4 -
3.1	System Description.....	- 8 -
3.1.1	Hardware Description	- 10 -
3.1.1.1	Rack	- 13 -
3.1.1.2	Backplane.....	- 14 -
3.1.1.3	Assembly Panel	- 15 -
3.1.1.4	ALS Boards	- 16 -
3.1.1.4.1	Development Process.....	- 17 -
3.1.1.4.2	ALS-101 - Core Logic Board.....	- 27 -
3.1.1.4.3	ALS-301 - Input Boards	- 28 -
3.1.1.4.4	ALS-401 and ALS 411 - Output Boards.....	- 29 -
3.1.1.4.5	ALS-201 - Service & Test Board.....	- 31 -
3.1.1.4.6	ALS-905 - Power Supply Units.....	- 32 -
3.1.1.5	Communications	- 33 -
3.1.1.5.1	Communications from MSFIS to Other Safety-Related Equipment	- 34 -
3.1.1.5.2	Communications with Non-safety Systems	- 37 -
3.1.1.5.3	Communications between Separate Class 1E Divisions	- 38 -
3.1.1.5.4	Independence of Safety Signal Path within a Division.....	- 38 -
3.1.1.5.5	Internal Communications and Bus Structure	- 38 -
3.1.1.6	Staff Guidance in DI&C-ISG-04.....	- 40 -
3.1.1.6.1	DI&C-ISG-04, Section 1 - Interdivisional Communications	- 40 -
3.1.1.6.2	DI&C-ISG-04, Section 2 - Command Prioritization	- 41 -
3.1.1.6.3	DI&C-ISG-04, Section 3 - Multidivisional Control and Display Stations	- 41 -
3.2	Programmable Hardware.....	- 41 -
3.2.1	Life Cycle Planning Documentation	- 42 -
3.2.1.1	Management Plan.....	- 42 -
3.2.1.2	Software Development Plan.....	- 42 -
3.2.1.3	Quality Assurance Plan.....	- 44 -
3.2.1.4	Software Integration Plan.....	- 46 -
3.2.1.5	Software Installation Plan.....	- 47 -
3.2.1.6	Software Maintenance Plan	- 48 -
3.2.1.7	Training Plan.....	- 49 -
3.2.1.8	Software Operations Plan	- 50 -
3.2.1.9	Software Safety Plan	- 50 -
3.2.1.9.1	Failure Modes and Effects Analysis	- 51 -
3.2.1.10	Verification and Validation	- 52 -
3.2.1.10.1	Verification and Validation Plans	- 52 -
3.2.1.10.2	Verification and Validation Report	- 53 -
3.2.1.10.3	Requirements Traceability Matrix.....	- 54 -
3.2.1.11	Configuration Management Plan.....	- 54 -
3.2.1.12	Test Plan.....	- 57 -
3.2.2	Design Outputs.....	- 58 -
3.2.2.1	Requirements Specification.....	- 58 -
3.2.2.2	Software Architecture Description	- 59 -
3.2.2.3	Software Design Description.....	- 60 -

3.2.2.4	Software Design Review	- 60 -
3.2.2.5	System Build Documents	- 61 -
3.2.2.6	Installation Configuration Tables	- 61 -
3.3	System Qualifications	- 62 -
3.3.1	Environmental Qualification of System	- 62 -
3.3.1.1	Equipment Description and Testing	- 63 -
3.3.1.2	Temperature and Humidity Testing	- 65 -
3.3.1.3	Radiation Withstand Testing	- 66 -
3.3.1.4	Electromagnetic Compatibility Testing	- 66 -
3.3.1.4.1	EMC Emissions Testing	- 68 -
3.3.1.4.2	EMC Susceptibility Testing	- 69 -
3.3.1.4.3	Surge Withstand Testing	- 70 -
3.3.1.4.4	Electrostatic Discharge (ESD) Withstand Testing	- 71 -
3.3.1.4.5	Class 1E to Non-1E Isolation Testing	- 72 -
3.3.1.5	Seismic Withstand Testing	- 73 -
3.3.1.5.1	Pre-seismic Inspection and Operability Check	- 73 -
3.3.1.5.2	Resonance Search Test	- 73 -
3.3.1.5.3	Qualification-level Multiple-Frequency Tests	- 74 -
3.3.1.5.4	Post-seismic Baseline Test and Operability Check	- 75 -
3.3.2	Response Time	- 75 -
3.3.3	Diversity and Defense-in-Depth	- 76 -
3.3.4	Cyber Security	- 79 -
3.3.5	Review of System and IEEE 603 Requirement	- 81 -
3.3.5.1	IEEE 603-1991 Clause 4 - Safety System Designation	- 81 -
3.3.5.2	IEEE 603-1991 Clause 5 - Safety System Criteria	- 81 -
3.3.5.2.1	IEEE 603-1991 Clause 5.1 - Single-Failure Criterion	- 81 -
3.3.5.2.2	IEEE 603-1991 Clause 5.2 - Completion of Protective Action	- 82 -
3.3.5.2.3	IEEE 603-1991 Clause 5.3 - Quality	- 82 -
3.3.5.2.4	IEEE 603-1991 Clause 5.4 - Equipment Qualification	- 82 -
3.3.5.2.5	IEEE 603-1991 Clause 5.5 - System Integrity	- 83 -
3.3.5.2.6	IEEE 603-1991 Clause 5.6 - Independence	- 84 -
3.3.5.2.7	IEEE 603-1991 Clause 5.7 - Capability for Test and Calibration	- 86 -
3.3.5.2.8	IEEE 603-1991 Clause 5.8 - Information Displays	- 87 -
3.3.5.2.9	IEEE 603-1991 Clause 5.9 - Control of Access	- 88 -
3.3.5.2.10	IEEE 603-1991 Clause 5.10 - Repair	- 89 -
3.3.5.2.11	IEEE 603-1991 Clause 5.11 - Identification	- 89 -
3.3.5.2.12	IEEE 603-1991 Clause 5.12 - Auxiliary Features	- 89 -
3.3.5.2.13	IEEE 603-1991 Clause 5.13 - Multi-Unit Stations	- 90 -
3.3.5.2.14	IEEE 603-1991 Clause 5.14 - Human Factors Considerations	- 90 -
3.3.5.2.15	IEEE 603-1991 Clause 5.15 - Reliability	- 90 -
3.3.5.3	IEEE 603-1991 Clause 6 - Sense and Command Features Functional and Design Requirements	- 91 -
3.3.5.3.1	IEEE 603-1991 Clause 6.1 - Automatic Controls	- 91 -
3.3.5.3.2	IEEE 603-1991 Clause 6.2 - Manual Control	- 92 -
3.3.5.3.3	IEEE 603-1991 Clause 6.3 - Interaction Between the Sense and Command Features and Other Systems	- 92 -
3.3.5.3.4	IEEE 603-1991 Clause 6.4 - Derivation of System Inputs	- 93 -
3.3.5.3.5	IEEE 603-1991 Clause 6.5 - Capability for Testing and Calibration	- 93 -

3.3.5.3.6	IEEE 603-1991 Clause 6.6 - Operating Bypasses.....	- 94 -
3.3.5.3.7	IEEE 603-1991 Clause 6.7 - Maintenance Bypass.....	- 94 -
3.3.5.3.8	IEEE 603-1991 Clause 6.8 – Setpoints.....	- 94 -
3.3.5.4	IEEE 603-1991 Clause 7 - Execute Feature - Functional and Design Requirements	- 95 -
3.3.5.4.1	IEEE 603-1991 Clause 7.1 - Automatic Control.....	- 95 -
3.3.5.4.2	IEEE 603-1991 Clause 7.2 - Manual Control	- 95 -
3.3.5.4.3	IEEE 603-1991 Clause 7.3 - Completion of Protective Action	- 96 -
3.3.5.4.4	IEEE 603-1991 Clause 7.4 - Operating Bypasses.....	- 96 -
3.3.5.4.5	IEEE 603-1991 Clause 7.5 - Maintenance Bypass.....	- 96 -
3.3.5.5	IEEE 603-1991 Clause 8 - Power Source Requirements	- 97 -
3.3.6	Review IEEE 7-4.3.2 Requirements.....	- 97 -
3.3.6.1	IEEE 7-4.3.2 Clause 4 - Safety System Design Basis	- 97 -
3.3.6.2	IEEE 7-4.3.2 Clause 5 - Safety System Criteria	- 97 -
3.3.6.2.1	IEEE 7-4.3.2 Clause 5.1 - Single-Failure Criterion	- 97 -
3.3.6.2.2	IEEE 7-4.3.2 Clause 5.2 - Completion of Protective Action	- 97 -
3.3.6.2.3	IEEE 7-4.3.2 Clause 5.3 – Quality	- 98 -
3.3.6.2.4	IEEE 7-4.3.2 Clause 5.4 - Equipment Qualification	- 101 -
3.3.6.2.5	IEEE 7-4.3.2 Clause 5.5 - System Integrity	- 103 -
3.3.6.2.6	IEEE 7-4.3.2 Clause 5.6 – Independence	- 104 -
3.3.6.2.7	IEEE 7-4.3.2 Clause 5.7 - Capability for Test and Calibration.....	- 105 -
3.3.6.2.8	IEEE 7-4.3.2 Clause 5.8 - Information Displays	- 105 -
3.3.6.2.9	IEEE 7-4.3.2 Clause 5.9 - Control of Access.....	- 106 -
3.3.6.2.10	IEEE 7-4.3.2 Clause 5.10 – Repair	- 106 -
3.3.6.2.11	IEEE 7-4.3.2 Clause 5.11 – Identification	- 106 -
3.3.6.2.12	IEEE 7-4.3.2 Clause 5.12 - Auxiliary Features	- 106 -
3.3.6.2.13	IEEE 7-4.3.2 Clause 5.13 - Multi-Unit Stations.....	- 107 -
3.3.6.2.14	IEEE 7-4.3.2 Clause 5.14 - Human Factors Considerations.....	- 107 -
3.3.6.2.15	IEEE 7-4.3.2 Clause 5.15 – Reliability	- 107 -
3.3.6.3	IEEE 7-4.3.2 Clause 6 - Sense and Command Features	- 107 -
3.3.6.4	IEEE 7-4.3.2 Clause 7 - Execute Features.....	- 108 -
3.3.6.5	IEEE 7-4.3.2 Clause 8 - Power Source Requirements	- 108 -
4.0	NRC Findings	- 108 -
4.1	Summary of Regulatory Compliance.....	- 108 -
4.2	Future Use of ALS Platform	- 110 -
4.2.1	ALS Process Documentation	- 110 -
4.2.2	ALS Hardware and Programming Documentation.....	- 111 -
5.0	State Consultation.....	- 112 -
6.0	Environmental Consideration	- 112 -
7.0	Conclusion.....	- 113 -
8.0	References	- 113 -



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 181 TO

RENEWED FACILITY OPERATING LICENSE NO. NPF-42

WOLF CREEK NUCLEAR OPERATING CORPORATION

WOLF CREEK GENERATING STATION

DOCKET NO. 50-482

1.0 INTRODUCTION

By application dated March 14, 2007 (Reference 1), as supplemented by letters dated April 18, 2007 (Reference 2), May 9, 2007 (Reference 3), June 15, 2007 (Reference 4), August 31, 2007 (Reference 5), September 12, 2007 (Reference 6), September 20, 2007 (Reference 7), and October 16, 2007 (Reference 8), November 16, 2007 (Reference 9; later withdrawn); two letters dated December 14, 2007 (References 10 and 11), December 18, 2007 (Reference 12); two letters dated January 18, 2008 (References 13 and 14), January 31, 2008 (Reference 15), February 26, 2008 (Reference 16), February 28, 2008 (Reference 17), March 14, 2008 (Reference 18), April 26, 2008 (Reference 19), May 14, 2008 (Reference 20), June 19, 2008 (Reference 21), July 31, 2008 (Reference 22); January 16, 2009 (Reference 23), January 29, 2009 (Reference 24), February 17, 2009 (Reference 25), and February 27, 2009 (Reference 26), Wolf Creek Nuclear Operating Corporation (WCNOC, the licensee), requested changes to the Technical Specifications (TSs) for Wolf Creek Generating Station (WCGS).

The proposed changes would allow replacement of main steam isolation valves (MSIVs) and associated actuators, main feedwater isolation valves (MFIVs) and associated actuators, and replacement of the Main Steam and Feedwater Isolation System (MSFIS) controls. The replacement of the MSIVs and associated actuators, the MFIVs and associated actuators, and the TS changes were addressed in the U.S. Nuclear Regulatory Commission (NRC) staff Safety Evaluations (SEs) related to Amendment No. 174, dated August 28, 2007 (Reference 143), Amendment No. 175, dated March 3, 2008 (Reference 144), Amendment No. 176, dated March 21, 2008 (Reference 145), and Amendment No. 177, dated April 3, 2008 (Reference 146). This SE addresses the replacement of the MSFIS controls.

The replacement MSFIS controls proposed the use of field programmable gate array (FPGA) technology. The original application included only a brief description of the FPGA and the system that used the FPGA; however, on April 18, 2007 (Reference 2), the licensee submitted additional documentation. The additional documentation was considered during an earlier acceptance review, and was found to be insufficient. On May 17, 2007 (Reference 141), the NRC staff provided WCGS a list of documentation required for the NRC staff to determine if the specification, design, development, test, production, and verification and validation (V&V) processes were of sufficient high quality to result in a product useable in a safety-related

application at a nuclear power plant. On June 15, 2007 (Reference 4), the licensee provided documentation in response to the NRC staff's required documentation list of May 17, 2007. Additional information was provided by the licensee in supplemental letters (References 3 through 26 and 148). The supplemental information did not expand or change the scope of the application as originally noticed, and did not change the NRC staff's original proposed no significant hazards consideration determination published in the *Federal Register* on June 19, 2007 (72 FR 33785). The NRC staff conducted on-site audits between May 12-18, 2008, and December 10-11, 2008.

2.0 REGULATORY EVALUATION

2.1 Regulatory Criteria

The NRC's NUREG-0800, "Standard Review Plan (SRP) for the Review of Safety Analysis Reports for Nuclear Power Plants," Revision 5, dated March 2007 (Reference 87), defines the acceptance criteria for this review. Specifically, SRP Chapter 7, "Instrumentation and Controls," addresses the requirements for instrumentation and control (I&C) systems in light-water nuclear power plants. The procedures for review of digital systems are principally contained within SRP Chapter 7, Appendices 7.0-A, 7.1-A; Sections 7.1, 7.8, and 7.9; and Branch Technical Positions (BTPs) SRP BTP-14, SRP BTP-17, and SRP BTP-21. SRP Chapter 7, Appendix 7.1-C and Appendix 7.1-D; and Sections 7.2 through 7.7 provide additional criteria that the NRC staff applied in the review.

The suitability of a digital platform for use in safety systems depends on the quality of its components; quality of the design process; and system implementation aspects such as real-time performance, independence, and online testing. Because this equipment is being supplied as Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, Appendix B, qualified equipment, the NRC staff evaluated the licensee's submittals in accordance with the provisions of Institute of Electrical and Electronics Engineers (IEEE) Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Reference 108), and IEEE Standard 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Reference 120), as well as the guidance contained in SRP Chapter 7.

The NRC staff considered the codes, criteria, and standards that follow to evaluate the replacement MSFIS controls.

The following acceptance criteria and guidelines for reviewing an Emergency Safety Features Actuation System (ESFAS) or an engineered safety features control system, such as the proposed MSFIS system, are identified in SRP Chapter 7, Section 7.3:

- 10 CFR 50.55a(a)(1), requires that "[s]tructures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed."
- 10 CFR 50.55a(h), "Protection and safety systems," approves the 1991 version of IEEE Standard 603, "IEEE Standard Criteria for Safety Systems for Nuclear

Power Generating Stations,” for incorporation by reference including the correction sheet dated January 30, 1995.

- 10 CFR 50, Appendix A, General Design Criteria for Nuclear Power Plants (GDC):
 - GDC 1, “Quality standards and records.”
 - GDC 2, “Design basis for protection against natural phenomena.”
 - GDC 4, “Environmental and dynamic effects design bases.”
 - GDC 10, “Reactor design.”
 - GDC 13, “Instrumentation and control.”
 - GDC 15, “Reactor coolant system design.”
 - GDC 16, “Containment design.”
 - GDC 19, “Control room.”
 - GDC 20, “Protection systems functions.”
 - GDC 21, “Protection system reliability and testability.”
 - GDC 22, “Protective system independence.”
 - GDC 23, “Protection system failure modes.”
 - GDC 24, “Separation of protection and control systems.”
 - GDC 29, “Protection against anticipated operational occurrences.”

Industry standards, documents, and reports use the word “requirements” to denote provisions that must be implemented to ensure compliance with the corresponding document. Additionally, these standards, documents, and reports provide guidance or recommendations that need not be adopted by the user to ensure compliance with the corresponding document, and the optional items are not designated as “requirements”. The word “requirement” is used throughout the instrumentation and control discipline. However, licensee or vendor documentation of conformance to the “requirements” provided in industry standards, documents, and reports referenced in this SE only constitutes conformance with NRC regulatory requirements insofar as endorsed by the NRC. Furthermore, use of the word “requirements” in these documents does not indicate that the “requirements” are NRC regulatory requirements.

2.2 Precedents

This is the first time an FPGA has been used in a safety-related application in nuclear power plants and, therefore, a precedent does not exist. However, as discussed in the NRC staff May 29, 2007, letter concerning the acceptance review (Reference 142), FPGA-based applications, like microprocessor (μ P)-based applications, are programmed to perform the desired safety functions and, therefore, undetected errors in design and implementation can cause these systems to exhibit unexpected behavior; the performance of digital systems over the entire range of input conditions cannot generally be inferred from testing of a sample of input conditions; and the use of inspections, type testing, and acceptance testing of digital systems and components does not alone accomplish design qualification at high confidence levels. For these reasons, the review of this application will be similar to the review of a traditionally programmed μ P application. The NRC staff used SRP Chapter 7, “Instrumentation and Controls,” as the review guidance to determine that a high-quality development process that incorporates a disciplined specification and implementation of design requirements was used to develop the MSFIS.

3.0 TECHNICAL EVALUATION

The WCGS MSFIS provides valve control equipment for main steam and feedwater automatic isolation and manual valve control. Separate divisions provide redundant WCGS-MSFIS equipment. The two divisions maintain electrical and physical separation of equipment via dedicated Class 1E circuits in a point-to-point manner.

The WCGS has four steam generators (SGs). Each SG has one MSIV in the main steam system. Each SG also has one MFIV in the condensate and feed system. These valves isolate the non-safety-related portions from the safety-related portions of the plant systems. The WCGS-MSFIS is responsible to perform this isolation function, when required, such that no single failure can prevent any valve from performing its required function.

This FPGA-based system will replace the existing safety-related electronic MSFIS controls to perform the control functions of the MSIVs and MFIVs.

This system does not generate the ESFAS isolation signal, but transfers the isolation signal to the valves. The automated ESFAS command is generated from the Solid State Protection System (SSPS), and manual open or close signals are generated from switches in the control room. The SSPS provides the inputs to the MSFIS from a separate slave relay for each of the MSIVs and MFIVs. Each slave relay provides four contacts into the MSFIS, one contact for each valve. The four contacts from a particular slave relay for either the MSIVs or MFIVs shall be evaluated using signal logic for actuation (2-out-of-4 vote). The 2-out-of-4 vote shall be required for a valid ESFAS command. The ESFAS command shall place the CLOSE output state for the particular valve based on the contact inputs from the SSPS slave relay, and the particular system MSIV or MFIV. Note: Under normal operating conditions, the four ESFAS commands will come in at the same time, as they are derived from the same slave relay coil.

The WCGS-MSFIS enclosure pair, containing one set of MSIV and MFIV control circuitry, is separate, but otherwise functionally identical. Each enclosure and the internal electronics maintain divisional segregation. The CS Innovations 6101-00002, "MSFIS System Specification," Revision 0.98, dated June 9, 2007 (References 27 and 28), refers to these two divisions as "Trains" - "A and B" within "Separation Groups" - "1 and 4," respectively. The independent functions that are replicated between the divisions provide redundancy for the safety-related valve isolation (closure) function. One WCGS-MSFIS is to be installed into the existing cabinet "SA075A." Likewise, the second WCGS-MSFIS is to be installed into the existing cabinet "SA075B." This installation will reuse existing infrastructure to include: 1) mechanical structures to mount racks and components, 2) terminal blocks within the cabinets, and 3) field-wiring external to the cabinets.

Figure 1 depicts the relationship between the WCGS-MSFIS and other equipment. This figure is copy of "Figure 2: MSFIS Input/Output Logical Overview" from References 27 and 28. The two divisions of WCGS-MSFIS equipment are shown within the boxes labeled "SA075A Sep. Grp. 1" and "SA075B Sep. Grp. 4." The Main Control Board (MCB) is the operator control panel.

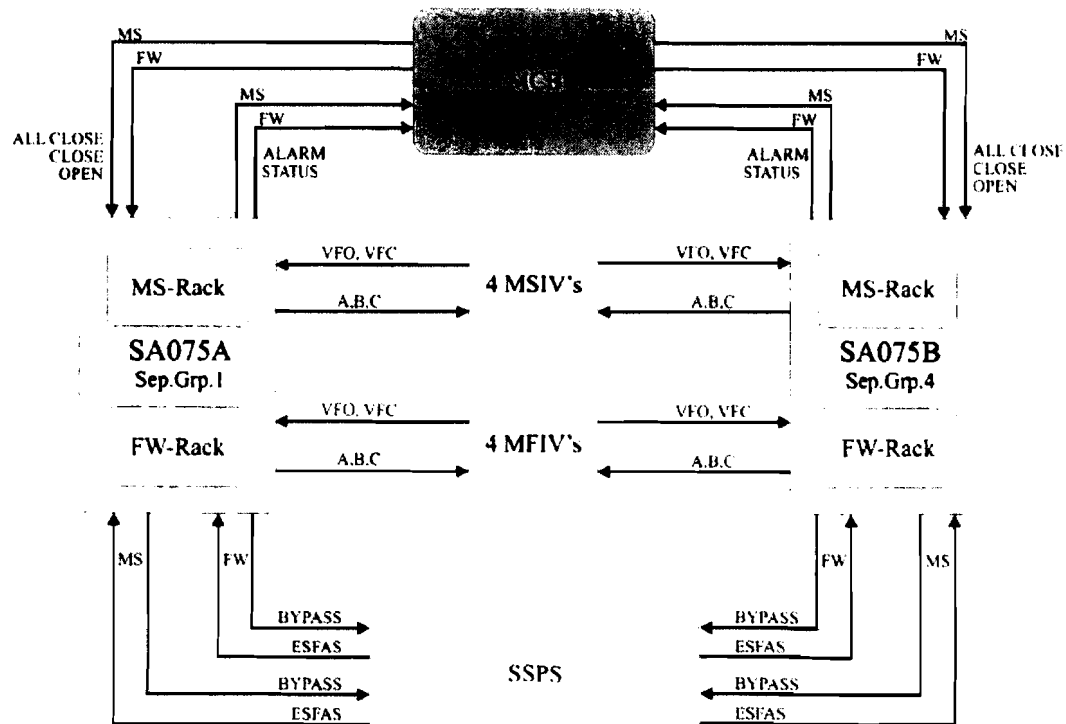


Figure 1 - Context of MSFIS Equipment

Because use of an FPGA in a safety-related application in nuclear power plants is a first-of-a-kind application, this section provides a short and simplified description of FPGA technology as used by the CS Innovations Advanced Logic System (ALS), and a differentiation between FPGA and μ P-based systems.

An FPGA is a collection of logic elements such as “and” gates, “or” gates, bi-stable flip-flops, registers, inverters, adders, and other digital logic. Some logic elements are combinations of individual gates. The field programmable portion of the name refers to the ability to determine the functionality of the FPGA by the end user, in contrast to a μ P chip, whereas the functionality is determined only by the manufacturer.

The FPGA logic elements are arranged in an array of unprogrammed connections. This could be compared to a series of similar but unconnected discrete logic elements on a breadboard, where the functionality of the overall circuit is undetermined until the connections are made. The FPGA also contains a series of reconfigurable interconnects that allow the logic elements to be “wired together.” The connections between the logic elements are of two basic types, the “flash” type where the connection is made in a similar manner as flashing an electronically erasable programmable read-only memory, or the “anti-fuse” type, where the connection is burned open in a manner similar to traditional programmable read-only memory. The flash type FPGA can be reprogrammed; whereas the anti-fuse type can be programmed only one time, and then must be replaced rather than reprogrammed.

Once the desired functionality of a circuit is determined, that functionality is described using a hardware description language (HDL). This language uses standard text-based expressions for the structure and behavior of the desired electronic system. HDL can be considered a method of refining the natural language requirements within the specification into a more precise set of formatted requirements. This is somewhat similar to "formal methods," where natural language requirements are converted into mathematically or logic-based specifications. Use of HDL allows a simulation program to model the desired circuit before it is created physically. The simulation program is generally called a "test bench." At this point, because it is only the HDL code that is being simulated, the test validates the designer's intent rather than actual circuit.

The next step in the design process is the synthesis of the circuit. A software program called a synthesizer will determine the required hardware logic operations from the HDL statements, and produce a "netlist," that could be considered a proposed schematic of the hardware circuit. The proposed circuit, as described by the netlist, can again be tested for proper operation by simulation of the circuit, and a determination can be reached that the circuit will perform the needed functions. After this determination is made, the synthesized circuit undergoes a place-and-route operation, where each proposed logic element will be assigned to an actual logic element within the FPGA, and the interconnection of those logic elements will be determined. This is performed using another software tool developed by the FPGA manufacturer for that particular FPGA. The place and route is device-specific, and translates the hardware description into device-specific characteristics. Once again, the circuit as described can be tested using a specifically designed "workbench" to verify proper operation. One output of the place-and-route tool is a flash or burn list, that will be used to actually program the FPGA into the desired functionality.

Programmed FPGAs as used in the MSFIS are, by nature, finite state machines. A finite state machine is one where within each state, for each input event, there can be only one transition from the present state to the new state. A simplistic example of this may be a two input "or" gate. With both inputs at "0," the output is "0." If one of the inputs changes to "1," there is only one way for the internal circuits to react to change the output to "1." There is no manner in which an undetermined state (i.e., an output of "1/2") can be reached without a hardware failure. However, FPGA applications may also contain many interconnected or independent state machines, depending on the overall functionality required. As an example, on a trip decision process, one state machine holding sensor inputs may feed the state machine making the comparison with the setpoint and making the trip decision, and that may feed another state machine that sends the trip decision to the final actuators. The example chain of state machines, as described, is not representative of the MSFIS application. An example of trip decision for valve control, based upon MSFIS, is shown below in Figure 2.

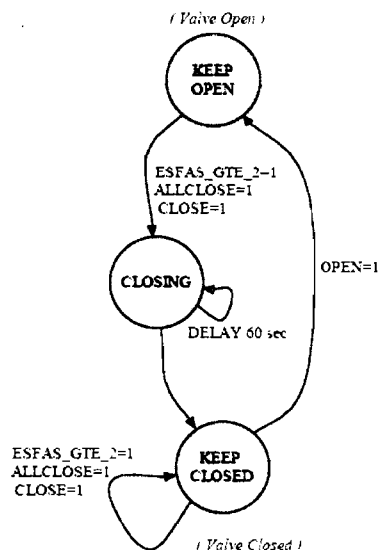


Figure 2 - Example Valve Controller Finite State Machine

Under normal conditions where the valve has been commanded open, the MSFIS FPGA valve controller finite state machine will remain in the “Keep Open” state until one of the closure signals is received. These are the automated ESFAS isolation signal from the SSPS, or the “All Close” or “Close” signal from the operator. Any of these signals will cause the valve controller finite state machine to enter the “Closing” state. The “Closing” state energizes the solenoid outputs to cause the valve to close. As the valves close, the “Closing” state implements a 60-second time delay to lock in the protective action and allow the valves to reach a fully closed position. Once the 60-second time delay expires, this event causes the valve controller finite state machine to enter the “Keep Closed” state. The state machine now remains in the “Keep Closed” state waiting for an open signal, and does nothing until an “Open” signal is received from the operator. Upon the open event, the valve controller finite state machine enters the “Keep Open” state that energizes the proper solenoid output to cause the valve to open and remain open. For the MSFIS, there are other inputs, such as the system reset, ALS Service Unit (ASU) connection status, and the bypass signals, that are not shown in Figure 2. A parallel state machine, unconnected to the trip process, may be monitoring the ASU port and the operate/bypass switches, in order to send an alarm when the ASU connection is active and provide remote status to the operator of the equipment bypass condition. These FPGA circuits similarly just sit and wait in a defined state until the next input that requires a response is received. Some circuit state machines, such as sampling sensor values, could occur frequently, and others, such as transmitting a changing the valve position, could be infrequent events.

Programming using HDL has the same potential for issues as the use of any other programming language, in that there may be errors in the program that require as well as test of the programming, to detect. The programming also has the same configuration control, quality assurance and other issues as exist with traditional programming and for this reason, the NRC staff review of the use of HDL is similar to the NRC staff review required with the use of a more traditional programming language. In both cases, because programming errors can occur, a well-defined high-quality design process, and a rigorous V&V effort are needed to provide reasonable assurance that the resulting system will perform its safety function in a predictable

and reliable manner. While the less complex nature of state machines and FPGAs may make this determination easier than for traditional μ P-based software programming, the reasonable assurance determination is still required.

A μ P-based system operates on a very different principle. In general, a μ P operates on a continuous loop of instructions. This loop may first receive each sensor input and store that value in memory. After each input is received, the setpoint must be retrieved from memory and compared to the sensor input. A determination is made on whether the sensor value or the setpoint is higher, and the trip decision is made. This trip decision is then sent to the voting logic. These steps are repeated for each sensor. The μ P then may check all communications inputs, and prepare output messages. At some point in the loop the diagnostic routines are run, and when diagnostic time runs out, the present test point is stored in memory for test resumption at the end of the next cycle. A watchdog timer may now be reset, and the loop of instructions is started again. This entire process may be performed under the direction of an operating system. Unplanned interruption of any portion of this loop will stop the entire loop, and an error in the instructions may send the μ P into an undetermined state. The internal working of a μ P is proprietary; however, due to the wide use of some μ Ps, the proper operation of the μ P can be reasonably assured. This is in contrast to the transparency of FPGAs, where the internal working is readily available as a schematic, and the proper operation can be determined by examination of that schematic.

3.1 System Description

The CS Innovations MSFIS product uses generic ALS boards; however, the programming in these boards is application-specific. The replacement MSFIS will consist of application-specific individual boards mounted in racks and these racks will be installed into existing enclosures. The system consists of FPGA-based electronics and an assembly panel installed within existing enclosures. The enclosures' mechanical structures and existing field wiring and terminal blocks remain unmodified. The ALS boards are printed circuit boards (PCBs) that contain solid-state electronics and digital electronics, and the digital electronics use flash-based FPGAs. CS Innovations controls the design, configuration, and manufacture of the ALS boards and the design, configuration, and programming of the FPGAs. CS Innovations is a 10 CFR Part 50, Appendix B, supplier and developed the ALS platform as Class 1E compliant equipment. An MSFIS isolation valve controller is the first application of the ALS platform. An example of a generic ALS platform is provided below in Figure 3. It should be noted that the MSFIS does not use a communications board, and no communications board or use of a communications board has been reviewed or approved by the NRC staff.

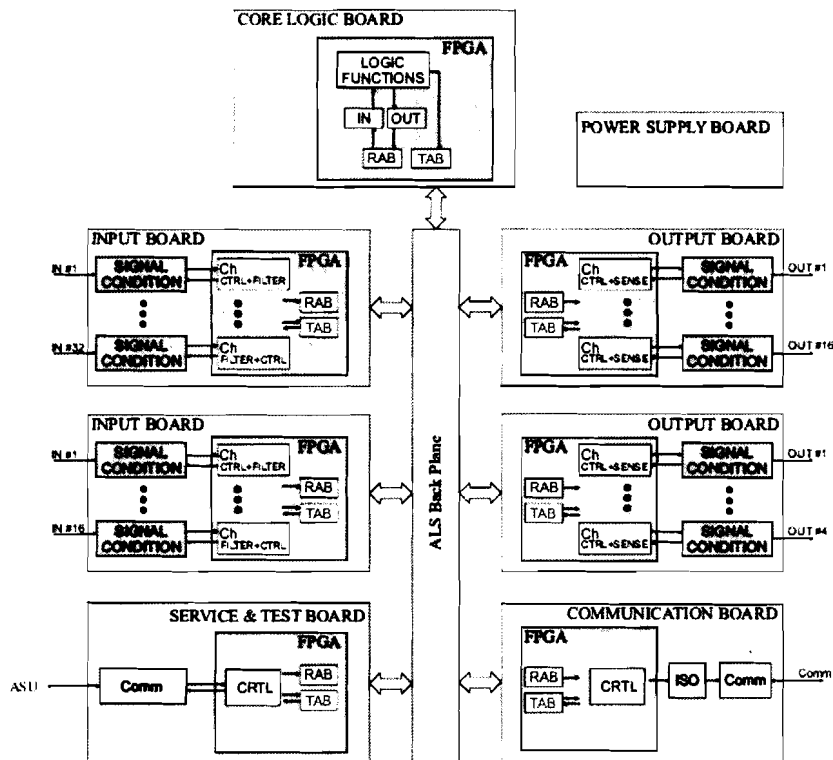


Figure 3 - Generic ALS Platform Architecture

Within each enclosure, the MSFIS includes two isolation valve controllers. These controllers are the MSIV Controller and MFIV Controller. References 27 and 28 refer to these two isolation valve controllers as the “MS-Rack” and “FW-Rack,” respectively. Within each enclosure, MSIV control daughter boards are installed into one backplane and MFIV control daughter boards are installed into a second backplane. The separate backplanes are installed in separate racks. This configuration maintains segregation of the MSIV control function from the MFIV control function within the enclosure.

Application-specific cabling provides signals from the racks to an assembly panel. The assembly panel connects to the existing terminal blocks/field wiring. One assembly panel supports both isolation valve controllers. The assembly panel provides fuses and fuse holders.

The modification preserves the separation, cabinets and field wiring, as it presently exists. Legacy plant interfaces are maintained as part of the WCGS “Specification J-105A(Q) for Replacement MSFIS System,” Revision 5, dated February 16, 2009, enclosure to WCNO letter dated February 17, 2009 (Reference 25). The only new plant interfaces are the cabinet summary alarm and valve actuator interfaces. Because the controller racks are identical, except for nameplates and input/output signal sources/destinations, and there is continuity of legacy interfaces, this SE focuses on the suitability of the ALS platform as a single isolation valve controller of a division.

MSIV Division A and MSIV Division B, or MFIV Division A and MFIV Division B, control the isolation valves, MSIV#1, MSIV#2, MSIV#3, and MSIV#4, or MFIV#1, MFIV#2, MFIV#3, and

MFIV#4, respectively. Figure 4 - Simplified Context for Control of One Valve shows the relationship between an isolation valve controller rack and the control and monitoring signals for a single valve. Except for the all close, alarm, and troubleshooting port signals, each signal shown in Figure 4 exists per valve. Each of the all close, alarm, and troubleshooting port signals exist only one per isolation valve controller rack.

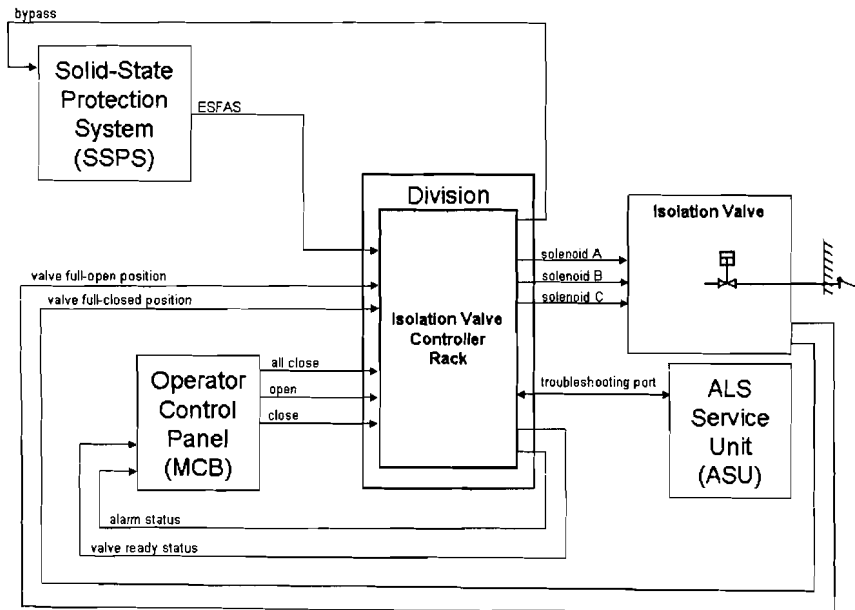


Figure 4 - Simplified Context for Control of One Valve

3.1.1 Hardware Description

The safety function of the MSFIS is to receive isolation actuation signals for the main steam and feedwater systems from the SSPS, and to send closure signals to the individual main steam and feedwater valves. For automatic valve closure, the MSFIS receives four ESFAS signals from the SSPS, and, for manual valve operation, the MSFIS receives operator switch signals from operator control panels. For operator control of the valves, the operator control panel provides 1) an “All Close” switch to close all main steam or feedwater valves per division, 2) a “Close” switch for each individual valve of both divisions, and 3) an open switch for each individual valve of both divisions. In response to automatic or manual signals, the MSFIS energizes a valve’s solenoid A, B, and C to change its position. The MSFIS also monitors the position of each valve with the valve full-open and valve full-closed position signals that each valve provides.

The MSFIS provides to operators a summary alarm status for each cabinet that indicates whether the MSFIS has detected a self-test failure, and a valve-ready status per valve that indicates the ability to control the valve. The MSFIS provides to the SSPS a bypass status per valve that enables ESFAS test circuitry and will prevent the MSFIS from energizing a valve’s solenoids in response to SSPS or operator control panel signals while in bypass. The MSFIS provides diagnostics, maintenance, and troubleshooting data to the ASU as serial communications over the troubleshooting port.

The MSFIS application uses six ALS platform board types to perform five platform functions. Figure 5 - MSFIS Isolation Valve Controller Rack Architecture, shows each of the five ALS platform board types and the communications paths for each board. These are: 1) ALS-101 Core Logic Board performs application-specific control logic, 2) ALS-301 Input Boards acquire system input signals, 3) ALS-401 and ALS 411 Output Boards generate system output signals, 4) ALS-201 Service & Test Board provides maintenance and troubleshooting support, and 5) ALS-905 Power Supply Boards generate power.

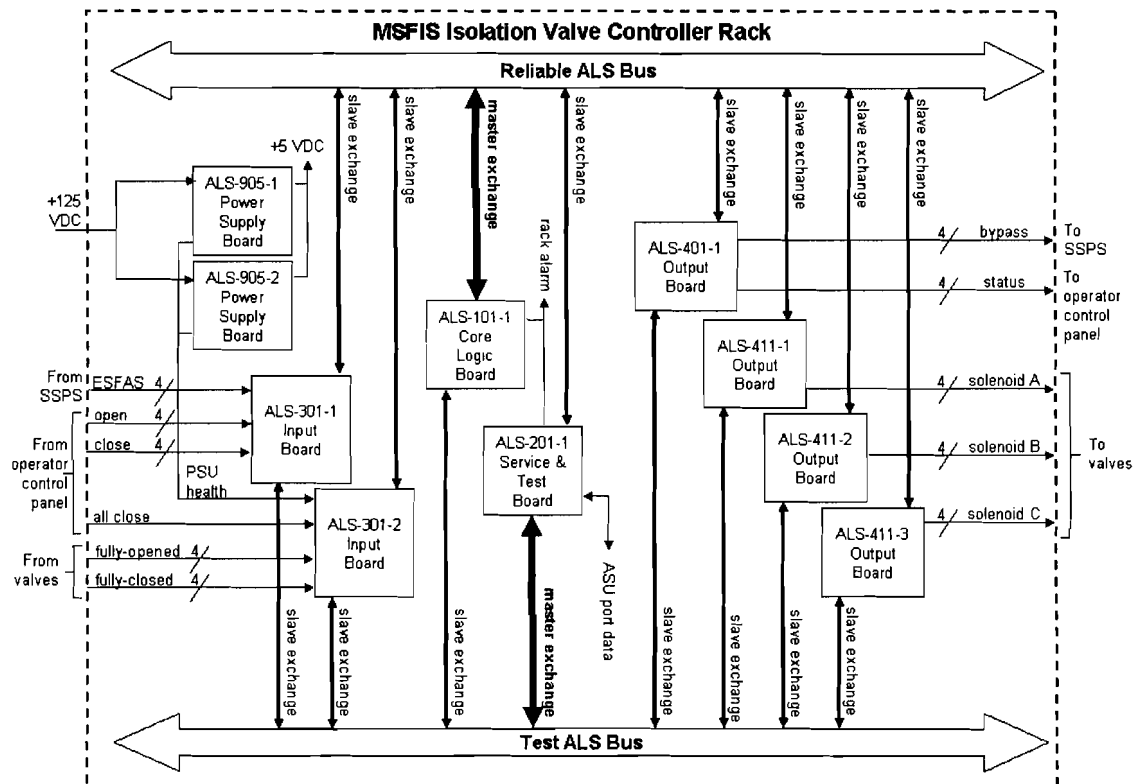


Figure 5 - MSFIS Isolation Valve Controller Rack Architecture

Figure 6 - MSFIS Physical Block Diagram with Signal Flow, shows the data exchanged between the ALS-101 board and other boards within an MSFIS isolation valve controller rack. Figure 6 is an extract of References 27 and 28, "Figure 15: Signal flow between ALS boards in MSFIS-configuration."

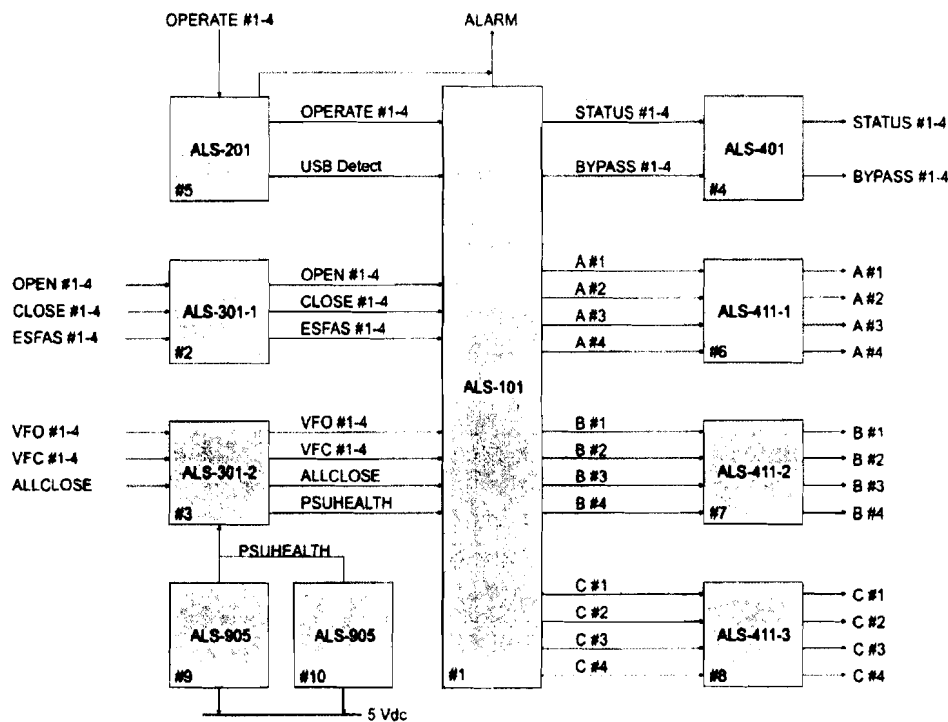


Figure 6 - MSFIS Physical Block Diagram with Signal Flow

The Core Logic Board (ALS-101) performs the MSFIS application-specific control logic. The Core Logic Board is responsible for the MSFIS safety functions and is the bus master for the safety signal bus. The Core Logic Board acquires MSFIS input statuses from the Input Boards and the Service & Test Board, implements the safety function logic, and directs control of MSFIS outputs via the Output Boards. This cycle is repeated at fixed intervals (once every 10 milliseconds for MSFIS) within a fixed time frame that is allocated to a board access (100 microseconds per board access for MSFIS). The ALS platform provides a dedicated and independent serial bus for the safety signal path. This safety signal bus is the Reliable ALS Bus (RAB) that is described in greater detail in Section 3.1.1.5.5 of this SE.

The two input boards (ALS-301-1 and ALS-301-2) condition MSFIS input signals and make status available to the Core Logic Board over the safety signal bus, the RAB. The Output Boards (ALS-401-1, ALS-411-1, ALS-411-2, and ALS-411-3) receive command signals from the Core Logic Board over the safety signal bus and condition MSFIS output signals to reflect the commanded state.

The Service & Test Board (ALS-201) provides maintenance and troubleshooting support. The Service & Test Board has operate/bypass switches and makes their status available to the Core Logic Board over the safety signal bus. When an ASU is connected, the Service & Test Board can provide solenoid test requests to the Core Logic Board over the safety signal bus for any valves that have been placed into bypass.

The Service & Test Board is responsible for the diagnostics, maintenance, and troubleshooting signal path within the MSFIS and is the bus master for the test signal bus. The Service & Test

Board acquires self-test status from all boards except for the power supplies. A cycle is repeated at fixed intervals (once every 10 milliseconds for MSFIS) within a fixed time frame that is allocated to a board access (100 microseconds per board access for MSFIS). Each board reports self-test statuses resulting from diagnostic logic to the Service & Test Board over the test signal bus. The Service & Test Board transmits each board's self-test status, including its own, to an ASU when an ASU is connected to the troubleshooting port. When an ASU is connected, the Service & Test Board can be used to acquire and report additional detailed equipment state information including equipment configuration data. The ALS platform provides a dedicated and independent serial bus for the diagnostics, maintenance, and troubleshooting signal path. This test signal bus is the Test ALS Bus (TAB) that is described in greater detail in Section 3.1.1.5.5 of this SE.

The power supply boards (ALS-905-1 and ALS-905-2) generate the +5 VDC (Volt Direct Current) that is required by all other boards. The power supply boards do not contain serial bus communications capability. The power supply boards report their integrity using a discrete output to one of the input boards.

3.1.1.1 Rack

The rack provides the mounting structure for backplane and boards for installation into the existing cabinetry. The rack is of aluminum construction in an industry standard form factor for use within an industry standard 19-inch cabinet. The MSFIS rack and the backplane accommodate the standard ALS board. Table 1 – ALS Board Positions within Rack, identifies (from left to right when facing the rack) the slot position of each board and the nameplate of an isolation valve controller rack.

Table 1 - ALS Board Positions within Rack

Slot	ALS Board
1	ALS-101 Core Logic Board
2	ALS-301-1 Input Board
3	ALS-301-2 Input Board
4	ALS-401 Solid-state Output Board
5	ALS-201 Service & Test Board
6	ALS-411-1 FET (Field-effect Transistor) and Sensor Board
7	ALS-411-2 FET and Sensor Board
8	ALS-411-3 FET and Sensor Board
	ALS-NP1/NP2 (MSIV or MFIV nameplate)
9	ALS-905-1 Power Supply Unit
10	ALS-905-2 Power Supply Unit

Each rack has the electronics for one isolation valve controller. In addition to the ten boards installed within a rack, a valve controller-specific nameplate is installed between the eighth and ninth card slot. Customizable board front-plates provide labeling for local indications and switches that are specific to the MSFIS application. Figure 7 - Front View of Valve Controller Rack, depicts one isolation valve controller (MSIV is shown). This figure is an extract of "Figure 13: ALS Rack configuration" from References 27 and 28.

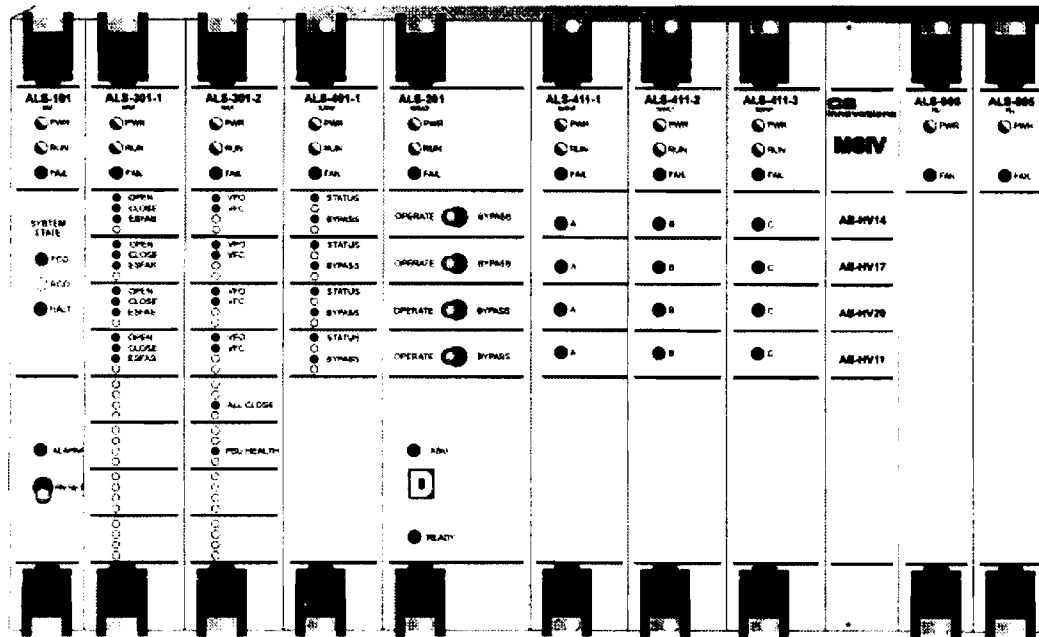


Figure 7 - Front View of Valve Controller Rack

Each board slides into a pre-designated slot of the rack from the front on molded thermoplastic board guides to align the board to mate with a board's backplane and field-wiring connectors. The position of the field-wiring connector varies by board type, and this variation provides a measure of mechanical prevention that limits the ability to install a board into an incorrect position. The ALS platform accommodates the option for additional board connector keying; however, the MSFIS does not utilize this option. While insertion of a board into an incorrect slot remains a possibility, the ALS platform will detect and report an incorrect rack configuration. The front-plate of each board provides low-insertion-force handles/latches to engage and retain the board within the rack. Micro-switches within the latch mechanism of each board disable power to the card through the micro-switches before removal of the board is possible to enable replacement of an individual board without removing power to the entire rack. Each board monitors the position of its latching mechanism's micro-switches.

3.1.1.2 Backplane

The backplane is a printed circuit board that is application-specific to the MSFIS. The backplane provides the interconnection mechanism between installed boards and connects the set of boards with power and field signals. Wire harnesses provide modular connections at the rear of the backplane between the fused terminal blocks and the electronics. The backplane dimensions are designed so it mounts to an aluminum back plate to form the back of the rack.

The backplane provides a mating connector for an ALS board's "X1 connector." The "X1 connector" provides the physical and data interconnection for the RAB and TAB serial communications between installed boards. The backplane provides the media to carry these

communication signals between boards. The backplane provides the EIA-485 bus termination at each end of each serial bus.

The backplane provides a pass-through connector for an ALS board's "X2 connector." An "X2 connector" provides field signals and +5 VDC to controller boards. An "X2 connector" mates with the front shell of a backplane connector. A wire harness for field signals mates with the rear shell of the same backplane connector when both the backplane and field signal cables are mounted to the aluminum back plate.

Figure 8 - Typical ALS Board Layout, shows the location of the X1 and X2 connectors. This figure is an extraction of "Figure 2-2: Generic ALS Board" of the CS Innovations 6002-00026, "ALS Platform Overview," Revision 2, dated January 16, 2009 (Reference 29). The vertical position of the "X1 connector" is standardized as part of the ALS platform. The vertical position of the "X2 connector" connector is not similarly standardized.

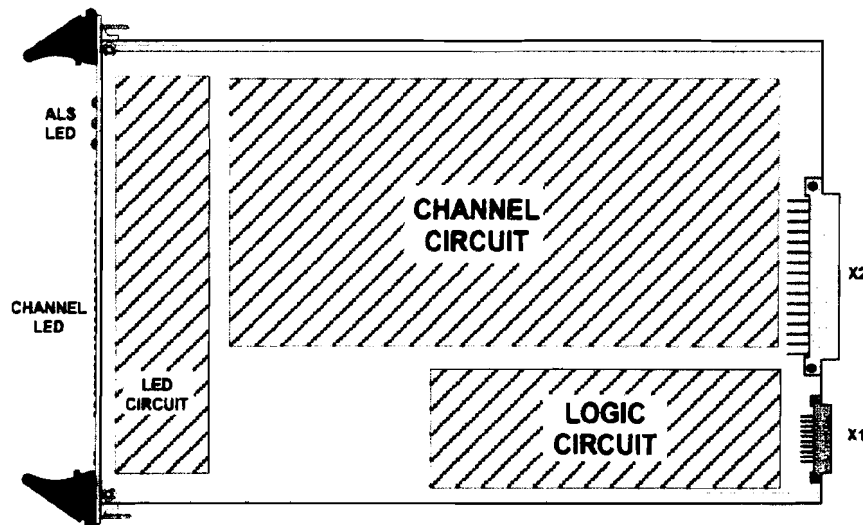


Figure 8 - Typical ALS Board Layout

3.1.1.3 Assembly Panel

One assembly panel mounts within a cabinet to service both isolation valve controller racks. The assembly panel provides the electrical and mechanical interfaces for the rack wire harnesses, field signals, and the Class 1E 125 VDC power. The assembly panel uses terminal blocks to connect with the rack and field signal wire harnesses, and uses a power distribution block with surge protection to connect with 125 VDC input power.

The assembly panel has fuses and fuse-holders for circuit protection for solenoid and input power. The assembly panel has 48 fuses, where a pair is applied to each solenoid output and its return, as well as four input power fuses, where a pair is applied to each rack's 125 VDC input and its return. The assembly panel utilizes standard time-delay Class CC fuses.

The assembly panel has a screw-mounted power distribution block to connect the Class 1E 125 VDC power to the assembly panel. The assembly panel provides a screw-mounted surge

protection terminal block with surge protection devices. The surge protection is provided on the Class 1E 125 VDC power feed and return. The surge protection devices must be replaced at 10-year intervals (maximum).

3.1.1.4 ALS Boards

Each board installs in an isolation valve controller's backplane. Each board is a printed circuit board that may be removed and inserted with power applied to the rack as described in Section 3.1.1.1. The ALS boards connect to the backplane using the X1 and X2 connectors previously discussed in Section 3.1.1.2 and depicted in Figure 8. Each board type, except for the Power Supply Unit, has an FPGA for communications, control, monitoring, and self-test functions. The FPGA is the flash-based Actel ProASICPlus APA600-BG456I device.

For standard board types that process safety signals to perform a safety function, ALS boards include an FPGA with two diverse logic cores that independently and in parallel perform the application-specific logic. This FPGA also has diverse logic for ALS platform standard functions such as RAB communication, TAB communication, and self-test functions. Diversity between the logic cores is obtained through differing synthesis directives within the development process as described in Section 3.1.1.4.1.4.3 of this SE. During operation, a logic self-check circuit detects a mismatch error by comparison of the parallel diverse logic core outputs. An ALS board that detects a mismatch between diverse logic core outputs identifies itself as failed and will set its outputs to a fail-safe state before halting operation. When an ALS-101 Core Logic Board recognizes that an ALS board has failed, it will isolate that board from further RAB communications. For the MSFIS application, the ALS-201 Service & Test Board is the only standard board type with an FPGA containing non-diverse logic cores, because the ALS-201 Service & Test Board is not used to process safety signals.

As part of the ALS platform, boards provide local front-plate indicators. There are two standard indicators that apply to all boards: 1) "PWR" - that indicates power availability and incorporates the status of the micro-switches within the latch mechanism, and 2) "FAIL" - that indicates the overall integrity of the board. Boards provide additional indicators that correspond to the board's function and will be discussed in the board-specific subsections that follow. Except for the power supply board, all boards provide a "RUN" indicator to show whether the board is operating with full capability, reduced capability, or the ALS rack is halted.

With the exception of the Power Supply Units, each board provides configurability through non-volatile memory (NVM) device programming. Configurability enables use of a standard board design in multiple system applications through device programming. The configuration data establishes the specific values for available standard board settings that are required by the system application of the board. The configuration data accommodates application-specific variations such as but not necessary limited to: 1) whether a signal is active high or active low, 2) whether a signal is normally open or normally closed, and 3) the fail-safe state for a signal. Maintenance and configuration control precautions are necessary to avoid incorrect configuration of boards prior to installation. The board configuration is programmed off-line using the CS Innovations' ALS Test Unit (ATU). The ATU communicates with the board using the TAB. The board configuration data has a Cyclic Redundancy Check (CRC) to ensure the integrity of the stored data. During operation, an ALS board periodically tests the validity of the

configuration via its CRC. A failure of a CRC check results in actuation of the alarm status output.

The MSIV and MFIV controller racks contain a common suite of ALS boards. The replacement components of an MSFIS isolation valve controller rack consist of ten ALS boards and the backplane. The ten boards are of six types. Table 2 – MSFIS Board Types, Quantities, Descriptions, and Versions, summarizes the MSFIS application of the ALS boards by type and lists the boards in the order that they shown in Figure 7. The remaining subsections further describe the general board design process and each board in the MSFIS.

Table 2 - MSFIS Board Types, Quantities, Descriptions, and Versions

Designation	Qty	Description	MSFIS Use	Hardware ¹ Version	FPGA ² Version
ALS-101	1	Core Logic Board	MSFIS Logic Board	B	1.02
ALS-301	2	32-channel 24 VDC digital input signal conditioning board	Input Board #1	B	1.01
			Input Board #2	B	1.01
ALS-401	1	16-channel solid-state output signal conditioning board	Solid-state Output Board	B	1.01
ALS-201	1	Service & Test Board	MSFIS Service & Test Board	B	1.00
ALS-411	3	4-channel solid-state FET output signal conditioning board w/ double 125 VDC FET driver & sensor	A-Solenoids Board	B1	1.01
			B-Solenoids Board	B1	1.01
			C-Solenoids Board	B1	1.01
ALS-905	2	Power Supply Board (Input 125 VDC, Output 15 Amps (A) @5 VDC)	Power Supply #1	B3	Not Applicable
			Power Supply #2	B3	Not Applicable
Backplane	1	Rack Backplane	MSFIS Backplane	A	Not Applicable

Notes:

1. Hardware versions are from Section 5.2.2 of CS Innovations 6101-00200, "MSFIS V&V Report," Revision 4, dated January 15, 2009 (Reference 30).
2. FPGA versions are from Section 5.5.5 as modified by Section 11.5.1 of Reference 30.

3.1.1.4.1 Development Process

As part of its obsolescence management strategy, WCGS pursued the MSFIS development with the intention to include the specification of a generic platform that WCGS could deploy in future I&C system upgrades. Because of this approach, this section describes MSFIS application-specific and ALS platform-generic development activities. Though used within the MSFIS, the ALS platform portion of the development activities is not specific to the MSFIS; therefore, the ALS platform portion of this description may be suitable for reference 1) when developing new boards that comply with the ALS platform architecture, or 2) when applying the ALS platform to

other safety-related uses in nuclear power plants. The suitability of the ALS platform will depend on the extent that the NRC staff determines the associated bases, as discussed under Sections 3.2 and 3.3, are acceptable, and to the extent that the accepted plans and procedures, as executed, remain unmodified. The application-specific development portion of this description may also provide a suitable framework for SEs of additional ALS platform uses for other safety-related applications in nuclear power plants. The application-specific suitability will depend on the degree that the roles and relationships established between the MSFIS application-specific development activities and the ALS platform development activities remain unchanged and valid for any new use that is proposed.

The MSFIS program development is structured to follow a traditional waterfall life cycle that includes a top-down requirement and specification development, design implementation, and a bottoms-up V&V effort at each level of integration. The program development allows prototyping activities, and in-process quality assurance efforts are executed integral to the development stages.

3.1.1.4.1.1 Initial Planning and Requirements

WCGS created the "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 16, 2009 (Reference 25), based upon the plant safety requirements applicable to main steam valve and feedwater valve containment isolation for the valve actuators that were identified in the license amendment request (LAR) (Reference 1). The WCGS "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 16, 2009 (Reference 25), contains MSFIS-specific equipment, documentation, qualification and delivery requirements. WCGS engaged CS Innovations for both the MSFIS application-specific development and a generic platform development. Using WCGS "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 16, 2009 (Reference 25), as the customer formal requirements input, CS Innovations produced CS Innovations 6101-00000, "MSFIS Management Plan," Revision 0.4, dated June 14, 2007 (Reference 31), that is CS Innovations MSFIS project level 0 specification. The initial stage of the CS Innovations plan is a concept and planning stage.

3.1.1.4.1.2 Concept Development

The vendor uses the concept and planning stage to produce a conceptual design that was approved by the licensee. CS Innovations produced several documents that represent the conceptual design for the MSFIS and its underlying ALS platform. The vendor conceptual design documentation that was reviewed by the NRC staff is contained in two documents, CS Innovations documents 6002-00010, "ALS Platform Requirements Specification," Revision 2, dated January 15, 2009 (Reference 32), and 6002-00011, "ALS Platform Specification," Revision 2, dated January 14, 2009 (Reference 33). These documents were approved by WCGS and subsequently parsed into the platform and board-specific requirement and hardware design specifications that are identified in Table 3 of Section 3.1.1.4.1.3 that follows.

The concept and planning stage contains a provision to execute prototyping activities that enable the vendor to explore more fully initial customer requirements in order to derive an appropriate set of follow-on detailed requirements and specifications. Prototyping activities typically explore new system interfaces for which a previous ALS platform board design does

not yet exist, or new logic functionality for which a previous standard logic design does not yet exist. The concept and planning stage is described in Sections 4.1 and 4.6 of Reference 31.

3.1.1.4.1.3 Requirements Development

The vendor requirements development activities start with the licensee requirements. WCGS provided "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 16, 2009 (Reference 25), as the formal customer requirements input. Subsequent to the concept development activities, CS Innovations produced a series of requirement and hardware design specification documents. Table 3 - Requirement Documentation Tree, summarizes the system and component hardware requirements documentation and their basis.

Table 3 - Requirement Documentation Tree

Level	Scope	Author	Specification Type	Title	Basis
0	MSFIS	Licensee	Requirements	Specification J-105A(Q) for Replacement MSFIS System (Reference 25)	Plant License with LAR (Reference 1)
0.1	MSFIS	Vendor	Requirements	6101-00002 MSFIS System Specification (References 27 and 28)	Specification J-105A(Q) for Replacement MSFIS System (Reference 25)
0.1.1	ALS Platform	Vendor	Requirements	6002-00010 ALS Platform Requirements Specification (Reference 32)	6101-00002 MSFIS System Specification (References 27 and 28)
0.1.2			Design	6002-00011 ALS Platform Specification (Reference 33)	6002-00010 ALS Platform Requirements Specification (Reference 32)
0.2.1	ALS-101 Board	Vendor	Requirements	6002-10101 ALS-101 Requirements Specification (Reference 35)	6101-00002 MSFIS System Specification (References 27 and 28) 6002-00010 ALS Platform Requirements Specification (Reference 32)
0.2.2			Design	6002-10102 ALS-101 Hardware Specification (Reference 36)	6002-00011 ALS Platform Specification (Reference 33) 6002-10101 ALS-101 Requirements Specification (Reference 35)

Level	Scope	Author	Specification Type	Title	Basis
0.2.1	ALS-301 Board	Vendor	Requirements	6002-30101 ALS-301 Requirements Specification (Reference 37)	6002-00010 ALS Platform Requirements Specification (Reference 32)
0.2.2			Design	6002-30102 ALS-301 Hardware Specification (Reference 38)	6002-00011 ALS Platform Specification (Reference 33) 6002-30101 ALS-301 Requirements Specification (Reference 37)
0.2.1	ALS-401 Board	Vendor	Requirements	6002-40101 ALS-401 Requirements Specification (Reference 39)	6002-00010 ALS Platform Requirements Specification (Reference 32)
0.2.2			Design	6002-40102 ALS-401 Hardware Specification (Reference 40)	6002-00011 ALS Platform Specification (Reference 33) 6002-40101 ALS-401 Requirements Specification (Reference 39)
0.2.1	ALS-411 Board	Vendor	Requirements	6002-41101 ALS-411 Requirements Specification (Reference 41)	6002-00010 ALS Platform Requirements Specification (Reference 32)
0.2.2			Design	6002-41102 ALS-411 Hardware Specification (Reference 42)	6002-00011 ALS Platform Specification (Reference 33) 6002-41101 ALS-411 Requirements Specification (Reference 41)

Level	Scope	Author	Specification Type	Title	Basis
0.2.1	ALS-201 Board	Vendor	Requirements	6002-20101 ALS-201 Requirements Specification (Reference 43)	6101-00002 MSFIS System Specification (References 27 and 28) 6002-00010 ALS Platform Requirements Specification (Reference 32)
0.2.2			Design	6002-20102 ALS-201 Hardware Specification (Reference 44)	6002-00011 ALS Platform Specification (Reference 33) 6002-20101 ALS-201 Requirements Specification (Reference 43)
0.2.1	ALS-905 Board	Vendor	Requirements	6002-90501 ALS-905 Requirements Specification (Reference 45)	6002-00010 ALS Platform Requirements Specification (Reference 32)
0.2.2			Design	6002-90502 ALS-905 Hardware Specification (Reference 46)	6002-00011 ALS Platform Specification (Reference 33) 6002-90501 ALS-905 Requirements Specification (Reference 45)

Table 3 contains requirements that are tested at the various levels of the design development and integration. From the documentation listed and their basis, it is recognized that several different, but not necessarily mutually exclusive, purposes exist for the testing to be performed. For example, alternative purposes include testing for compliance of performance against an MSFIS requirement versus some generic requirement derived for the platform but not applicable to MSFIS. If a generic requirement that is not applicable to MSFIS exists, then testing MSFIS cannot verify the requirement. An example of a generic requirement that is not applicable to MSFIS would be the validity of a board configuration that MSFIS does not use. For example, the ALS-301 board supports either "Voltage-sense" or "Contact-sense" to detect the state of an input, as described in requirement R0743 of Section 7.4 in Reference 37; however, the MSFIS will only use "Contact-sense" mode detection as described in Sections 4.3.3 and 4.3.4 of References 27 and 28.

Any development of a generic platform and associated board suite creates requirements and board features that remain unused in some applications. This situation has a direct affect on the variety and scope of testing that must be performed to verify and validate all requirements. This situation also creates a potential to defer V&V of any requirement that is yet unused by any application. In part due of this situation, CS Innovations and WCGS, or their independent V&V designees, each perform V&V activities in support of the development. As the vendor, CS Innovations is responsible for V&V activities to assure 1) a board meets each board-specific

requirement prior to any application's use of the feature associated with the requirement, 2) a board and its usage complies with the Reference 32, and 3) a resultant system that is based upon the ALS platform complies with its system-specific requirements. These three levels of V&V correspond to 1) board-specific, 2) ALS platform, and 3) system application. The requirements development, design implementation, and first article tests are part of the "Development Stage" as described in Sections 4.2 and 4.7 of Reference 31 and include these vendor activities.

CS Innovations has created CS Innovations 6002-00003, "ALS VV Plan," Revision 1, dated January 5, 2009 (Reference 47), that provides greater detail into the overall development, V&V processes than that within Reference 31. Reference 47 1) addresses levels of integration below the system, that are the FPGA and board levels, 2) recognizes the distinction between ALS platform system test needs and the application-specific system test needs, and 3) makes CS Innovations responsible for factory acceptance testing as part of a Class 1E equipment development.

As the licensee, WCGS, through its independent V&V designees, is responsible for V&V activities to assure the on-site system application of the equipment is compliant 1) upon receipt at the nuclear power plant (on-site acceptance test), and 2) following installation (on-site installation test) within the nuclear power plant.

3.1.1.4.1.4 Design

The vendor has performed MSFIS design development activities in a top-down fashion that progresses from the system level, to the board level, and then to an FPGA digital logic programming level. CS Innovations refined and restated within References 27 and 28 the customer-supplied MSFIS requirements contained in WCGS "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 17, 2009 (Reference 25). Additionally, References 27 and 28 explicitly associate customer-supplied system requirements to an ALS platform-based implementation to include board level function and capability allocations. The board level and FPGA digital logic programming level are coupled. Both the board level and FPGA digital logic programming level derive their requirements from two distinct requirement sources 1) References 27 and 28 for MSFIS functions, interfaces, constraints and capabilities, and 2) Reference 32 for ALS platform and architecture functions, interfaces, constraints and capabilities.

3.1.1.4.1.4.1 System

As described in Sections 3.0 and 3.1 of this SE, the system is 1) the MSFIS as an application-specific system, and 2) the ALS platform as a generic system. The system level design development addresses these two aspects, and the resulting board and FPGA levels of the design development carry forward these two aspects in terms of their design development and the V&V that are performed. However, the in-process system level design quality assurance activity focuses only on the correctness and completeness for a specific application, such as MSFIS, to include: 1) a system's configuration-controlled use of ALS boards, 2) system level requirements compliance, and 3) system level tests performed. This activity ensures that a suitable requirements traceability matrix (RTM) and verification cross-reference matrix exist for the application-specific system. The "Appendix G System Design Review Checklist" of

Reference 47 summarizes the design review efforts for in-process system level design quality assurance.

3.1.1.4.1.4.2 Board

The development of the board level requirements and specifications addresses board functions, interfaces, and constraints and capabilities that have been derived from 1) system-specific needs that are generally applicable and have been allocated to the board, and 2) the ALS platform architecture constraints. Each board has a requirements specification and a hardware specification that trace to parent requirement sources, shown as the "Basis" column in Table 3. The in-process board level design quality assurance activity focuses in areas similar to the system level except that the scope is limited to the board's use as an integrated entity. A further difference exists wherever the board's performance or features are application-specific, as is the case for the ALS-101-1 and ALS-201-1 boards of MSFIS. The board level design quality assurance activity assures the correctness and completeness of 1) a configuration-controlled ALS board, 2) board level requirements compliance, and 3) board level tests performed. Board level tests include its compliance with ALS platform architecture constraints. The board level design quality assurance activity ensures that a suitable RTM and verification cross-reference matrix exists for the board. The "Appendix H Board Design Review Checklist" of Reference 47 summarizes the design review efforts for in-process board level design quality assurance. The NRC staff has reviewed CS Innovations 9002-00035, "Board Design Development Procedure," Revision 1, dated May 13, 2007 (Reference 48), and CS Innovations 9002-00025, "Board Design Review Procedure," Revision 2, dated June 9, 2007 (Reference 49).

3.1.1.4.1.4.3 FPGA

The development of the FPGA digital logic circuits includes functionality, interfaces, constraints, and capabilities that have been derived 1) from board-specific functions, and 2) from the ALS platform architecture constraints. Each FPGA does not have its own requirements specification as a distinct requirement document set; rather, each FPGA is developed to the associated board requirements specification and a hardware specification, and its programmable image developed in accordance with Reference 48. Because an FPGA image contains both board-specific digital logic circuits and standardized ALS platform digital logic circuits, a modular HDL programming approach is used that is similar to traditional μ P-based software programming.

For ALS platform FPGA-based digital logic circuits, the functionality is captured using a text-based high-level language. CS Innovations uses HDL as its high-level language to specify FPGA circuit behavior. The HDL language uses standard text-based expressions to govern the structural and behavioral aspects of the desired digital circuit.

CS Innovations uses personnel that are not otherwise associated with the design development to create the test vectors and test suites. This test development is performed in parallel with the design development and for use throughout the V&V process.

The CS Innovations design process performs simulation of the HDL to model, explore, and test the behavior of the resultant circuit before the use of specific elemental digital building blocks and device interconnections are established. This initial stage of simulation is integral to the

FPGA circuit developer's test bench and validates the designer's intent rather than an actual circuit. HDL simulation does not require a physical FPGA or board, and this stage of HDL simulation and validation is independent of the underlying FPGA device technology.

HDL allows for multiple distinct logic circuits to be designed independently and simulated before integrating them within a single FPGA. After individual modular FPGA logic circuits have been validated, the next step in the FPGA-based circuit development includes the integration and HDL simulation of the integrated modular logic circuits. Again, this simulation validates the designer's intent rather than an actual circuit. The ALS platform FPGA development includes standard and application-specific FPGA logic circuits that are integrated into an overall FPGA logic circuit.

The next step to realize the FPGA-based circuit is the synthesis of the circuit implementation from the high-level descriptions. A software-based development tool that is referred to as a "synthesizer" determines the required FPGA elemental digital building blocks and their interconnections from the HDL statements using synthesizer directives. The synthesizer produces a "netlist" of elemental digital building blocks and interconnects from the HDL, while applying the synthesizer directives. An FPGA circuit developer selects the directive(s) to be used per HDL logic circuit for the FPGA from a list of available digital circuit implementation techniques. During synthesis per the directives, the specific digital circuit building blocks and required interconnections are identified. For ALS platform safety signal path FPGA logic circuits, a pair of logic cores implements identical HDL where each in the pair utilizes a different synthesis directive to create a resultant diverse digital logic circuit implementation. The FPGA-based logic circuits, as described by the netlist, are simulated and validated for proper operation, so that the determination can be made that the circuit will correctly perform the specified functions. The simulation and validation of the synthesis output includes an additional level of circuit detail, but does not yet represent all performance specifics of the targeted FPGA device.

After acceptable performance of the synthesis output has been determined, the synthesized circuit undergoes a place-and-route operation. The place-and-route operation uses an FPGA device manufacturer-specific software-based development tool. During the place-and-route operation, each proposed logic element is assigned to an actual elemental digital building block within the targeted FPGA device. The place-and-route operation also determines the specific physical interconnections required between the elemental digital building blocks. Through these determinations, the place-and-route operation adds an additional level of detail to the circuit definition. These details include device-specific timing characteristics, propagation delays, and input or output pin assignments that are associated with the specific circuit implementation and FPGA device. Once again, CS Innovations simulates and validates the described circuit before programming an FPGA device. This stage of FPGA design validation requires use of specialized software-based development tools to emulate the overall FPGA characteristics. CS Innovations uses two diverse test setups developed independently from one another and independent of the FPGA circuit designer to verify each FPGA circuit design. In this manner, both diverse digital logic circuit implementations are tested in each diverse and independent test setup.

One output of the place-and-route tool is a flash (or burn) list. The flash list is the record that is used to program the FPGA device. The FPGA device image is programmed into a

board-specific test board whose configuration is controlled as part of the V&V process. This programming and its verifications integrates the FPGA program with the FPGA device on a board as part of the overall design development.

The FPGA in-process design review quality assurance activity focuses in areas similar to the board level except that the scope is limited to the FPGA behavior. This activity assures the correctness and completeness of 1) a configuration-controlled FPGA image, and 2) FPGA level behavioral compliance. FPGA level tests include compliant use of standard ALS platform architecture FPGA digital logic functions and the board-specific digital logic functions for which the FPGA was primarily developed, but exclude compliance with a system-specific application. The FPGA level design quality assurance activity ensures that a suitable HDL configuration, test vectors, and test suite exist for the FPGA. The "Appendix I FPGA Design Review Checklist" of Reference 47 summarizes the design review efforts for FPGA level design in-process quality assurance. The NRC staff has reviewed Reference 48 and Reference 49.

3.1.1.4.1.5 Verification and Validation

The vendor and the licensee have performed MSFIS V&V activities in a bottoms-up fashion that progresses from the FPGA digital logic programming level, to the board level, and then to the system level.

3.1.1.4.1.5.1 FPGA

As discussed in Section 3.1.1.4.1.4.3, the FPGA is a programmed device that is subjected to in-process V&V activities that are integral to the associated board's development. The design engineer performs initial simulation and verification activities of the FPGA HDL aided by test vectors developed by personnel not associated with the design effort. The design engineer efforts include validation of the design intent within the development activities of: 1) modular FPGA logic circuits specific to the board, 2) integration of other standardized modular FPGA logic circuits into an overall FPGA logic circuit, and 3) the development of two diverse digital logic circuit implementation cores for the ALS platform safety signal path FPGA logic circuits via differing synthesis directives.

Independent FPGA V&V validates the back annotated FPGA image that results from the place-and-route operation subsequent to circuit synthesis. These back annotated FPGA images include diverse logic circuit cores. Independent V&V activities for the FPGA utilize HDL test benches that are diverse and independent of the design engineer's development. The independence of the two V&V FPGA test benches is achieved by having the two diverse test benches developed using personnel not associated with the design activities. The diversity of the two V&V FPGA test benches is achieved by requiring different HDL simulators within each test bench, both of which differ from the HDL simulator used by the design engineer. These independent V&V test benches rely on the defined set of test vectors and expected results. Both V&V FPGA test benches test each diverse logic circuit core.

3.1.1.4.1.5.2 Board

Board V&V activities require the board's FPGA to be programmed. A configuration-controlled version of the FPGA image that has completed FPGA V&V is used to program the board. The

board V&V utilizes a suite of test fixture ALS boards that have been developed to test the board's compliance against its requirements and specifications. The test fixture is used to verify and validate board performance against the defined set of test vectors and expected results. The test fixture for ALS board testing will also be used to perform individual board level acceptance testing prior to delivery of spares to the customer.

3.1.1.4.1.5.3 System

System V&V activities state that all board FPGAs be programmed and configured in accordance with application-specific requirements and be installed in the application-specific backplane/rack configuration. A configuration-controlled version of each board, FPGA and NVM image is used within the application-specific system configuration. The system V&V utilizes a test fixture with external interface simulators/stimulators to exercise the system against application-specific scenarios. The test fixture is used to verify and validate system performance against the defined system tests and expected results. The test fixture for application-specific system testing will also be used to perform system level acceptance testing prior to delivery of the system to the customer.

3.1.1.4.1.6 Factory Acceptance Tests

Reference 31 does not directly address formal factory acceptance testing except for the integrated system-specific application. This is referred to as the "System Test Stage" as described in Sections 4.4 and 4.9 of Reference 31; however, Reference 47 does address both board level and system level factory acceptance testing.

3.1.1.4.1.6.1 Board

Board factory acceptance tests are planned for spares prior to delivery to the customer. The customer will have no provisions to program FPGAs or the NVM configuration that reside on ALS platform boards. For boards like the ALS-101-1 and ALS-201-1, the FPGA image is application-specific. For these boards, the NVM configuration of a board will also be application-specific. A configuration-controlled version of the FPGA image that has completed FPGA V&V will be used to program the board. A configuration-controlled version of the NVM image that has completed system V&V will be used to program the board. The board factory acceptance test will utilize the suite of test fixture ALS boards that is used in the board V&V activities. A board factory acceptance test procedure will be performed prior to delivery of spares to the customer. This acceptance test procedure will be based upon the board V&V activities.

3.1.1.4.1.6.2 System

System factory acceptance tests are planned for application-specific systems prior to delivery to the customer. The customer will have no provisions to configure the system. For the system application of boards, like the ALS-101 and ALS-201 in MSFIS, the FPGA image is application-specific. For the system application of boards, the NVM configuration of the boards will also be application-specific. A configuration-controlled version of each FPGA image that has completed FPGA V&V will be used to program the boards used by the application-specific system. A configuration-controlled version of each NVM image that has completed system V&V

will be used to program the boards used by the application-specific system. The system factory acceptance test will utilize the suite of test fixture simulators/stimulators that is used in the system V&V activities. A system factory acceptance test procedure will be performed prior to delivery of the system to the customer. This acceptance test procedure will be based upon the system V&V activities.

3.1.1.4.1.7 Site Tests

Unlike preceding V&V efforts that are performed on both an individual board and an integrated system, site tests are only performed on an integrated application-specific system. Regardless, the NRC staff considers it noteworthy that the WCGS MSFIS site tests are based upon the CS Innovations MSFIS system factory acceptance tests. The site tests, 1) Acceptance and 2) Installation, are performed in the Hand-off Stage as described in Sections 4.5.3, 4.5.4, and 4.10 of Reference 31.

3.1.1.4.1.7.1 Acceptance

Site acceptance tests occur following equipment shipment and prior to installation. The site acceptance tests verify that the equipment continues to operate, as specified, such that the equipment is deemed free from any defect that could have resulted from shipment. The MSFIS site acceptance test is application-specific, a licensee responsibility, and is subject to NRC inspection.

3.1.1.4.1.7.2 Installation

Site installation tests occur following equipment installation and prior to use. The site installation tests verify that the equipment has been correctly installed and operate, as specified and expected, such that the equipment is deemed free from any defect that could have resulted from installation. The MSFIS site installation test is application-specific, a licensee responsibility, and is subject to NRC inspection.

3.1.1.4.2 ALS-101 - Core Logic Board

For the MSFIS application, the ALS-101 Core Logic Board is the safety function processor. The MSFIS ALS-101 Core Logic Board provides the valve isolation application logic to control the Solenoid Outputs using the 1) SSPS ESFAS data, 2) operator control panel Input switch data, 3) local manual operate/bypass switch data, and 4) ASU commands for valves in bypass. Also, the MSFIS rack alarm status signal is implemented using the solid-state relay output of the ALS-101 Core Logic Board. The ALS-101 Core Logic Board alarm status signal is connected in series with the ALS-201 Service & Test Board alarm status signal to create the MSFIS rack alarm status signal.

As a standard board type, an ALS-101 Core Logic Board provides application-specific function logic to process safety signals for an ALS-based application using an FPGA with two diverse cores as described in Section 3.1.1.4 of this SE. The ALS-101 Core Logic Board performs its application-specific digital logic within its flash-based FPGA. The ALS-101 Core Logic Board hardware specification is Reference 36.

An ALS-101 Core Logic Board is the RAB serial bus master and all other boards are RAB serial bus slaves. The ALS-101 Core Logic Board collects inputs via the RAB, performs logic, and provides outputs via the RAB. In contrast to the RAB, an ALS-101 Core Logic Board is a TAB serial bus slave. The ALS-101 Core Logic Board responds to ALS-201 Service & Test Board TAB requests in a manner that does not impact safety signal processing. The ALS-101 Core Logic Board provides its diagnostic data to the ALS-201 Service & Test Board in response to TAB requests. Section 3.1.1.5.5 of this SE describes the RAB and TAB communications in greater detail.

In addition to ALS platform standard indications, an ALS-101 Core Logic Board provides local indicators to determine the overall system mode of operation as described in Section 2.3 of Reference 33. These local system mode indications are 1) "FCO," 2) "RCO," and 3) "HALT." "FCO" stands for Full Capability Operation and indicates that the ALS platform is operating normally and can perform the intended safety function. When in "FCO" mode, all circuits are 100 percent functional and operational, input channels are updated, evaluated, and are in accordance with expected values; output channels are controlled in the manner for which they are intended such that the feed-back information received is as expected; and the diverse core logic is fully functional. "RCO" stands for Reduced Capability Operation and indicates that the ALS platform has detected one or more conditions, such as failures, that prevent Full Capability Operation. When in "RCO" mode, identified failures will be isolated to prevent them from propagating through the system or otherwise causing unintended events. The system will continue to perform as specified and all unaffected circuits, such as input and output channels, will continue to perform their intended function. The ALS platform alarm status will be activated when in "RCO" mode. "HALT" indicates that the ALS platform has halted operation or is powering up. After power-up, the "HALT" mode is indicative of a detected failure that prevents performance of the safety function and requires the ALS platform to place itself into a fail-safe state. When in "HALT" mode, the ALS platform is inoperable and incapable of performing the intended safety function. All RAB communication will stop when the ALS rack is in "HALT."

An ALS-101 Core Logic Board front-plate provides a local indication of the rack alarm status signal status and a local reset switch to force the rack to restart. Details of the MSFIS ALS-101 Core Logic Board front-plate indications and controls are provided in Section 13.1 of References 27 and 28.

3.1.1.4.3 ALS-301 - Input Boards

The MSFIS has one type of input board, ALS-301, to monitor switch and relay contact signals. The first of the two MSFIS Input Boards, ALS-301-1, uses 12 of its available 32 channels, and the second, ALS-301-2, uses 10 of its available 32 channels. The MSFIS ALS-301-1 Input Board receives signals and provides the input data to the ALS-101 Core Logic Board for 1) each operator control panel manual open switch contact, 2) each operator control panel manual close switch contact, and 3) each SSPS ESFAS signal. Details of the MSFIS ALS-301-1 Input Board signals are contained in Section 4.3.3 of References 27 and 28. The MSFIS ALS-301-2 Input Board receives signals and provides the input data to the ALS-101 Core Logic Board for 1) each valve full-open position switch contact, 2) each valve full-closed position switch contact, 3) the operator control panel all close switch contact, and 4) the internal power supply unit (ALS-905), health status. Details of the MSFIS ALS-301-2 Input Board signals are contained in Section 4.3.4 of References 27 and 28.

As a standard board type, an ALS-301 Input Board provides the capability to monitor 32 input signal channels to process safety signals for an ALS-based application using an FPGA with two diverse cores as described in Section 3.1.1.4 of this SE. An ALS-301 Input Board performs its standardized digital logic within its flash-based FPGA. An ALS-301 Input Board provides 10 milliamps at 24 VDC to determine the state of a contact signal, and determines a contact signal to be open when it senses a resistance greater than 2,000 ohms or determines a contact signal to be closed when it senses a resistance less than 400 ohms. The ALS-301 Input Board hardware specification is Reference 38.

An ALS-301 Input Board is a RAB serial bus slave. An ALS-301 Input Board provides its input signal data to the ALS-101 Core Logic Board in response to RAB requests. An ALS-301 Input Board is also a TAB serial bus slave. An ALS-301 Input Board responds to ALS-201 Service & Test Board TAB requests in a manner that does not impact input signal monitoring functions. An ALS-301 Input Board provides its diagnostic data to the ALS-201 Service & Test Board in response to TAB requests.

An ALS-301 Input Board conducts its built-in self check of channel input integrity at least once every 15 minutes or upon a state change event.

In addition to ALS platform standard indications, an ALS-301 Input Board provides local indicators to show the status of its inputs. For ALS-301-1, open indicators are on when the associated operator control panel manual open switch contact input is closed; otherwise, they are off. Close indicators are on when the associated operator control panel manual close switch contact input is closed; otherwise, they are off. ESFAS indicators are on when the associated ESFAS contact input is open; otherwise, they are off. The details of the ALS-301-1 front-plate indications are provided in Section 13.2 of References 27 and 28. For ALS-301-2, valve full-open indicators are on when the associated valve position switch contact input is closed; otherwise, they are off. Valve full-closed indicators are on when the associated valve position switch contact input is closed; otherwise, they are off. An all close indicator is on when the associated operator control panel manual all close switch contact input is closed; otherwise, it is off. A power supply unit health indicator is on when both power supplies are operational; otherwise, it is off. Details of the ALS-301-2 front-plate indications are provided in Section 13.3 of References 27 and 28.

3.1.1.4.4 ALS-401 and ALS 411 - Output Boards

The MSFIS has two types of output boards: 1) the ALS-401 Solid-state Output Board, and 2) the ALS-411 FET & Sensor Board. The ALS-401 Solid-state Output Board is used to control lower power loads such as indicators, relay inputs, and other solid-state logic devices. The ALS-411 FET & Sensor Board is used to drive higher power inductive loads such as the isolation valve solenoids for the MSFIS application.

3.1.1.4.4.1 ALS-401 - Solid-state Output Board

The MSFIS ALS-401 Solid-state Output Board uses eight of its available 16 channels. The MSFIS ALS-401 Solid-state Output Board receives output data from the ALS-101 Core Logic Board and provides signals for 1) each valve ready output, and 2) each valve bypass output.

Details of MSFIS ALS-401 Solid-state Output Board signals are contained in Section 4.3.5 of References 27 and 28.

As a standard board type, an ALS-401 Solid-state Output Board provides the capability to control and monitor 16 solid-state output channels to process safety signals for an ALS-based application using an FPGA with two diverse cores as described in Section 3.1.1.4 of this SE. The ALS-401 Solid-state Output Board performs its standardized logic within its flash-based FPGA. An ALS-401 Solid-state Output Board output channel provides an optical isolated solid-state relay contact to provide 0.38 amperes at 118 VAC (volt alternative current) to energize and de-energize a status signal output. The ALS-401 Solid-state Output Board hardware specification is Reference 40.

An ALS-401 Solid-state Output Board is a RAB serial bus slave. An ALS-401 Solid-state Output Board responds to ALS-101 Core Logic Board RAB data transfers to control its solid-state output signals. An ALS-401 Solid-state Output Board is also a TAB serial bus slave. An ALS-401 Solid-state Output Board responds to ALS-201 Service & Test Board TAB requests in a manner that does not impact output signal control functions. An ALS-401 Solid-state Output Board provides its diagnostic data to the ALS-201 Service & Test Board in response to TAB requests.

In addition to ALS platform standard indications, the MSFIS ALS-401 Solid-state Output Board provides local indicators to show the status of its outputs. Status indicators are on when the associated valve ready output relay is closed; otherwise, they are off. Bypass indicators are on when the associated bypass status relay output is closed; otherwise, they are off. Details of the MSFIS ALS-401 Solid-state Output Board front-plate indications are provided in Section 13.4 of References 27 and 28.

3.1.1.4.4.2 ALS-411 - FET & Sensor Boards

Each of the three MSFIS ALS-411 FET & Sensor Board utilizes all four of the available four output channels to control valve positions. Each of the MSFIS FET & Sensor Boards, ALS-411-1, ALS-411-2, and ALS-411-3, provide the Solenoid A, Solenoid B, or Solenoid C outputs, respectively. Each MSFIS ALS-411 FET & Sensor Board receives output data from the ALS-101 Core Logic Board and provides Solenoid signals to each valve. Details of the MSFIS ALS-411 FET & Sensor Board output signals are contained in Sections 4.3.6, 4.3.7, and 4.3.8 of References 27 and 28.

As a standard board, an ALS-411 FET & Sensor Board provides the capability to control and monitor four solid-state FET output channels to process safety signals for an ALS-based application using an FPGA with two diverse cores as described in Section 3.1.1.4 of this SE. The ALS-411 FET & Sensor Board performs its standardized digital logic within its flash-based FPGA. Each of the four channels has redundant solid-state circuitry. An ALS-411 FET & Sensor Board output channel provides 1 ampere at 125 VDC via the isolated solid-state FET devices to energize and de-energize an actuation signal output. The ALS-411 FET & Sensor Board hardware specification is Reference 42.

An ALS-411 FET & Sensor Board is a RAB serial bus slave. An ALS-411 FET & Sensor Board responds to ALS-101 Core Logic Board RAB data transfers to control its FET output signals. An

ALS-411 FET & Sensor Board is also a TAB serial bus slave. An ALS-411 FET & Sensor Board responds to ALS-201 Service & Test Board TAB requests in a manner that does not impact output signal control functions. An ALS-411 FET & Sensor Board provides its diagnostic data to the ALS-201 Service & Test Board in response to TAB requests.

An ALS-411 FET & Sensor Board conducts its built-in self check of channel output integrity at least once every 60 seconds.

In addition to ALS platform standard indications, each ALS-411 FET & Sensor Board provides local indicators to show the status of its outputs. Status indicators blink when the associated FET output channel has failed. When no failure exists, the status indicators are on when the associated FET output has energized the solenoid; otherwise, they are off. Details of the ALS-411-1, ALS-411-2, and ALS-411-3 FET & Sensor Board front-plate indications are provided in Sections 13.6, 13.7, and 13.8, respectively, of References 27 and 28.

3.1.1.4.5 ALS-201 - Service & Test Board

The MSFIS ALS-201 Service & Test Board provides input status data to the ALS-101 Core Logic Board for 1) each local manual operate/bypass switch status, and 2) the Universal Serial Bus (USB) port connection status. Details of MSFIS ALS-201 Service & Test Board signals are contained in Section 4.3.2 of References 27 and 28.

The MSFIS ALS-201 Service & Test Board provides the capability to observe internal equipment states and data by an ASU operator in support of maintenance and troubleshooting. The Service & Test Board provides 1) a USB port for connection to an ASU, where the ASU provides the operator interface to view the complete TAB data set for the all installed boards, and 2) local manual operate/bypass switches via its front-plate to place valves into bypass in support of surveillance testing. Also, the MSFIS rack alarm status signal is implemented using the solid-state relay output of the ALS-201 Service & Test Board. The ALS-201 Service & Test alarm status signal is connected in series with the ALS-101 Core Logic Board alarm status signal to create the MSFIS rack alarm status signal.

The ALS platform approach of two diverse logic cores applies only to potential safety function uses. Because the ALS-201 Service & Test Board will not be used to perform safety functions and cannot impact the safety signal path, the ALS-201 Service & Test Board does not include two diverse logic cores, as described in Section 3.1.1.4 of this SE. The ALS platform only applies the channel self-tests to signals with potential safety function uses. Because the operate/bypass switch is not considered a safety function use and cannot impact the safety signal path in an undetectable manner if failed, the ALS-201 Service & Test Board does not include built-in self check of each operate/bypass switch channel's input integrity for the ALS-201 Service & Test Board similar to that provided for the ALS-301 Input Board. The ALS-201 Service & Test Board hardware specification is Reference 44.

When connected, the USB port provides communication with an ASU. When a USB connection is detected by the presence of valid data communications, the ALS-201 Service & Test Board generates its alarm status signal. The ALS-201 Service & Test Board does not generate its alarm status signal solely in response to the physical insertion of a USB connector.

Use of the bypass position of the ALS-201 Service & Test Board switches forces a valve to remain in its present state. When in the bypass position, inputs associated with controlling the valve position will be ignored by the ALS-101 Core Logic Board, so as to continue to keep a valve in its present state. When the switch is in the operate position, inputs associated with controlling the valve position will not be ignored. Use of the bypass position causes the ALS-101 Core Logic Board to activate corresponding bypass status outputs to the SSPS via the ALS-301 Solid-state Output Board. As described in “Figure 26: Valve-Logic FSM [finite state machine] (embedded in the valve logic module)” of References 27 and 28, use of the bypass position also enables individual control of a Solenoid output (A, B, or C) via ASU commands. Exercising a Solenoid output control individually cannot change the actual valve position.

The ALS-201 Service & Test Board is the TAB serial bus master and all other boards are TAB serial bus slaves. The ALS-201 Service & Test Board polls each slave board within the system to obtain the complete set of self-test, diagnostics and test data. The complete set of diagnostic data is used by the “Blackbox” and “LiveView” features described under Section 3.2, “Diagnostics,” paragraph of Reference 29. The utility of these features rely on the connection and operation of an ASU. Data is serially transferred by the ALS-201 Service & Test Board to the ASU over the USB. In contrast to the TAB, the ALS-201 Service & Test Board is a RAB serial bus slave. The ALS-201 Service & Test Board provides the operate/bypass switch and USB connected status data to the ALS-101 Core Logic Board in response to RAB requests. Section 3.1.1.5.5 of this SE describes the RAB and TAB communications in greater detail.

In addition to ALS platform standard indications, each ALS-201 Service & Test Board provides local indicators. An ASU indicator is on when a valid ASU communication is present through the USB port; otherwise, it is off. A Ready indicator is energized when the ALS rack is fully operational; otherwise, it is off. Details of the ALS-201 Service & Test Board front-plate indications and controls are provided in Section 13.5 of References 27 and 28.

3.1.1.4.6 ALS-905 - Power Supply Units

The pair of ALS-905 Power Supply Units, as MSFIS ALS-905-1 and ALS-905-1, provides source +5 VDC power for all boards within an isolation valve controller rack. From the ALS-905 Power Supply Unit +5 VDC supply, individual boards generate regulated voltages in accordance with board-specific circuitry needs.

As a standard board type, an ALS-905 Power Supply Unit provides the power for use by all boards within an ALS rack. This power is derived from a Class 1E 125 VDC feed using DC-to-DC converter technology. An ALS-905 Power Supply Unit provides a regulated output of 15A @5 VDC. The pair of ALS-905 Power Supply Units provides load sharing and redundancy, where each ALS-905 Power Supply Unit is capable of providing 100 percent of the power required by the rack for uninterrupted operation in the event of a single power supply failure. Either ALS-905 Power Supply Unit can be replaced while the rack is energized, so that the replacement of a failed power supply does not require taking the equipment out of service. The ALS-905 Power Supply Unit hardware specification is Reference 46.

The ALS-905 Power Supply Unit front-plate only has the ALS platform standard “PWR” and “FAIL” indications. Details of the ALS-905 Power Supply Unit front-plate indications are provided in Section 13.10 of References 27 and 28.

3.1.1.5 Communications

IEEE 603-1991 Clause 5.6, "Independence," requires independence between (1) redundant portions of a safety system, (2) safety systems and the effects of design basis events, and (3) safety systems and other systems. SRP Chapter 7, Appendix 7.1-C, Section 5.6, "Independence," provides acceptance criteria for this requirement, and among other guidance, provides additional acceptance criteria for communications independence. Section 5.6 states that where data communication exists between different portions of a safety system, the analysis should confirm that a logical or software malfunction in one portion cannot affect the safety functions of the redundant portions, and that if a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, a logical or software malfunction of the non-safety system must not be able to affect the functions of the safety system.

IEEE 7-4.3.2-2003, endorsed by Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" (Reference 130), Clause 5.6, "Independence," provided guidance on how IEEE 603 requirements can be met by digital systems. This clause of IEEE 7-4.3.2 states that, in addition to the requirements of IEEE Standard 603-1991, data communication between safety channels or between safety and non-safety systems shall not inhibit the performance of the safety function. SRP Chapter 7, Appendix 7.1-D, Section 5.6, "Independence" provides acceptance criteria for equipment qualifications. This section states 10 CFR 50, Appendix A, GDC 24, "Separation of protection and control systems," states that the protection system be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system, and that interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired. Additional guidance on interdivisional communications is contained in "Interim Staff Guidance, Digital Instrumentation and Controls, DI&C-ISG-04, Task Working Group #4, Highly-Integrated Control Rooms—Communications Issues (HICRc)," dated September 28, 2007 (Reference 140). DI&C-ISG-04 compliance is discussed further in Section 3.1.1.6 of this SE.

The NRC staff has reviewed the overall design as discussed in the following subsections. As part of this review, the NRC staff evaluated applicability and compliance with SRP Section 7.9, "Data Communication Systems," SRP Chapter 7, Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems," and Branch Technical Position 7-11, "Guidance on Application and Qualification of Isolation Devices."

Because signal communication may exist between different portions of the safety system, the evaluation includes a review to determine if a malfunction in one portion affects the safety functions of the redundant portion(s). Because the safety system can be connected to a digital computer system that is non-safety, the evaluation includes a review to determine if a logical or software malfunction of the non-safety system affects the functions of the safety system.

The MSFIS communicates with other safety-related equipment for the containment isolation control functions of Main Steam and Feedwater and with non-safety-related equipment to

support maintenance, test and troubleshooting. As discussed in Sections 3.0 and 3.1 of this SE, the MSFIS is safety-related equipment with two separate Class 1E divisions.

The MSFIS does not contain transmission of signals between independent channels. Therefore, requirements of SRP Chapter 7, Appendix 7.0-A, SRP Section 7.9, and DI&C-ISG-04 applicable to transmission of signals between independent channels do not apply to the MSFIS, and no further review is required. DI&C-ISG-04 compliance is discussed further in Section 3.1.1.6 of this SE.

Except for the safety to non-safety interface, all MSFIS communications are made via individual one-way on/off signals. This type of communications does not allow data other on/off initiation to be contained in this communications, and no handshaking or acknowledgement is used or required. Therefore, this SE only evaluates the safety to non-safety interface compliance with the guidance in SRP Chapter 7, Appendix 7.0-A and DI&C-ISG-04. DI&C-ISG-04 compliance is discussed further in Section 3.1.1.6 of this SE.

BTP 7-11 provides guidance for the application and qualification of isolation devices. BTP 7-11 applies to the use of electrical isolation devices to allow connections between redundant portions of safety systems or between safety and non-safety systems. The MSFIS does not contain connections between redundant portions of the safety systems. Therefore, this SE only considers applicability between safety and non-safety systems.

3.1.1.5.1 Communications from MSFIS to Other Safety-Related Equipment

The MSFIS communications with other safety-related equipment are with the: 1) SSPS for automatic valve closure and valve operational status signals, 2) operator control panel for manual valve position control and monitoring, and 3) isolation valves for actuation control and position monitoring.

For each MSFIS safety-safety communication, the interface maintains division separation and the interconnecting equipments are both Class 1E circuits. Section 2.5 of References 27 and 28 states that the system "shall provide electrical isolation and physical separation to develop the required independence on the replacement MSFIS." Section 2.5 of References 27 and 28 states that "application of short circuit, ground, open circuit, or potential to one device shall not cause loss of function of the circuits or devices from which it is isolated." These top-level requirements flow down into the MSFIS design elements to develop regulatory compliant safety communications.

3.1.1.5.1.1 Communications with the SSPS

The MSFIS receives automatic valve closure control signals from the SSPS. The ESFAS control signals are one-way open/closed signals from the SSPS to the MSFIS. This MSFIS locally indicates the status of these signals on its front panel. The MSFIS performs a two-of-four voting evaluation of these signals. In response to the ESFAS signal voting, the MSFIS initiates closure of each isolation valve that remains operational and is not in bypass. The system architecture requires that only one division request valve closure to close the valves.

The WCGS "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 16, 2009 (Reference 25), Section 5.2.4 subpart a) contains the specification for the ESFAS signals. The ESFAS signals are received by the ALS-301-1 Input Board. Existing copper wiring provides the signal path for the ESFAS control signals from the SSPS to the MSFIS. When the SSPS determines main steam and feedwater isolation is required, four relay contacts in the SSPS are opened. The MSFIS ALS-301-1 board determines the status of the relay contacts by determining the resistance through each contact.

The MSFIS also provides bypass status signals to the SSPS. The bypass status signals are one-way on/off signals from the MSFIS to the SSPS. Existing copper wiring provides the signal path for the bypass status signals from the MSFIS to the SSPS. The ALS-401-1 board provides an optical isolated solid-state relay contact to energize and de-energize the bypass status signal output, closing the solid-state relay contact when in bypass, or opening the solid-state relay contact when not in bypass. This MSFIS locally indicates these signals on its front panel. The MSFIS provides one bypass status signal for each valve, and this bypass is generated via a MSFIS front panel operate/bypass switch. Administrative controls at WCGS state that the complete set of four valves of an isolation valve controller rack will be placed into bypass when any one of its four valves is in bypass.

The NRC staff reviewed the communications between the SSPS and MSFIS for both the isolation signal and bypass signals, and determined that because the communications from the SSPS is a one-way, on/off signal, no data other than the valve close initiation can be contained in this communications. The signal is received by the MSFIS, and no handshaking or acknowledgement is required. This communications complies with guidance provided in SRP Section 7.9 and DI&C-ISG-04, in that a malfunction in one portion of the MSFIS cannot affect the safety functions of the redundant portion and is, therefore, acceptable. DI&C-ISG-04 compliance is discussed further in Section 3.1.1.6 of this SE.

3.1.1.5.1.2 Communications with the Operator Control Panel

The MSFIS receives remote manual valve control signals from the operator control panel. The remote manual valve control signals are 1) all close, 2) close, and 3) open. The remote manual valve control signals are one-way open/closed signals from the operator control panel to the MSFIS. This MSFIS locally indicates the status of these signals on its front panel. Each signal is taken from an operator control panel operator switch contact by an ALS-301 Input Board in the same manner as switch open or close status is determined from the SSPS. In response to the all close signal, the MSFIS initiates a closure of each isolation valve that remains operational and is not in bypass. In response to an individual valve close signal, the MSFIS performs a closure of the associated isolation valve if that valve is operational and not in bypass. The system architecture requires that only one division request a valve closure to close the valve. In response to an open signal, a MSFIS attempts to perform an opening of the selected isolation valve, if that valve is operational and not in bypass. The system architecture requires that both divisions request a valve opening at the same time to open the valve. Existing copper wiring provides the signal path for the remote manual valve control signals from the operator control panel to the MSFIS.

The MSFIS also provides valve ready status and alarm status signals to the operator control panel. These signals are one-way on/off signals from the MSFIS to the operator control panel.

The ALS-401-1 board provides an optical isolated solid-state relay contact via existing copper wiring for the valve ready status signals from the MSFIS to the operator control panel to energize and de-energize the valve ready status signal output, with the contact closed when the valve is ready, or open when the valve is not ready. The MSFIS cabinet provides one alarm status signal per rack for two signals per cabinet. Circuitry between the MSFIS and the operator control panel indicator combines these two signals to provide a single cabinet remote alarm indication on the operator control panel. The alarm indicates the full operational availability of the MSFIS racks. Copper field wiring, to be installed as part of the MSFIS upgrade, provides the signal path for the alarm status signals from the MSFIS to an alarm circuit associated with the operator control panel. The ALS-101-1 and ALS-201-1 boards provide optical isolated solid-state relay contacts to energize and de-energize the alarm status signal output. The NRC staff reviewed the communications between the MSFIS and the operator control panel, and determined that this communications complies with guidance provided in SRP Section 7.9 and DI&C-ISG-04, in that a malfunction in one portion of the MSFIS cannot affect the safety functions of the redundant portion. DI&C-ISG-04 compliance is discussed further in Section 3.1.1.6 of this SE.

3.1.1.5.1.3 Communications with the Isolation Valves

The MSFIS provides valve actuation control signals to each isolation valve. The valve actuation control signals are one-way on/off signals from the MSFIS to an isolation valve. The MSFIS provides three valve actuation control signals per valve. The valve actuation control signals are 1) Solenoid A, 2) Solenoid B, and 3) Solenoid C. This MSFIS locally indicates the status of these signals on its front panel. The MSFIS uses these signals to change a valve's position in response to automatic or manual requests. This is performed by the ALS-411 boards energizing Solenoids. The Core Logic Board controls the pattern, sequence and timing of the Solenoid A, B, and C outputs to change the isolation valve's position. Copper wiring associated with the replacement valve actuators (see the April 3, 2008, SE for Amendment No. 177, Reference 146) provides the signal path for the valve actuation control signals from the MSFIS to an isolation valve.

The MSFIS energizes and de-energizes solenoids to control pilot valves that pressurize and de-pressurize the upper or lower piston chambers of the valve. To close a valve, the MSFIS de-energizes all three solenoids (A, B & C) for about 1 minute in order to ensure the valve is driven closed by the process fluid. After the 1-minute delay, the MSFIS energizes only solenoid C to keep the valve closed. Either division can independently close a valve, but to perform the closure the division's solenoids A & B must be de-energized until the valve is closed. To open a valve, the MSFIS energizes solenoids A & B and de-energizes solenoid C. Both divisions' solenoid sets are required to open the valve.

The MSFIS receives valve full-position status signals, either full open or full closed, from each isolation valve. The full-position status signals are one-way open/closed signals from isolation valves to the MSFIS. Each full position status signal is provided by an isolation valve switch contact. This MSFIS locally indicates these signals on its front panel. The operator control panel uses these signals to control the state of valve status indications that are provided to the operator. These signals are received by the ALS-301-2 Input Board via the same type of resistance determination as described in Section 3.1.1.4.3 of this SE. The signals are transmitted via copper wiring associated with the replacement valve actuators

The NRC staff reviewed the communications between the MSFIS and the isolation valves, and determined that this communications complies with guidance provided in SRP Section 7.9 and DI&C-ISG-04, in that a malfunction in one portion of the MSFIS cannot affect the safety functions of the redundant portion. DI&C-ISG-04 compliance is discussed further in Section 3.1.1.6 of this SE.

3.1.1.5.2 Communications with Non-safety Systems

The only communications between MSFIS and a non-safety system is the communications with the ASU, for test, diagnostics, maintenance, and troubleshooting of the MSFIS. The ASU is non-safety related, and its use is subject to administrative controls.

The MSFIS-ASU communications is two-way data communications. MSFIS generates the alarm status signal when an active MSFIS-ASU communications is detected. MSFIS indicates an active MSFIS-ASU communications on its front panel. The ASU is a portable personal computer with a windows-based MSFIS-specific software application. This software application implements a proprietary data protocol to exchange data with the MSFIS. The MSFIS-ASU interface is a USB 2.0 port.

The MSFIS provides test and diagnostics data to the ASU. The ASU displays the test and diagnostic data. The ASU sends data requests to the MSFIS to obtain troubleshooting information. The ASU provides data commands to the MSFIS to support testing of the valve actuator control signals when that valve is in bypass. The MSFIS automatically restores valve actuator control signals to their appropriate state when the ASU is disconnected or the valve undergoing ASU testing is removed from bypass.

The ASU and its MSFIS-specific application are non-safety related for use in accordance with administrative controls. Administrative controls are described in Section 1.2.2 of WCGS "Operation Plan," Revision 2, dated January 14, 2009 (Reference 50). The administrative restrictions are that the associated MSFIS rack will have all four of its isolation valves in bypass whenever an ASU connection exists, and that only a single MSFIS-ASU connection among the MSFIS racks may be made at any given time.

The USB port providing the connection to the ASU is on the ALS-201 board. This board is safety-related hardware, and provides the communications interface between the MSFIS and the ASU. The USB connection provides isolation from the ALS rack, and the ALS-201 board acts as a buffering circuit. The segregation of test and safety data, as described in Section 3.1.1.5.4 of this SE provides the communications independence described in IEEE 7-4.3.2 for communication between safety and non-safety computers.

After NRC staff review of WCGS "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 16, 2009 (Reference 25); References 27 and 28; CS Innovations 6000-00000, "ALS Level-1 System Specification," Revision 1.02, dated June 9, 2007 (Reference 51); Reference 43; and Reference 44, the NRC staff determined that the MSFIS-ASU communications satisfies the requirements for safety to non-safety communications. The MSFIS-ASU communications complies with the isolation guidance in BTP 7-11 by providing the signal isolation per Section 13.1 of Reference 51. After review of the

documents mentioned above, and the signal paths they describe, the NRC staff determined that the MSFIS-ASU communications maintains division separation and cannot compromise the independence of redundant portions of the safety system, in compliance with SRP Section 7.9 and DI&C-ISG-04, when used in accordance with identified administrative controls. DI&C-ISG-04 compliance is discussed further in Section 3.1.1.6 of this SE.

3.1.1.5.3 Communications between Separate Class 1E Divisions

The MSFIS utilizes two separate Class 1E powered division within separate enclosures. The MSFIS utilizes pre-existing enclosures and plant wiring.

The NRC staff reviewed the specifications for 1) use of common components to redundant portions of the safety system, 2) physical separation, and 3) electrical independence. The NRC staff reviewed the following specifications for compliance: 1) WCGS "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 16, 2009 (Reference 25), 2) References 27 and 28, and 3) Reference 51. Based upon this review, the NRC staff determined that there is no communications between separate divisions of the MSFIS, and with no communications, there is no malfunction in one division of the MSFIS that could be communicated to a separate division of the MSFIS and, therefore, affect the safety functions of that redundant division. The NRC staff also determined that MSFIS 1) does not use common components to redundant portions of the safety system, 2) maintains physical separation, and 3) maintains electrical independence.

3.1.1.5.4 Independence of Safety Signal Path within a Division

The MSFIS performs safety-related functions for automatic and manual isolation. MSFIS also has functions associated with maintenance, test and troubleshooting, and while these functions are not directly associated with safety-related valve control, they are implemented within the safety-related FPGA, support the valve control functions, and were developed as safety-related functions. Therefore, no non-safety functions exist within the MSFIS.

3.1.1.5.5 Internal Communications and Bus Structure

Internal communication within the ALS platform architecture is limited to serial data transfers over one of two buses. The first of two buses is the "RAB: Reliable ALS Bus" that is used for the safety signal path. The second bus, "TAB: Test ALS Bus," that is used for diagnostics and test data. Each bus follows a master-slave protocol. The Core Logic Board is the bus master of the RAB, and the Service & Test Board is the bus master of the TAB.

The NRC staff reviewed the documentation in Reference 29 and Reference 51 and determined that communications independence is provided by the inclusion of two separately controlled buses, as described by the CS Innovations design. Communication independence exists, because 1) the RAB segregates the operational safety signal path from the TAB that provides the maintenance and troubleshooting diagnostic signal path, 2) independent digital logic circuits in the form of separate finite state machines implement the bus logic, and 3) operation of the TAB does not affect operation of the RAB.

Each bus protocol is based on the EIA-485 differential standard. The MSFIS boards are connected using the application backplane of each rack. Each bus is half-duplex and, therefore, does not allow simultaneous data transmission and reception. The serial communication protocol for each bus utilizes Cyclic Redundancy Checks (CRCs) to ensure the integrity of a data transfers between boards.

Each bus follows a master-slave protocol, with the Core Logic Board always being the RAB bus master, and the Service & Test Board always being the TAB bus master. The half-duplex communications allows for only one active transmitter at any point in time as controlled by the bus master. Each bus master (Core Logic Board or Service & Test Board) controls its serial data bus resource (RAB or TAB) that is shared among boards, so that two boards cannot simultaneously access a bus. The master controls the bus, and the slaves only communicate when requested and enabled. Each slave board listens for a broadcast message that does not require an acknowledgement. For other than broadcast messages, the slave has 100 microseconds to respond to the master after the master makes a data exchange request with the slave board. The bus master sequentially communicates with each installed board within a fixed time cycle repeated every 10 milliseconds. The bus master performs a single retry in response to an unsuccessful slave response on the next cycle, and if that communications fails, the board is declared as failed by the bus master. When a board is declared as failed, it triggers the bus master's alarm status output and is indicated as failed on the operators control panel. For the RAB communications, a failed board is taken out of the cyclic communication sequence. This state of inactive RAB communications remains until intervention by an operator. This intervention includes the performance of a rack reset that would occur after any repair.

Each slave board can detect communication failure on the RAB or TAB, and can isolate itself from further communications on the RAB until the communication failure is corrected. Each RAB slave implements a communication watchdog time-out and "HALT" function for RAB communications. This watchdog function detects a condition where the slave board has not successfully been polled for a prescribed interval.

The CS Innovations proprietary communication protocol that is used for RAB and TAB serial data transfers is similar but not identical. Section 8.3.1 of Reference 29 states "The only exception is that the TAB will not force the board into HALT Mode, but instead will detect the failure and ensure no valid response is issued." When installed in the MSFIS, the TAB is only used to retrieve data from boards. The Service & Test Board does not have the capability to write to or attempt to otherwise configure slave boards.

The NRC staff reviewed the documentation in Reference 29 and Reference 51 and determined that the MSFIS application of the RAB and TAB buses provide for error detection to preclude the use of invalid data in accordance with the guidance of IEEE 7-4.3.2-2003.

The MSFIS RAB communications sequence is repeated every 10 milliseconds. This 10-millisecond periodic interval consists of 100 time slots (zero to 99) of 100 microseconds each. An individual time slot is dedicated to a master-slave communication exchange with each slave board. A MSFIS isolation valve controller rack contains seven slave boards. The RAB communications between the Core Logic Board and these seven slaves occupy time slots one through seven. The RAB remains idle during the remaining 93 time slots.

The NRC staff reviewed the documentation in Reference 29 and Reference 51 and determined that the communications protocol provided by the ALS platform provides deterministic point-to-point communications in accordance with IEEE 7-4.3.2-2003.

3.1.1.6 Staff Guidance in DI&C-ISG-04

The NRC Task Working Group #4, "Highly Integrated Control Rooms—Communications Issues," has provided interim NRC staff guidance on the review of communications issues. DI&C-ISG-04 contains three sections, 1) Interdivisional Communications, 2) Command Prioritization, and 3) Multidivisional Control and Display Stations.

3.1.1.6.1 DI&C-ISG-04, Section 1 - Interdivisional Communications

Section 1 of DI&C-ISG-04 provides guidance on the review of communications, includes transmission of data and information, among components in different electrical safety divisions and communications between a safety division and equipment that is not safety-related. This ISG does not apply to communications within a single division. As discussed in Section 3.1.1.5.3 of this SE, the MSFIS does not contain any communications with other safety divisions and, therefore, this analysis is only of the communications with equipment which is not safety-related.

Section 3.1.1.5.2 of this SE discusses communications with non-safety systems, and says that this is limited to communications between MSFIS and the ASU for test, diagnostics, maintenance, and troubleshooting of the MSFIS. In particular, NRC staff position 10 states that the safety division software should be protected from alteration while the safety division is in operation. On the ALS system, modification of the FPGA programming or the NVM contents requires removing the board from the system in order to physically connect the FPGA flashing equipment or attaching of the ASU via the USB cable. Removal of any board automatically takes the division off-line and generates an alarm. For the MSFIS, WCGS does not have the FPGA flashing equipment needed and, therefore, the boards must be returned to CS Innovations to modify any programming. This is discussed in Section 3.2.1.11 of this SE. In order to modify the NVM on each board, the board must be physically removed from the rack; ASU must be physically connected via a USB cable. These procedures are discussed in CS Innovations "MSFIS Safety Assessment" document 6101-00006, Revision 0.7, dated June 14, 2007 (Reference 52), and were audited by the NRC staff during a visit to CS Innovations on May 12-16, 2008. The bypass switch, intended to allow plant personnel to place valves into bypass in support of surveillance testing, is a physical switch which closed a circuit and provides the bypass signal to the valve control state machine. This puts the state machine into the bypass mode via a hardware circuit that prevents inputs from being recognized as valid inputs, and prevents a change in the output from changing the valve position. The bypass switch does not allow modification of either the FPGA programming or data contained within the NVM. This is discussed in Section 3.1.1.4.5 of this SE. The NRC staff has, therefore, determined that the ALS system meets the guidance provided by NRC staff position 10. The NRC staff review of the communications between the MSFIS and ASU resulted in a determination that this communications meets NRC staff positions 1 through 20 of DI&C-ISG-04, Section 1.

3.1.1.6.2 DI&C-ISG-04, Section 2 - Command Prioritization

Section 2 of DI&C-ISG-04 provides guidance applicable to a prioritization device or software function block, which receives device actuation commands from multiple safety and non-safety sources, and sends the command having highest priority on to the actuated device. As discussed in Section 3.1.1.5.2 of this SE, there are no input commands to the MSFIS from non-safety sources. As discussed in Section 3.1.1.5.1 of this SE, the MSFIS can receive actuation commands from two sources, automated actuation commands from the SSPS, and manual valve control signals from the operator control panel. These are both safety-related sources, and both perform the safety function of closing the isolation valves. The manual "open" command will be ignored while the automated actuation command from the SSPS is present.

The NRC staff has reviewed the command prioritization of the MSFIS, and has determined that it meets NRC staff positions 1 through 10 of DI&C-ISG-04, Section 2.

3.1.1.6.3 DI&C-ISG-04, Section 3 - Multidivisional Control and Display Stations

Section 3 of DI&C-ISG-04 provides guidance concerning operator workstations used for the control of plant equipment in more than one safety division and for display of information from sources in more than one safety division, and applies to workstations that are used to program, modify, monitor, or maintain safety systems that are not in the same safety division as the workstation. The MSFIS does not use operator workstations for control of the MSFIS equipment. The only workstation used to modify, monitor, or maintain the MSFIS is the ASU, discussed in Sections 3.1.1.5.3 and 3.1.1.6.1 of this SE. Since the ASU is only connected to one MSFIS division while that division is in bypass and not performing its safety function, the programming of the FPGAs can not be changed by the ASU, and the ASU is electrically isolated from the division while connected, the NRC staff has determined that the use of the ASU meets NRC staff positions 1 through 4 of DI&C-ISG-04, Section 3.1, "Independence and Isolation." The NRC staff has further determined that since the only controls and displays for the MSFIS are manual action switches and status indicators on the operators control panel, the MSFIS meets the NRC staff position of DI&C-ISG-04, Section 3.2, "Human Factors Considerations." The NRC staff has also determined that since there are not multidivisional operator workstations, and since the MSFIS has adequate diversity and defense-in-depth (D3) as discussed in Section 3.3.3 of this SE, the guidance provided in DI&C-ISG-04, Section 3.3, "Diversity and Defense in Depth (D3) Considerations," does not apply to the MSFIS.

3.2 Programmable Hardware

As discussed in Section 3.0 of this SE, the MSFIS is an FPGA-based system that does not use software in a traditional sense; however, its FPGAs are programmed, and that program is developed in a manner similar to a traditional μ P-based software program development, with the same versatility and the same potential weaknesses and, therefore, must rely on high-quality programming to meet its design objectives. For this reason, the programming aspect of the MSFIS FPGA is being reviewed in the same manner as a traditional μ P-based software programmed system would be reviewed, that is, the various life cycle stages, with attendant planning documentation and design outputs are being reviewed to the guidance contained in SRP BTP 7-14, and the remainder of the SE Section 3.2 will document that review.

The development, design, V&V, and test of the ALS platform and MSFIS is described in Sections 3.1.1.4.1, 3.2.1.10, and 3.3 of this SE.

3.2.1 Life Cycle Planning Documentation

3.2.1.1 Management Plan

SRP BTP 7-14, in Section B.3.1.1, provides acceptance criteria for software management plans. This section states that Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Reference 135), endorses IEEE Standard 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes" (Reference 117), and that Clause A.1.2.7, "Plan Project Management," contains an acceptable approach to software project management. Clause A.1.2.7 states that the plan should include planning for support, problem reporting, risk management (RM), and retirement.

The management plan used by WCGS is the MSFIS Controls Replacement Project Plan (The Plan), dated August 22, 2007 (Reference 53). The WCGS project plan discusses the project overview, the overall objectives of the project, selection of the vendor, project deliverables, and references the validation and verification, configuration management, quality assurance, training, installation, operations, and maintenance plans. The plan discusses the project organization and defines the roles and responsibilities of the various management personnel involved with the project. The Plan also discusses schedule and cost issues.

The purpose of the NRC staff review of the project management plan is to ensure that the management aspects of the development project demonstrate that high-quality programming will be the result of a deliberate, careful and high-quality development process. The NRC staff has determined that the WCGS project plan was sufficiently comprehensive and appropriate for a project of this type, will result in effective vendor oversight and is, therefore, acceptable.

The requirements for the vendor management plan are the same as that for the licensee. The management plan used by CS Innovations is Reference 31. The management plan is divided into five sections: 1) Project Description, 2) the Project Organization, including Roles and Responsibilities, 3) the Project Life cycle from planning, development, manufacturing and final certification, 4) the Project Schedule, and 5) the Project Delivery. Each of these sections meets the requirements of IEEE Standard 1074-1995, Clause A.1.2.7, "Plan Project Management," and, therefore, is an acceptable method of meeting NRC staff requirements. The "MSFIS Management Plan" does not, however, discuss retirement of the MSFIS system, because the replacement system may not be of similar design or manufacture, and that exception is acceptable for a vendor.

Both the WCGS and CS Innovations management plans are project-specific and are, therefore, not suitable for reuse with future projects.

3.2.1.2 Software Development Plan

As discussed in Section 3.0 of this SE, the MSFIS is an FPGA-based system that does not use software in a traditional sense; however, its FPGAs are programmed, and that program is

developed in a manner similar to a traditional μ P-based software program development. For this reason, the NRC staff had determined that a software or programming development plan is required. The acceptance criteria for a software development plan are contained in the SRP, BTP 7-14, Section B.3.1.2. This section states that Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Standard 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," subject to exceptions listed, as providing an approach acceptable to the NRC staff, for meeting the regulatory requirements and guidance as they apply to development processes for safety system software and that Clause 5.3.1 of IEEE Standard 7-4.3.2-2003 contains additional guidance on software development.

The NRC staff review of the software development is primarily intended to determine that use of the Software Development Plan results in a careful, deliberate and high-quality development process that will result in high-quality programming, suitable for use in safety-related systems in nuclear power plants. While many of the details on how this will be performed may be found in other plans, the important aspect of the software development plan is the method to be used to make sure these other plans are being applied. This includes a provision for effective oversight to monitor the software development process, and to consider risk associated with the size and complexity of the product.

The plan should clearly state which tasks are a part of each life cycle, and state the life cycle inputs and outputs. The review, V&V of those outputs should be defined. The methods and tools to be used during the development process should be evaluated, and the method used to detect defects produced through the use of those methods and tools. The plan should list the international, national, industry, and company standards and guidelines that will be followed during the development process.

Since WCGS is not doing any of the programming for the MSFIS system, WCGS does not have a software development plan. There are management and oversight requirements that are addressed in the same MSFIS Controls Replacement Project Plan (Reference 53), as previously identified, in conjunction with the management plan. The project plan describes the responsibilities of various management positions, and project, cost and schedule management, along with the various plans needed for the design life cycle. The NRC staff has determined that the MSFIS Controls Replacement Project Plan adequately addressed the requirements otherwise associated with a development plan and is, therefore, acceptable.

The CS Innovations development plan is contained in Section 4, "Project Life Cycle," of Reference 31. This section describes each life cycle phase, what inputs are required to start that phase, which tasks are to be accomplished during the phase, and what documented outputs and other criteria are required to exit that phase. Because the ALS platform does not contain traditional software programming, but rather development of the FPGA programming, the life cycle phases discussed are not the same as described in IEEE Standard 1074-1995; however, the NRC staff has determined these life cycle phases are appropriate for development of the MSFIS. In addition, the NRC staff has determined that Section 4 of the "MSFIS Management Plan" adequately describes the ALS development process and, therefore, use of the described life cycle will provide reasonable assurance that the MSFIS will perform the intended safety function. Because the management plan is MSFIS-specific, it is not suitable for

reference in future applications of the ALS platform in safety-related system in nuclear power plants.

3.2.1.3 Quality Assurance Plan

Quality Assurance (QA) A is required by 10 CFR Part 50, Appendix B, and the QA Plan should be implemented under an NRC-approved QA program. 10 CFR Part 50, Appendix B, allows the licensee to delegate the work of establishing and executing the quality assurance program, but the licensee shall retain responsibility. The plan should identify which QA procedures are applicable to specific programming processes, and identify particular methods chosen to implement QA procedural requirements. There are several regulatory guides and standards that offer guidance. While some of this guidance is intended for traditional software development, it is equally applicable for programming of FPGAs.

1. Regulatory Guide 1.28, Revision 3, "Quality Assurance Program Requirements (Design and Construction)" (Reference 122), that endorses American National Standards Institute/American Society of Mechanical Engineers (ANSI/ASME) NQA-1-1983, "Quality Assurance Program Requirements for Nuclear Facilities," and the ANSI/ASME NQA-1a-1983 Addenda, "Addenda to ANSI/ASME NQA-1-1983, "Quality Assurance Program Requirements for Nuclear Facilities."
2. Regulatory Guide 1.152, Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," endorses IEEE Standard 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Clause 5.3.1 "Software Development" of IEEE 7-4.3.2.
3. Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Standard 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes."
4. NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," dated November 1, 1993 (Reference 89), Section 3.1.2, "Software Quality Assurance Plan," and Section 4.1.2, "Software Quality Assurance Plan," contain guidance on these plans.

The NRC staff review of the QA plans is required to determine that the plan exhibits the appropriate management, implementation, and resource characteristics as discussed in the SRP, BTP 7-14, Section 3.1.3, and that use of the plan will result in high-quality software that will perform the intended safety function.

The WCGS "Main Steam & Feedwater Isolation System (MSFIS) Quality Assurance Plan, Revision 0," dated February 16, 2006 (Reference 54), delegated a portion of the effort associated with execution of quality assurance to the vendor, CS Innovations, an independent audit and review contractor, Nutherm International, and an independent V&V contractor, Baseline Engineering. The WCGS QA Plan requires WCGS perform audits, managerial reviews, and supplier oversight. The plan requires, among other items, that problem reporting and corrective action be implemented in accordance with the WCGS 10 CFR Part 50,

Appendix B, program, that all documentation will be collected, maintained, and retained in accordance with WCNO's QA Program, and that RM practices be an integral part of the test program to be performed in accordance with the V&V Plan.

Baseline Engineering, the independent V&V contractor, does not have a QA Plan, but worked under the auspices of the various WCNO's plans and procedures.

CS Innovations "Quality Assurance Manual, Revision 1, dated May 16, 2007 (Reference 55), contains 19 sections on various QA procedures. These are:

1. Organization
2. QA Program
3. Design
4. Procurement Document Control
5. Instructions, Procedures and Drawings
6. Document Control
7. Control of Purchased Equipment and Services
8. Identification and Control of Materials Parts and Components
9. Control of Special Processes
10. Inspection
11. Test Control
12. Control of Measuring and Test Equipment
13. Fabrication, Assembly Handling, Shipping and Storage
14. Inspection, Test and Operating Status
15. Nonconforming Materials, Parts or Components
16. Corrective Action
17. QA Records
18. Audits
19. Contract Review

The NRC staff has reviewed these procedures, and has determined that the manual has the appropriate management, implementation, and resource characteristics, and that use of the procedures listed above provides reasonable assurance of high-quality software that will perform the intended safety function. The NRC staff has, therefore, determined that the manual and the procedures are appropriate for development of programmable FPGA systems for use in safety-related systems in nuclear power plants. The NRC staff also audited the use of these procedures during the May 12-15, 2008, Thread Audit at CS Innovations, and determined that the procedures were being used in an appropriate manner. Because the CS Innovations QA Manual is not specific to the WCGS MSFIS project, it is suitable for use in future projects. Any revision to the manual will need to be reviewed to determine that the revisions did not make the revised manual unsuitable for use when developing safety-related systems for use in nuclear power plants.

The Nutherm International, "Quality Assurance Manual (QA-N-10179-5), Revision 5, dated March 8, 1983 (Reference 56), is also organized into various sections containing procedures for specific quality assurance activities. Nutherm International is a 10 CFR Part 50, Appendix B, qualified contractor that specializes in the manufacture and commercial grade dedication of Class 1E and seismically qualified electrical equipment, and performs a variety of testing

services. While Nutherm International did not perform any of the programming for the MSFIS system, Nutherm International performed or supervised much of the qualification testing on the CS Innovations system and hardware and, therefore, the QA manual was reviewed by the NRC staff. The NRC staff review determined that the Nutherm International QA Manual, QA-N-10179-5, is appropriate for the activities that Nutherm International performed on the MSFIS system and components, and that there is reasonable assurance that use of the Nutherm International QA Manual QA-N-10179-5 in this manner is appropriate for environmental test and qualification of programmable FPGA systems for use in safety-related system in nuclear power plants.

3.2.1.4 Software Integration Plan

The acceptance criteria for a software integration plan are contained in the SRP, BTP 7-14, Section B.3.1.4, "Software Integration Plan." This section states that Regulatory Guide 1.173, endorses IEEE Standard 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," and that within that standard, Clause A.1.2.8, "Plan Integration," contains an acceptable approach relating to planning for integration. Clause A.1.2.8 states that the Software Requirements and the Software Detailed Design should be analyzed to determine the order for combining software components into an overall system, and that the integration methods should be documented. The integration plan should be coordinated with the test plan. The integration plan should also include the tools, techniques, and methodologies needed to perform the integrations. The planning shall include developing schedules, estimating resources, identifying special resources, staffing, and establishing exit or acceptance criteria.

NUREG/CR-6101, Section 3.1.7, "Software Integration Plan," and Section 4.1.7, "Software Integration Plan," provide additional guidance on software integration plans. Section 3.1.7 states that software integration actually consists of three major phases: integrating the various software modules together to form single programs, integrating the result of this with the hardware and instrumentation, and testing the resulting integrated product. It further states that during the first phase, the various object modules are combined to produce executable programs. The second phase is when these programs are then loaded into test systems that are constructed to be as nearly identical as possible to the ultimate target systems, including computers, communications systems, and instrumentation. The final phase consists of testing the results, and is discussed in another report.

As discussed in Section 3.0 of this SE, the MSFIS is an FPGA-based system that does not use software in a traditional sense. While the program is developed in a manner similar to traditional μ P-based software, the FPGA program is not integrated with the hardware in the same manner as traditional software. Depending on the type of FPGA, the programming results in a flash or burn list, and that is flashed or burned into the FPGA in the same manner as a programmable read-only memory device is flashed or burned.

Because all programmable device and system integration is performed by CS Innovations, and the boards and system are delivered to WCGS as completed items, WCGS does not have any programmable device integration activities and, therefore, has no corresponding software integration plan. The NRC staff has determined this is acceptable.

The CS Innovations integration activities are contained in Reference 48; however, the details on how this is done are contained in several documents. The first phase, as described in NUREG/CR-6101, Section 3.1.7, the integrating of various modules together to form single programs, is contained in "FPGA Development Procedure," document 9000-00313, Revision 1, dated October 6, 2008. This procedure describes the derivation of module requirements from the overall FPGA requirements and the process of translating the module requirements into HDL modules. The HDL modules are tested on two diverse test benches, and after proper module operation has been determined, the modules are integrated into a complete HDL description for an FPGA design. This second phase from NUREG/CR-6101, Section 3.1.7, the integrating of various modules together to form single programs, is contained in CS Innovations procedure "Electronics Development Procedure," document 9000-00311, Revision 3, dated October 6, 2008, and the procedure used to flash the FPGA and the setpoint NVM is "ALS Board Flashing," document 9006-00001, Revision 3. The NRC staff audited these procedures during a visit to CS Innovations on December 10-11, 2008, to verify that the FPGA Design Development Procedure was being appropriately implemented. The final phase, testing the results of these integration activities, is described in various board test procedures, and is discussed in Sections 3.1.1.4.1.5.2 and 3.1.1.4.1.5.3 of this SE.

The NRC staff has reviewed these procedures during the December 10-11, 2008, site visit, and observed a demonstration of the process. The NRC staff determined that the documentation provides an acceptable method of integration; and because this procedure is generic to the ALS design process and not specific to the MSFIS, this determination is suitable for reference when using the ALS platform for other safety-related systems in nuclear power plants of similar complexity. However, for future systems of greater complexity, where integration of various programming of greater complexity may be required, the determination of suitability of the integration planning will need to be revisited.

3.2.1.5 Software Installation Plan

The acceptance criteria for a software installation plan are contained in the SRP, BTP 7-14, Section B.3.1.5, "Software Installation Plan. This section states that Regulatory Guide 1.173, endorses IEEE Standard 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," and that Clause A.1.2.4 of that standard, "Plan Installation," contains an acceptable approach relating to planning for installation. This clause states that an installation plan describe the tasks to be performed during installation, and shall include the required hardware and other constraints, detailed instructions for the installer, and any additional steps that are required prior to the operation of the system. Further guidance is provided in NUREG/CR-6101, Section 3.1.8, "Software Installation Plan," and Section 4.1.8, "Software Installation Plan," that contains a sample outline of an installation plan.

Because all programmable device installation is performed by CS Innovations, and the boards and system are delivered to WCGS as completed items, WCGS does not have any software installation activities and, therefore, has no corresponding software installation plan. The NRC staff has determined this is acceptable.

The installation plan reviewed by the NRC staff was the WCGS "Installation Plan for the Replacement MSFIS Controls," Revision 1, dated May 29, 2007 (Reference 57). Because the MSFIS replacement will retain the existing cabinets, external power supply feeds; the

replacement is limited to removal of the existing equipment rack within the cabinets and replacing them with the new racks, assembly panel, and internal wire harnesses. The replacement is limited to two instrumentation cabinets in the Main Control Building within the Control Room equipment area. The installation plan describes the equipment to be removed from the existing cabinets, the equipment to be installed, and lists procedures to be used during this removal and installation. The installation plan also contains items that must be completed before installation can begin, items that must be achieved for the installation to be deemed complete, and an installation schedule. The NRC staff has reviewed the WCGS Installation Plan, Revision 1, and has determined that the plan meets the requirements for an installation plan to be used for installation of safety-related equipment in a nuclear power plant and is, therefore, acceptable. The NRC staff notes that the actual installation and the installation procedures may be audited by the staff of the regional office during the installation. The NRC staff further notes that the installation plan is MSFIS-specific and is, therefore, not suitable for reuse with future FPGA-based systems.

3.2.1.6 Software Maintenance Plan

The acceptance criteria for a software maintenance plan are contained in the SRP, BTP 7-14, Section B.3.1.6, "Software Maintenance Plan." This section states that NUREG/CR-6101, Section 3.1.9, "Software Maintenance Plan," and Section 4.1.9, "Software Maintenance Plan," contain guidance on software maintenance plans. These sections break the maintenance into three activities, failure reporting, fault correction, and re-release procedures.

The WCGS "Maintenance Plan," Revision 1, dated January 21, 2008 (Reference 58), treats the MSFIS system as a hardware-based system. This is based on the fact that WCGS will not identify problems down to the programmable device level, will not be modifying the programmable devices, and that all maintenance will be limited to the board level and above. The maintenance of the device programming has been delegated to the vendor, CS Innovations.

Because all programming maintenance is performed by CS Innovations, and the boards and system are delivered to WCGS as completed items, WCGS does not have any software maintenance activities and, therefore, has no corresponding software maintenance plan. The NRC staff has determined this is acceptable.

WCNOC does have Post Maintenance Test Procedures dated May 6, 2008 (Reference 20). These procedures provide a detailed list of tests to be performed after maintenance. The review and determination of acceptability of these procedures is the responsibility of the staff of the regional office and will, therefore, not be addressed in the SE.

CS Innovations has two documents that contain pertinent information. CS Innovations document 6101-00007, "MSFIS Instruction, Operating & Maintenance Manual," Revision 1, dated March 13, 2008 (Reference 59), contains guidance to operators and technicians on the operation and maintenance of the MSFIS, including guidance on troubleshooting failed or faulted systems. For testing of failed hardware returned for repair, CS Innovations 9006-00008, "Return for Material Repair Procedure," Revision 0, dated January 15, 2009 (Reference 60), describes how failed equipment and boards will be tested and repaired. The NRC staff has reviewed these documents, and has determined that they offer the appropriate level of detail

and guidance for a vendor maintenance plan for FPGA-based systems and are, therefore, acceptable; however, the review of the WCGS operations manuals, including the determination that the CS Innovations guidance has been appropriately incorporated, is the responsibility of the staff of the regional office and will, therefore, not be addressed in the SE. The NRC staff also notes that while the "MSFIS Instruction, Operating & Maintenance Manual" is MSFIS-specific and not suitable for reference with future uses of the ALS platform, Reference 60 is not MSFIS-specific and is, therefore, suitable for reference when using the ALS platform for other safety-related uses in nuclear power plants.

3.2.1.7 Training Plan

The acceptance criteria for a training plan are contained in the SRP, BTP 7-14, Section B.3.1.7, "Software Training Plan." This section states that Regulatory Guide 1.173 endorses IEEE Standard 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes" and that Clause A.1.2.6 of that standard, "Plan Training," contains an acceptable approach relating to planning for training. BTP 7-14, Section B.3.1.7 also states that NUREG/CR-6101, Section 3.1.10, "Software Training Plan," contains further guidance on Software Training Plans.

Clause A.1.2.6 of IEEE Standard 1074 requires different types of training depending on the need. It states that training tools, techniques, and methodologies shall be specified, and that the planning shall include developing schedules, estimating resources, identifying special resources, NRC staffing, and establishing exit or acceptance criteria. This planning shall be documented in the Training Planned Information.

BTP 7-14, Section B.3.1.7, "Software Training Plan," points out that the training plan may be quite simple or very complex, depending on whether the vendor or the licensee is doing the maintenance. The section states that if the licensee has contracted with the vendor to perform the maintenance, the licensee personnel only need to know how to operate the digital equipment, and this is typically less complex than the knowledge required to maintain the equipment. The review guidance also points to an intermediate step, where the licensee personnel perform first level maintenance, determining which sub-unit, such as an individual printed circuit board, is failed, replacing that sub-unit, and then sending the unit to the vendor for repair. This is the case for the MSFIS system.

The WCGS Maintenance Plan, as referenced in Section 3.2.1.6 of this SE, states that "spare boards will be stocked and all troubleshooting and replacement will be at the board level only." WCGS personnel therefore fall into the intermediate step of maintenance, where training is only required to the degree necessary to identify failed boards, replace them, and perform post-maintenance testing.

The WCNOG documentation on training, "Wolf Creek Training Overview, Revision 0," dated May 6, 2008 (Reference 20, pages 33-37), discusses the training provided to WCNOG personnel. This overview documents the training provided for WCNOG technicians and system engineers, and the training provided by the WCNOG Operations training group for the operators on the user interface and overall functions of the ALS platform-based MSFIS Controls. WCNOG also documented the requirement for testing after maintenance to ensure the system is operating correctly. This is in a procedure titled "Post Maintenance Test," Revision 0, dated May 6, 2008 (Reference 20, pages 6-32). The review and determination of acceptability of the

licensee training and the procedures is the responsibility of the staff of the regional office and will, therefore, not be addressed in the SE.

3.2.1.8 Software Operations Plan

The acceptance criteria for a software operations plan are contained in the SRP, BTP 7-14, Section B.3.1.8, "Software Operations Plan." This section states that the primary aspect is completeness; however, it adds that the operations plan needs to address the security of the system, and in particular, the means used to ensure that there are no unauthorized changes to hardware, software and system parameters, and that there is monitoring to detect penetration or attempted penetration of the system.

Because the operation of the system is a licensee, and not a vendor responsibility, there is no requirement for the vendor to have an operations plan and, therefore, there is no CS Innovations plan reviewed in the SE. CS Innovations does have Reference 59 which contains information concerning the operations of the system. Because FPGA-based systems do not contain traditional software, this manual also does not contain a section on the operations of software. The NRC staff has determined that this is acceptable. This manual is application-specific and, therefore, is not suitable for reference in new uses of the ALS platform.

The licensee, WCGS, is responsible for the proper operation of the system and, therefore, developed Reference 50. This plan, in Section 1.2, discusses security requirements, and includes both physical and cyber security aspects of operation of the MSFIS. The NRC staff has reviewed this plan, and in conjunction with the review of the MSFIS communications as discussed in Sections 3.1.1.5 and 3.1.1.5.5 of this SE, and the review of cyber security aspects of the MSFIS and ALS, as discussed in Section 3.3.4 of this SE, has determined that the WCGS operations plan meets the requirements for an operations plan to be used for operation of safety-related equipment in a nuclear power plant and is, therefore, acceptable. The NRC staff notes that the actual operations and the operations procedures may be audited by the staff of the regional office. The NRC staff further notes that the operations plan is MSFIS-specific and is, therefore, not suitable for reuse with future FPGA-based systems.

3.2.1.9 Software Safety Plan

The acceptance criteria for a software safety plan are contained in the SRP, BTP 7-14, Section B.3.1.9, "Software Safety Plan" and Section B.3.2.1, "Acceptance Criteria for Safety Analysis Activities." These sections state that the Software Safety Plan should provide a general description of the software safety effort, and the intended interactions between the software safety organization and the general system safety organization. It further states that NUREG/CR-6101, Section 3.1.5, "Software Safety Plan," and Section 4.1.5, "Software Safety Plan," contain guidance on Software Safety Plans. Further guidance on safety analysis activities can be found in NUREG/CR-6101 and Regulatory Guide 1.173, Section C.3, "Software Safety Analyses," contains guidance on safety analysis activities.

Because the MSFIS system does not contain traditional software, there is no software safety plan. However, the FPGAs and NVMs are programmed and this programming is modifiable; therefore, the safety of the programming and possible unintended changes to the programmed devices needs to be evaluated.

The CS Innovations safety plan is contained in Reference 52. This assessment covers malicious and inadvertent alterations to the MSFIS, as well as component failures and test coverage of the automated self-test features. The assessment also contains the failure modes and effects analysis (FMEA) for board and system level failures, and when combined with the component level FMEAs as described in Section 3.2.1.9.1 of this SE, provides a total system FMEA.

ALS communications is described in Section 3.1.1.5 of this SE, and an assessment of cyber security is described in Section 3.3.4 of this SE. The NRC staff has reviewed these documents, and has determined that the planning for safety is appropriate for this system and is, therefore, acceptable. This determination is specific to the MSFIS and is, therefore, not suitable for reuse with future FPGA-based systems.

As discussed in Section 3.0 of this SE, the MSFIS is an FPGA-based system that does not contain software. For this reason, WCNOG is treating the system as a hardware item (SE Section 3.2.1.6), and WCGS does not have a software safety plan. As discussed in Sections 3.1.1.5.2, 3.1.1.5.5, and 3.3.4 of this SE, the only communications between the safety-related MSFIS to non-safety systems is under administrative controls, alarmed to the operators, buffered by the Service & Test Board, and segregates the safety signal path from the diagnostics, maintenance and troubleshooting path to preclude a cyber intrusion path into the MSFIS. The NRC staff has determined that this is acceptable.

3.2.1.9.1 Failure Modes and Effects Analysis

FMEA is a procedure for analysis of potential hardware or programming failure modes within a system for determination of the effect of failures on the system. This information can then be used to assess the potential for an undetectable failure or a common mode failure. There is no specific regulatory guidance on the required format, complexity or conclusions concerning the FMEA. Each system must be independently assessed by the NRC staff to determine if the FMEA is sufficiently detailed to provide a useful assessment of the potential failures and the effects of those failures.

The CS Innovations document, "MSFIS Safety Assessment" document 6101-00006, Revision 0.7, as mentioned in Section 3.2.1.9 of this SE, contains the FMEA of the MSFIS. This document also contains functional failure path analysis, and discusses test coverage by both automated and surveillance tests. The information provided is proprietary and, therefore, will not be discussed in this SE. The NRC staff has, however, reviewed this information and has determined that the level of detail is appropriate for a system with this degree of complexity, and that the analysis shows that there is reasonable assurance that this system is appropriate for use in this safety-related application at WCGS. The generic portions of this FMEA, the sections

on individual boards and components, are contained in the board hardware specifications. These are as follows:

Document Name	Document #, Revision	Document Date	ADAMS Accession No.	Reference
ALS-101 Hardware Specification	6002-10102, Revision 1	1/15/2009	ML090270688	36
ALS-201 Hardware Specification	6002-20102, Revision 1	1/15/2009	ML090270705	44
ALS-301 Hardware Specification	6002-30102, Revision 1	1/15/2009	ML090270707	38
ALS-401 Hardware Specification	6002-40102, Revision 1	1/15/2009	ML090270955	40
ALS-411 Hardware Specification	6002-41102, Revision 1	1/15/2009	ML090270953	42
ALS-905 Hardware Specification	6002-90502, Revision 0	1/15/2009	ML090270958	46

The NRC staff has reviewed the individual board FMEAs, and has determined that the level of detail is appropriate. Because these board level FMEAs are not MSFIS-specific, they are suitable for reference in the event these boards are used in future safety-related applications of the ALS platform. Any new design of boards intended for use in the ALS platform in safety-related applications would require an equivalent FMEA.

3.2.1.10 Verification and Validation

3.2.1.10.1 Verification and Validation Plans

The acceptance criteria for V&V plans are contained in the SRP, BTP 7-14, Section B.3.1.10, "Software V&V Plan," and Section B.3.2.2, "Acceptance Criteria for Software Verification and Validation Activities." These sections state that Regulatory Guide 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1 (Reference 131), endorses IEEE Standard 1012-1998, "IEEE Standard for Software Verification and Validation" (Reference 114), as providing methods acceptable to the NRC staff for meeting the regulatory requirements as they apply to V&V of safety system software. This section also states that further guidance can be found in Regulatory Guide 1.152, Revision 2, Section C.2.2.1, "System Features," and NUREG/CR-6101, Section 3.1.4 and 4.1.4.

Verification is defined as the process of determining whether the products of a given phase of the development cycle fulfill the requirements established during the previous phase. Validation is defined as the test and evaluation of the integrated computer system to ensure compliance with the functional, performance, and interface requirements. Combined, V&V is the process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill (i.e., implements) the requirements to meet the criteria imposed by the previous phase, and the final system or component complies with specified requirements. This determination may include analysis, evaluation, review, inspection, assessment, and testing of products and processes.

One of the required attributes of V&V is independence. Regulatory Guide 1.168 states that the organization performing the V&V tasks have financial, managerial, and technical independence; however, the NRC staff position is that this does not necessarily mean that a separate company should perform independent V&V. Regulatory Guide 1.168 also states that software used in

nuclear power plant safety systems should be assigned integrity level 4 as defined by IEEE Standard 1012-1998.

There are two V&V plans for the MSFIS project, the V&V plan used during the development of the system by the vendor, and the V&V plan used by the licensee and the independent V&V contractor. The CS Innovations V&V Plan is Reference 47. The V&V activities were performed by personnel from CS Innovations that was not involved with the design of the MSFIS FPGA system, but was involved with the basis design of the ALS concepts and architecture. For this reason, the V&V performed by CS Innovations is not sufficiently independent in management, schedule, and finance to be credited as the only V&V effort for this project.

Despite this lack of independence, this plan follows the requirements of IEEE 1012. During the thread audit of the design process on May 12-16, 2008, the NRC staff found the V&V effort performed by CS Innovations personnel to be thorough and complete. The personnel involved in the V&V effort were qualified, and the NRC staff review of this V&V effort found that the planned V&V activities to be appropriately comprehensive. For any future use of Reference 47, the personnel will either be required to be independent of the design of the ALS platform and the plant-specific design, or a second level of independent V&V, similar to that performed by Baseline Engineering, will be required.

The WCGS V&V activities were planned using WCGS "Design Verification," document AP 05F-001, Revision 3, dated February 6, 2007 (Reference 61). These activities were performed by an independent V&V contractor, Baseline Engineering, using the WCGS plans and procedures. Baseline Engineering is independent from both CS Innovations and WCGS in terms of management, schedule, and finance as required by IEEE Standard 1012-1998. This V&V plan is intended to specifically verify and validate the implementation of the WCGS MSFIS requirements, and does not represent all possible uses of the ALS platform and its boards. In particular, some boards have options on how they are used; however, this plan and the efforts resulting from this plan verify and validate the particular method used to implement the WCGS requirements. In addition, the NRC staff used the output of the Baseline Engineering effort to determine that the lack of independence in the CS Innovations V&V activities did not compromise the required degree of completeness and thoroughness needed for V&V on systems intended for safety-related use in nuclear power plants.

The NRC staff determined that the combination of the CS Innovations and WCGS V&V plans, including the use of an independent V&V contractor, provides reasonable assurance that if these plans are properly executed, the resulting V&V effort is appropriate for safety-related systems intended for use in nuclear power plants and, therefore, these plans are acceptable.

3.2.1.10.2 Verification and Validation Report

Again, there are two sets of V&V reports, those from CS Innovations and those from Baseline Engineering, the WCGS V&V contractor.

Reference 30 reports on the V&V of various stages of the design and test effort. The primary stages discussed are the requirement analysis, design analysis, implementation and test analysis, and the validation test analysis. The NRC staff has reviewed this report, and has determined that the report adequately describes a detailed and thorough V&V effort, and that

the report is written such that the information reviewed, level of detail, and findings of the V&V effort are understandable and informative; and that the effort described include all aspects of V&V required by the V&V plan.

The report on the V&V effort performed by Baseline Engineering is contained in WCGS "MSFIS V&V Report," Revision 2.5, dated January 25, 2009 (Reference 24). This report also contains reports on the V&V activities required by Reference 61. The NRC staff reviewed this report, and determined that the report adequately describes a detailed and thorough V&V effort appropriate for safety-related systems intended for use in nuclear power plants.

The NRC staff has determined that the two V&V reports provide sufficient information to determine that the V&V effort was appropriate for safety-related systems intended for use in nuclear power plants, and the reports are therefore acceptable.

3.2.1.10.3 Requirements Traceability Matrix

The definition of a RTM is contained in SRP, BTP 7-14, Section A.3, definitions, and says: "An RTM shows every requirement, broken down in to sub-requirements as necessary, and what portion of the software requirement, software design description, actual code, and test requirement addresses that system requirement." This is further clarified in Section B.3.3, "Acceptance Criteria for Design Outputs," in the subsection on Process Characteristics. This section states that a RTM, that needs to show every requirement, should be broken down in to sub-requirements as necessary. The RTM should show what portion of the software requirement, software design description, actual code, and test requirement addresses each system requirement.

The RTM for the MSFIS is contained in WCGS "MSFIS V&V Report," Revision 2.5, dated January 25, 2009 (Reference 24). As discussed in Section 3.0 of this SE, because the ALS platform does not contain traditional software programming, but rather development of the FPGA programming, the life cycle phases are not the same as described in IEEE Standard 1074-1995 and, therefore, the RTM sections are not the same as would be expected from a μ P-based application. The NRC staff has determined that the RTM contains the appropriate level of detail for this type of FPGA development. The NRC staff used an earlier version of this RTM during the thread audit on May 12-15, 2008, and was able to trace various WCGS requirements through the CS Innovations requirements and, when appropriate, determine what portion of the HDL code implemented that requirement. The NRC staff was also able to determine where the particular requirement was being tested. The results of the thread audit, along with a review of the RTM itself, led the NRC staff to the determination that the RTM was appropriate for review of the development effort of FPGA-based safety-related systems intended for use in nuclear power plants, and the RTM is therefore acceptable. The RTM is MSFIS-specific and, therefore, not suitable for reference in future safety-related applications of the ALS platform.

3.2.1.11 Configuration Management Plan

The acceptance criteria for configuration management plans are contained in the SRP, BTP 7-14, Section B.3.1.11, "Software Configuration Management Plan," and Section B.3.2.3, "Acceptance Criteria for Software Configuration Management Activities." These sections state that both Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital

Computer Software Used in Safety Systems of Nuclear Power Plants,” that endorses IEEE Standard 1074-1995, “IEEE Standard for Developing Software Life Cycle Processes” Clause A.1.2.4, “Plan Configuration Management,” and Regulatory Guide 1.169, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants” (Reference 132), that endorses IEEE Standard 828-1990, “IEEE Standard for Configuration Management Plans” (Reference 110), provide an acceptable approach for planning configuration management. BTP 7-14, Section B.3.1.11 further states that additional guidance can be found in IEEE Standard 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems on Nuclear Power Generating Stations,” Clause 5.3.5, “Software configuration management,” and in Clause 5.4.2.1.3, “Establish configuration management controls.” NUREG/CR-6101, Section 3.1.3, “Software Configuration Management Plan,” and Section 4.1.3, “Software Configuration Management Plan,” also contain guidance.

Configuration management provides the methods and tools to identify and control the system and programming throughout its development and use. Activities include 1) the identification and establishment of baselines, 2) the review, approval, and control of changes, 3) the tracking and reporting of such changes, 4) the audits and reviews of the evolving products, and 5) the control of interface documentation. Configuration management is the means through which the integrity and traceability of the system are recorded, communicated, and controlled during both development and maintenance. The configuration management plan needs to include an overview description of the development project and identify the configuration items that are governed by the plan. The plan will also identify the organizations, both technical and managerial, that are responsible for implementing configuration management.

The configuration management plan used by WCGS is the WCNO “Configuration Management Plan,” Revision 2, dated February 16, 2008 (Reference 62). The configuration management plan used by CS Innovations is CS Innovations 6002-00002, “ALS Configuration Management Plan,” Revision 2, dated July 28, 2008 (Reference 63). A non-proprietary version of this plan was also submitted (Reference 64).

The contents of these plans were compared to IEEE Standard 828-1998, “IEEE Standard for Software Configuration Management Plans,” and ANSI/IEEE Standard 1042-1987, “IEEE Guide to Software Configuration Management” (Reference 116). IEEE Standard 828-1998 is a revision of the 1990 version of the standard. As previously discussed, these standards are appropriate due to the programmable nature of the FPGA.

CS Innovations does not have a separate configuration management organization, but assigns the configuration management responsibilities to the program manager for each project. Due to the small size of CS Innovations, the program manager acts as the software librarian. The program manager is responsible for entering various design documents into the configuration management system. CS Innovations uses a software tool, “Concurrent Versions System,” to establish and manage the configuration of the hardware and FPGA programming. Items under configuration management are the hardware and FPGA programming documentation, the hardware configuration data for the design and test tools, the software used for design and test, all plan and specification documentation used for each project, the project test procedures and test cases, software tools used in the design process, and the dedicated test equipment developed by CS Innovations. The quality assurance manager is responsible for performing reviews and in-process audits of the configuration management documentation and process.

CS Innovations baselines the configuration of all design outputs at the end of each design phase, and once baselined and entered into the configuration management process, changes can only be initiated by engineering change notice. During the thread audit on May 12-15, 2008, the NRC staff reviewed the change process. The NRC staff postulated several changes, and followed the change process through the development and review procedures. The NRC staff determined that the process is in accordance with the requirements of IEEE 1042 and is, therefore, acceptable.

The NRC staff determined that the CS Innovations configuration management plans, procedures and activities meet the requirements of IEEE Standard 828-1998 and ANSI/IEEE Standard 1042-1987 and are, therefore, acceptable.

The WCGS configuration management process is related to the standard WCGS configuration management processes and procedures as documented in the WCNOG "AP 05-005, 'Design, Implementation & Configuration Control of Modifications,' Revision 11A" (Reference 65). This is not a project-specific process and, therefore, while it was reviewed by the NRC staff, AP 05-005 not considered to be a process for approval within the scope of the MSFIS LAR.

WCGS configuration management, as documented in WCNOG Configuration Management Plan, Revision 2, treats the FPGA system as a hardware item. As WCGS has explicitly stated that there will be no on-site capability for modification of the FPGA programming, this is acceptable. If the licensee had the capability to modify the FPGA programming without going through the configuration management procedures within CS Innovations, then the licensee would be required to have configuration management procedures that would be appropriate for programmable devices.

WCGS configuration management depends on the standard WCNOG design change process, where each change is evaluated for suitability and correctness. This process includes independent evaluation of the design change package by a qualified WCGS engineer. This independent evaluation by WCGS of a design change is performed prior to installation and occurs in addition to the V&V performed by the vendor and licensee during the design process. WCGS also maintains oversight of CS Innovations as a Class 1E supplier, in addition to having a Qualification and Quality Oversight Contractor, Nutherm International, to provide independent oversight of the requirements on the qualification of a safety-related system. As mentioned in the Section 3.2.1.10 of this SE on V&V, WCGS also used Baseline Engineering as an independent V&V contractor.

The WCGS Configuration Management Plan states that the following items be maintained under configuration management: 1) Project Control Documents, 2) System Design including Drawings, Documents, and Analyses, 3) Test Documents, 4) Test Data, and 5) Documentation of the installed system. The WCGS configuration management plan requires configuration review 1) prior to manufacture of the item that will be subjected to qualification testing (i.e. first article pre-production), 2) upon implementation completion of an ALS-based system or ALS platform board, and 3) prior to the first factory acceptance test of a production ALS-based system, such as MSFIS, or an ALS-based spare board. Configurations audits will be performed subsequent to design completion and MSFIS factory acceptance completion. All changes to controlled items must use engineering change notice.

The NRC staff has reviewed the CS Innovations and the WCGS configuration management plans, and has determined that these configuration management methods meet the requirements of IEEE Standard 828-1998 and ANSI/IEEE Standard 1042-1987 and are, therefore, acceptable. The NRC staff notes that both WCNOG Configuration Management Plan, Revision 2, and CS Innovations Report 6002-00002, revision 2, are not MSFIS-specific, both are suitable for reference in future safety-related applications at nuclear power plants.

3.2.1.12 Test Plan

The acceptance criterion for Test Plans is contained in the SRP, BTP 7-14, Section B.3.1.12, "Software Test Plan," and in Section B.3.2.4, "Acceptance Criteria for Testing Activities." These sections state that both Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Reference 133) that endorses IEEE Standard 829-1983, "IEEE Standard for Software Test Documentation" (Reference 111), and Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," that endorses IEEE Standard 1008-1987, "IEEE Standard for Software Unit Testing" (Reference 113), identify acceptable methods to satisfy software unit testing requirements.

The purpose for the test plan is to prescribe the scope, approach, resources, and schedule of the testing activities; to identify the items being tested, the features to be tested, the testing tasks to be performed, the personnel responsible for each task, and the risks associated with the plan. The test plan should cover all testing performed to the system and programming, including unit testing, integration testing, factory acceptance testing, site acceptance testing, and installation testing. The test plan needs to be understandable, ensure that testing responsibilities have been given to the appropriate personnel, and that adequate provisions are made for retest in the event of failure of the original test.

There are two test plans developed and used by CS Innovations, the "6000-00008, 'ALS Board Test Plan (and Procedures),' Revision 0.8, dated June 9, 2007 (References 66 and 67), and the "6101-00004, 'MSFIS System Test Plan,' Revision 0.8," dated June 9, 2007 (Reference 68). The Board Test Plan is a unit test, while the System Test Plan tests the system as an integrated system. Additional test documentation for the test equipment used for the ALS platform is contained in CS Innovations document ATE-101 Design Specification, document number 6101-00100, Revision 0, and in ATU-101 Design Specification, document 6101-00101 Revision 0, both dated June 9, 2007 (Reference 69).

The NRC staff has reviewed these plans. The ALS Board Test Plan is both a test plan and test procedure, and is sufficiently comprehensive to determine that the board testing provides reasonable assurance that the boards are useable in safety-related systems in nuclear power plants. This board test plan is not MSFIS-specific and is, therefore, suitable for reference in future safety-related uses of these boards; however, the board test plans only include those boards used in the MSFIS system, and any new board developed for future applications will require equivalent test plans and NRC staff approval of those new plans.

As discussed in Section 3.2.1.4 of this SE, due to the nature of the MSFIS system, there was no need for software integration testing and, therefore, no need to include software integration testing in the test plan. As was mentioned in Section 3.2.1.4 of this SE, for future systems of

greater complexity, where integration of various programming modules may be required, this determination will need to be revisited.

The CS Innovations MSFIS System Test Plan is a combination of test plan and test procedures. Staff review of this plan determined that the plan was sufficiently comprehensive to determine that the MSFIS system will meet its required functionality and that there is reasonable assurance that the MSFIS system will perform its safety function. The system test plan is MSFIS-specific, and is not suitable for reference in future use.

The MSFIS System Test Plan will also be used as both the factory acceptance test and the site acceptance test. The NRC staff review of the MSFIS System Test Plan has determined that this is acceptable for use as the factory acceptance test. The acceptability of the site acceptance test is the responsibility of the staff of the regional office, and therefore this SE will not address this issue.

The WCGS Installation Plan discussed in Section 3.2.1.5 of this SE states that the Post Maintenance Test procedure, mentioned in Section 3.2.1.6 of this SE, will be used as the installation test. Because it has been determined that review and acceptance of both the site acceptance and installation test are the responsibilities of the staff of regional office, the acceptability of these test will not be addressed in this SE.

3.2.2 Design Outputs

3.2.2.1 Requirements Specification

The acceptance criteria for the Requirements Specification is contained in the SRP, BTP 7-14, Section B.3.3.1, "Requirements Activities - Software Requirements Specification." This section states that Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (Reference 134), endorses IEEE Standard 830-1993, "IEEE Recommended Practice for Software Requirements Specifications" (Reference 112), and that standard describes an acceptable approach for preparing software requirements specifications for safety system software. The section also states that additional guidance can be found in NUREG/CR-6101, Section 3.2.1, "Software Requirements Specification," and Section 4.2.1, "Software Requirements Specifications."

IEEE Standard 830 was specifically written to address software requirements specification and, therefore, needs to be interpreted to address a programmable but not software driven FPGA-based system. The basis requirements for this specification remain unchanged. The requirements specification needs to address a number of basic issues that are unchanged whether or not the specification is for an FPGA-based or a μ P-based system. The items that need to be addressed are the functionality, external interfaces, performance, attributes, and design constraints imposed on an implementation.

The basis WCGS specification for the MSFIS is WCGS "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 16, 2009 (Reference 25). This document was the starting point for all future design and development. The CS Innovations requirement specification that was developed from the WCGS is the proprietary References 27 and 28.

The NRC staff reviewed the requirements documents and the portion of the V&V reports, Reference 30 and WCGS "MSFIS V&V Report," Revision 2.5, dated January 29, 2009 (Reference 24). The NRC staff also used the RTM during the May 12-15, 2008, Thread Audit at CS Innovations to trace the requirements from the WCGS requirements to the CS Innovations requirements. The NRC staff determined that each WCGS requirement was appropriately included in the CS Innovations requirements.

3.2.2.2 Software Architecture Description

The acceptance criteria for the software architecture description is contained in the SRP, BTP 7-14, Section B.3.3.2, "Design Activities - Software Architecture Description." This section states that the Software Architecture Description should describe all of the functional and software development process characteristics listed, and that NUREG/CR-6101, Section 3.3.1, "Hardware and Software Architecture," and Section 4.3.1, "Hardware/Software Architecture Specifications," contain relevant guidance.

When performing this review, the NRC staff should be able to refer to this architecture to understand how the software works, the flow of data, and the deterministic nature of the software. The architecture should be sufficiently detailed to allow the reviewer to understand the operation of the software.

As discussed in Section 3.0, the FPGA-based MSFIS does not contain traditional software, but is programmed. For this review, the NRC staff examined the submitted documentation to determine if the architecture of the programming was sufficiently described for the NRC staff to reach an equivalent level of confidence in the programming as would be required for a software-based system.

Since the MSFIS does not have traditional software, there is no software architecture or software and architecture description. The ALS platform defines hardware architecture, and that architecture is reflected in the HDL programming of the FPGA. The ALS and MSFIS architecture is contained in three documents, the CS Innovations documents Reference 32 and Reference 33, and References 27 and 28. A non-proprietary description of the ALS platform, including the architecture, was provided in Reference 29. These documents were sufficiently detailed to allow the NRC staff to understand how the overall system works and the flow of data within the system and are, therefore, acceptable. The CS Innovations documents Reference 32, Reference 33, and Reference 29 are generic and not MSFIS-specific and are, therefore, suitable for reference in future applications of the ALS platform in safety-related applications in nuclear power plants. The discussion of the MSFIS architecture in References 27 and 28 is application-specific, and in future uses of the ALS platform, this information should be contained in the application-specific specification.

WCGS did an analysis of the MSFIS architecture in "ALS Architecture Evaluation," Revision 0 dated February 25, 2008 (Reference 70 [proprietary], Reference 71 [non-proprietary]). The NRC staff reviewed this analysis, and agrees with the WCGS conclusion that the ALS architecture is acceptable for use as MSFIS controls replacement as well as generic safety-related use at WCGS. Future applications of the ALS platform at WCGS will not need a similar analysis.

3.2.2.3 Software Design Description

The acceptance criteria for the software design description is contained in the SRP, BTP 7-14, Section B.3.3.3, "Design Activities - Software Design Specification." This section states that the software code accurately reflects the software requirements, and that NUREG/CR-6101, Section 3.3.2, "Software Design Specification," and Section 4.3.2, "Software Design Specifications," contain relevant guidance.

Because the FPGA-based MSFIS system does not contain traditional software, there is no software design description. Instead, the FPGAs have hardware design descriptions and HDL programming, and that design and programming is discussed in References 27 and 28. More detailed descriptions of the HDL and the HDL code itself were examined by the NRC staff during the May 12-15, 2008, Thread Audit at CS Innovations. The thread audit checked a number of system and programming requirements using the requirement traceability matrix (contained within Reference 68), and followed the requirements through the design process. Particular attention was paid to the records of V&V activities and audits. Through the evaluation of References 27 and 28 and the thread audit, the NRC staff determined that sufficient information existed and was sufficiently understandable so that the intent of design description was met for the MSFIS FPGA programming that was audited and is, therefore, acceptable. Because a system level design description is application-specific, for any future use of the ALS platform or ALS board with application-specific programming in a safety-related system in nuclear power plants, this design description information should be contained in the application-specific documents and is not suitable for reference. However, for the standard printed circuit boards that contain programming that is not application-specific and that have been used in the MSFIS, which are the ALS-301, ALS-401, and ALS-411, to the degree approved by this SE, the board and FPGA level design descriptions are not application-specific; therefore, for future similar uses of these standard boards within an ALS-based system, the board and FPGA level design descriptions are suitable for reference in a safety-related applications in nuclear power plants.

3.2.2.4 Software Design Review

There are no specific acceptance criteria for a software design review. This review is the NRC staff review of the code listings, generally performed during the thread audit. The criteria for the code listings are contained in the SRP, BTP 7-14, Section B.3.3.4, "Implementation Activities - Code Listings." This section states that NUREG/CR-6463, Revision 1, "Review Guidelines for Software Languages for Use in Nuclear Power Plant Safety Systems" (Reference 91), contains relevant guidance.

For an FPGA-based system, the equivalent of code listings is the HDL listings. NUREG/CR-6463 does not discuss HDL, and as this is the first-of-a-kind use for FPGAs and HDL, no specific Reference coding standards were available. The NRC staff based its acceptance of the HDL listings on the ability to understand and follow the listing, and to understand the functionality of the code. The thread audit consisted of selecting various system or programming requirements, and using the RTM to determine if the requirement was adequately addressed in all subsequent documentation and in the test. The V&V effort for each phase of the design was reviewed. In the case of HDL listings, the RTM was used to determine

where in the HDL the requirement was addressed, this portion of the HDL was reviewed line-by-line, and the test for the requirement was examined to determine if the test actually determined the resulting system met the requirement. To audit verification for a sampling of requirements, the NRC staff asked CS Innovations personnel to perform testing to demonstrate test coverage and traceability of requirements through verification. The test procedures and results were examined to determine that the test results were appropriate. Based upon this review, the NRC staff determined that the programming design review was appropriate for safety-related use at nuclear power plants, and the HDL listings were appropriate for the MSFIS. Because HDL listings may be application-specific, for any future use of the ALS platform or ALS board with application-specific programming in a safety-related system in nuclear power plants, these HDL listings should be contained in the application-specific documents and is not suitable for reference. However, for the standard printed circuit boards that contain programming that is not application-specific and that have been used in the MSFIS, which are the ALS-301, ALS-401, and ALS-411, to the degree approved by this SE, the board and HDL listings are not application-specific; therefore, for future similar uses of these standard boards within an ALS-based system, the HDL listing are suitable for reference in a safety-related applications in nuclear power plants.

3.2.2.5 System Build Documents

The acceptance criteria for the system build documentation are contained in the SRP, BTP 7-14, Section B.3.3.5, "Integration Activities - System Build Documents." This section states that NUREG/CR-6101, Section 3.5.1, "System Build Documents," and Section 4.5.1, "System Build Documents," contain relevant guidance.

The build documentation is generally needed to verify that the programs actually delivered and installed on the safety system is the programming that underwent the V&V process and was tested. Any future maintenance, modifications or updates will require that the maintainers know which version of the programming to modify and, therefore, the system build documentation is closely tied to the configuration management program. The items, including programming, should check to ensure that the programming listed in the build documentation is identified by version, revision, and date, and that this is the version and revision that was tested.

For the MSFIS system, the information on the boards that underwent the V&V and test procedures is contained in Appendix F of Reference 30. The exact system configuration delivered to WCGS for use as the MSFIS is contained in the same V&V report, in Section 7.6. The actual comparison of this data to the delivered equipment is the responsibility of the staff of the regional office, and will not be verified in the SE.

3.2.2.6 Installation Configuration Tables

The acceptance criteria for the system build documentation is contained in the SRP, BTP 7-14, Section B.3.3.6 Installation Activities - Installation Configuration Tables.

This section states that in the event that the programming has options for use, variable setpoints or other data, or may operate in various methods, the programming needs to be configured for the particular plant requirements. Any item that is changeable should have the intended configuration recorded in the Installation Configuration Tables, and the reviewer should sample

these configuration items to verify that they are correct. The reviewer should verify that the V&V team has already made this determination, and should then sample various items.

For all ALS boards, including the MSFIS, this information is contained in the completed ALS SetPoint Flashing Procedure, CS Innovations form 9002-000007. This form is a part of each board's traveler, a collection of documentation that contains information on each individual board, and contains the schematics, assembly drawings and procedures, completed procedures for the FPGA and memory flashing, and completed test reports for the board and system. An example of a board traveler can be found in Appendix H of Reference 30. The actual comparison of this data to the delivered equipment is subject to NRC inspection.

3.3 System Qualifications

3.3.1 Environmental Qualification of System

Two objectives of the MSFIS system environmental testing are 1) to demonstrate that the system will not experience failures due to abnormal service conditions of temperature, humidity, power source, radiation, or seismic, and 2) to verify those tests meet the WCGS requirements.

Criteria for environmental qualifications of safety-related equipment are provided in 10 CFR Part 50, Appendix A, "General Design Criterion (GDC) 2, "Design Bases for Protection Against Natural Phenomena," and GDC 4, "Environmental and Dynamic Effects Design Bases." Additionally, 10 CFR 50.55a(h) incorporates IEEE Standard 603-1991, that addresses both system-level design issues and quality criteria for qualifying devices. Section 5.4 of IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," states that its use is in conjunction with the equipment qualification requirements for the safety systems of IEEE Standard 323, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations" (Reference 97). Regulatory Guide 1.89, Revision 1 (Reference 127) endorses and provides guidance for compliance with IEEE Standard 323-1974.

To comply with the requirements of GDC 4, 10 CFR 50.49 ("Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants"), and IEEE 603-1991, the licensee must demonstrate through environmental qualification that instrumentation and control (I&C) systems meet design-basis and performance requirements when the equipment is exposed to normal and adverse environments. The following subsections discuss the NRC staff's review of the MSFIS system environmental testing submitted by Nutherm International, Inc. (Nutherm), which was contracted by WCNOG as the third-party qualifier.

The NRC staff conducted its reviews in accordance with the guidance provided in Appendix 7.1-A to SRP Revision 5, dated March 2007 (NUREG-0800), that references Appendix 7.1-B and Appendix 7.1-C. These two appendices reference IEEE Standard 323-1974, and Electric Power Research Institute (EPRI) Topical Report (TR)-102323, Revision 2, "Guidelines for Electromagnetic Interference Testing in Power Plants," dated November 2000 (Reference 92).

The overall test requirements are contained in two documents. The testing to be performed on individual boards and on a generic ALS platform-based system is contained in CS Innovations document 6002-00004, "ALS EQ Plan," Revision 2, dated February 20, 2009 (Reference 34).

The MSFIS-specific testing is contained in WCGS "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 16, 2009 (Reference 25). The tests required by these two documents are the same; however, the WCGS specification provides required limits for temperature, humidity and seismic testing.

3.3.1.1 Equipment Description and Testing

The MSFIS system is described in Section 3.1 of this SE. The test specimen consists of one channel of the proposed main steam isolation circuits and its associated assembly panel as used in the WCGS MSFIS system. The test specimen is representative of the entire system and will serve as the basis for qualification.

The licensee's MSFIS is located in the control room of the WCGS. The environmental conditions for this location are defined in Section 5.4 of WCGS "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 16, 2009 (Reference 25), as a mild environment. The licensee performed an environment qualification test program for a mild environment, as defined in Clause 3 of IEEE Standard 323-1974. The test sequence of WCGS MSFIS system for the environment qualification test program includes the following:

1. Pre-test inspection - Visually inspected the test specimen to verify no damage has occurred due to handling or during shipment, and to establish an identification number for the test specimen.
2. Baseline functional test - Verified the proper operation of the system in accordance with Nutherm technical procedures.
3. Electromagnetic compatibility (EMC) test - Verified that the susceptibility and emissions characteristics of the system are suitable for use in nuclear power plant safety system applications. EMC testing consists of the following:
 - Pre-EMC Testing Inspection and Operability Check
 - Qualification Level EMC Emissions Testing
 - Qualification Level EMC Susceptibility Testing
 - Qualification Level EMC Surge Withstand Capability Testing
 - Post-EMC Testing Inspection and Operability Check
4. Baseline functional test - Repeated the baseline test to detect any change in performance following the EMC test.
5. Switch cycle aging test - Performed on the operate/bypass toggle switch located on the ALS-201 board.
6. Baseline functional test - Repeated the baseline test to detect any change in performance following the switch cycle aging test.
7. Seismic test - Performed a resonance search followed by a random multi-frequency (RMF) seismic simulation test program in accordance with a Nutherm seismic procedure and IEEE 344-1975 (Reference 99). The seismic testing included the following:

- Pre-seismic Inspection and Operability Check
 - Resonance Search
 - Pre-RMF Inspection and Operability Check
 - Qualification-level Multi-frequency Tests
 - Post-seismic Baseline Test and Operability Check
8. Post-test inspection - Inspected visually to document the condition of the test specimen after the test.
 9. FPGA verification - Performed to provide information on any changes that might have occurred within the FPGA chips.
 10. Post-test inspection - Inspected visually to document the condition of the test specimen after the test.

Elite Electronic Engineering, Inc. (Elite), performed the EMC testing at its test laboratories in accordance with Nutherm EMC Test Procedure 9715-EMC-01, Revision 4 (Reference 72). The EMC testing of MSFIS system follows the guidance of EPRI TR-102323, Revision 2, as endorsed and modified by Regulatory Guide 1.180, Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems" (Reference 136). Before and after every qualification test, Elite performed an inspection and operability check on the test specimen to verify equipment operation.

Wyle Laboratories, Inc. (Wyle), performed the seismic testing at its laboratories in accordance with Nutherm Seismic Test Procedure S-128P, Revision 2 (Reference 72). The seismic test verified structural integrity during a seismic event and documented any output discontinuities that may develop. Pre-seismic baseline testing, seismic monitoring that included an engineered safety features actuation system (ESFAS) "all valves closed" signal during the final safe-shutdown earthquake (SSE) test run, and post-seismic baseline test data supported the ability of the equipment to operate during and after the seismic event.

The following documents describe the detailed Nutherm test procedures and results:

Document Title	Document Number	ADAMS Accession No.	Reference
Nutherm Qualification Report	WCN-9175R, Revision 0	ML071160369	72
Nutherm International Inc., Technical Procedures: Baseline Testing for Main Steam And/or Feedwater Isolation System (MSFIS) Rack	TSP-9059, Revision 0, and Revision 1	ML071160369	72
Nutherm International Inc., Technical Procedures: Dielectric Strength Testing Test Report	TPG-0002, Revision 0	ML071160369	72
Nutherm International Inc., Technical Procedures: Cycle Aging of Control Switches Test Report	TPG-4751, Revision 0	ML071160369	72
Nutherm Qualification Report Seismic Test Procedure	S-128P, Revision 2	ML071160369	72

Document Title	Document Number	ADAMS Accession No.	Reference
Nutherm Qualification Report Seismic Test Data	WCN-9175R, Revision 0, Appendix V	ML071160369	72
Nutherm Qualification Report EMC Test Procedure	9715-EMC-01, Revision 4	ML071160369	72
Nutherm Qualification Report EMC Test Data	Elite Eng. Test Report No. 37485-01	ML071160369	72
Nutherm Qualification Report EMC Test Report with Data	WCN-9175R, Revision 0, Appendix VI	ML071160369	72
Nutherm Qualification Report Records of Anomaly	ROA-148	ML071160369	72
Nutherm Qualification Report Pre- and Post-EMC Baseline Test Results	WCN-9175R, Revision 0, Appendix VI	ML071160369	72
Test, Inspection, and QA Activities Report	9715-TR-01R, Revision 0 P	ML081290379	73

3.3.1.2 Temperature and Humidity Testing

Clause 3 of IEEE Standard 323-1974 defines the mild environment as “An environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences.” The licensee’s MSFIS system is located in the control room equipment cabinet area with air-conditioning and with the environmental parameters as described in the previous section.

Section 5.4 of WCGS “Specification J-105A(Q) for Replacement MSFIS System,” Revision 5, dated February 16, 2009 (Reference 25), states the WCGS control room is a mild environment, with normal operating temperature conditions of 65 °F to 84 °F and relative humidity of 20 percent to 70 percent. The WCGS Updated Safety Analysis Report (USAR), Revision 21, page 3.11(B)-22, Table 3.11(B), provides the worst-case operating conditions as a maximum temperature of 105 °F and a maximum humidity of 71 percent.

Reference 32 states that the operational temperature and humidity range for the ALS platform is 5 degrees Celsius (°C) to 60 °C (41 degrees Fahrenheit (°F) to 140 °F) with up to 95 percent relative humidity (non-condensing). Temperature and humidity testing on the ALS platform was performed by National Technical Services in accordance with Mil-Standard-810F, Method 501.3, run for one 144-hour cycle, and Mil-Standard-810G, method 507.5, run for two cycles of 24 hours each. This testing was documented in CS Innovations documents 6002-00206, “NTS Temperature Test Report,” Revision 0, dated January 14, 2009 (Reference 148), and 6002-00209, Humidity Test Surveillance Report, Revision 0, dated February 23, 2009 (Reference 26). These test reports are not MSFIS-specific, and are suitable for reference when using the ALS platform for other safety-related uses in nuclear power plants. Any new design of boards intended for use in the ALS platform in safety-related applications would require equivalent temperature and humidity testing.

WCGS has stated that the worst case environment in the control room during accident condition is 105 °F at 71 percent humidity. Since the ALS platform exceeds that requirement by being qualified to operate at 140 °F at 95 percent humidity, the NRC staff determined that the MSFIS is qualified for the WCGS control room temperature environment.

3.3.1.3 Radiation Withstand Testing

Because the MSFIS equipment is located in a mild environment in the control room the radiation exposure for a 40-year life is less than 200 rads. Digital systems susceptibility to radiation is discussed in Regulatory Guide 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants." This Regulatory Guide states that the radiation threshold is different for different types of digital technology, ranging from complementary metal oxide semiconductor, which can be susceptible as low as 1000 rad exposure, to bipolar devices, which are not susceptible until around 1 million rads. The maximum expected exposure level of 200 rads for the WCGS MSFIS is well below the minimum exposure required to cause degradation in any of these technologies, and therefore radiation aging is not required for the ALS platform in the WCGS environment. For this reason, the NRC staff finds the MSFIS system is acceptable to operate at the WCGS control room within the radiation exposure limit.

3.3.1.4 Electromagnetic Compatibility Testing

Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," endorses MIL-STD-461E and IEC 61000 series to evaluate conducted and radiated electromagnetic and radiofrequency interference (EMI/RFI) and power surges on safety-related I&C systems.

EPRI TR-102323, "Guideline for Electromagnetic Interference Testing in Power Plants," provides alternatives to perform site-specific EMI/RFI surveys to qualify digital plant safety I&C equipment in a plant's electromagnetic environment. In an SE issued in 1996, the NRC staff concluded that the recommendations and guidelines in EPRI TR-102323 provide an adequate method for qualifying digital I&C equipment for a plant's electromagnetic environment without the need for plant-specific EMI/RFI surveys if the plant-specific electromagnetic environment is confirmed to be similar to that identified in EPRI TR-102323.

Regulatory Guide 1.180 says, in the discussion section, that both the Regulatory Guide 1.180 and EPRI TR-102323 present acceptable means for demonstrating EMC, and that the licensee or applicant has the freedom to choose either method. It should be noted that for some types of testing, the maximum acceptable limits for emissions or susceptibility are different and, therefore, it is possible that tested equipment may meet the requirements of one test, and not meet the requirements of the equivalent test from the other document. Regulatory Guide 1.180 states that this is acceptable, as long as the requirements of a complete suite of EMI/RFI emissions and susceptibility criteria are met, with no mixing and matching of test criteria and methods.

EMC tests on the MSFIS system were conducted in accordance with EPRI TR-102323, Revision 2, issued November 2000, as modified by Regulatory Guide 1.180, Revision 1. EMC testing of the MSFIS system included the following:

- Pre-EMC Testing Inspection and Operability Check
- Qualification Level EMC Emissions Testing
- Qualification Level EMC Susceptibility Testing

- Qualification Level EMC Surge Withstand Capability Testing
- Post-EMC Testing Inspection and Operability Check

Nutherm EMC Test Procedure 9175-EMC-01, Revision 4, "EMI/RFI Test Procedure," and Elite Test Report No. 37485-01, "EMC Test Data" (Reference 72), describe details of the EMC tests and measurements for the MSFIS system. Specifically, Elite conducted the following EMC tests when the licensee submitted its LAR on March 14, 2007:

EMC Test	Description	Range
CE 101	Low-frequency conducted emissions	30 Hertz (Hz) to 10 kilohertz (kHz)
CE 102	High-frequency conducted emissions	10 kHz to 10 megahertz (MHz)
CS 101	Low-frequency conducted susceptibility	30 kHz to 150 kHz
RE 101	Radiated magnetic field emissions	30 Hz to 100 kHz
RE 102	Radiated electric field emissions	10 kHz to 10 gigahertz (GHz)
RS 101	Radiated magnetic field susceptibility	30 Hz to 100 kHz
IEC 61000-4-3	Radiated electric field susceptibility	26 MHz to 10 GHz
IEC 61000-4-4	Electrical fast transient/burst conducted susceptibility	2 kilovolts (kV)
IEC 61000-4-5	Surge conducted susceptibility	2 kV
IEC 61000-4-6	Disturbances induced by radio-frequency fields conducted susceptibility	10 kHz to 200 MHz
IEC 61000-4-8	Radiated magnetic field susceptibility	50 Hz and 60 Hz
IEC 61000-4-12	Ring wave susceptibility	2 kV
IEC 61000-4-16	Common-mode conducted susceptibility	0 Hz to 150 kHz
Not Applicable	Verification and safety function actuation data sheet	Not Applicable

After reviewing the submittals of the licensee's LAR, the NRC staff compared the submitted EMC tests with the EMC test requirements in Regulatory Guide 1.180, Revision 1, and EPRI TR-102323, Revision 2. The NRC staff found that the submitted EMC tests did not cover a complete test set of either (1) EMI/RFI test methods in MIL-STD-461E or (2) EMI/RFI test methods in IEC 61000-4 as specified in Regulatory Guide 1.180, Revision 1. The NRC staff issued a request for additional information to question the completeness of the WCGS EMC tests on December 7, 2007, and the licensee performed and submitted the following two additional tests:

EMC Test	Description	Range
IEC 61000-4-9	Radiated magnetic field susceptibility	50/60 Hz to 50 kHz
IEC 61000-4-10	Radiated magnetic field susceptibility	100 Hz and 1 MHz

The Nutherm "Qualification Report for CS Innovations Replacement MSFIS System," Revision 0, dated February 16, 2007 (Reference 72), states that "The MSFIS system contains only DC power and signal lines, therefore, susceptibility, test 61000-4-13 is not applicable and will not be performed," and also states "MIL-STD-461E Test CS-101 is equivalent to IEC 61000-4-13 and can be performed on DC equipment." Per Regulatory Guide 1.180 Section 4.1.3, Table 13, the IEC 61000-4-13 operating envelopes are specified for AC input power harmonics. The MSFIS equipment is powered from Class 1E DC power. Additionally,

Regulatory Guide 1.180 Section 4.1.3 states that CS-101, which was performed, corresponds to IEC 61000-4-13 and does apply to DC input power leads, not including grounds and neutrals. The NRC staff determined the inclusion of CS-101 is an acceptable substitution for IEC 61000-4-13 for the MSFIS.

The EMC testing review of WCGS MSFIS system will be discussed in the following subsections.

3.3.1.4.1 EMC Emissions Testing

The objective of EMC emissions testing is to reasonably ensure that the new equipment will not interfere with the function or operation of existing power plant equipment. Both conducted and radiated emissions testing were performed on the MSFIS system in accordance with MIL-STD-461E test methods. The four EMC emissions tests and the testing results of the MSFIS system are listed in the following table:

EMC Test	Description	Range	Result	Document
CE 101	Low-frequency conducted emissions	30 Hz to 10 kHz	Pass	Elite Report No. 37485-01 Appendix A
CE 102	High-frequency conducted emissions	10 kHz to 10 MHz	Pass	Elite Report No. 37485-01 Appendix B
RE 101	Radiated magnetic field emissions	30 Hz to 100 kHz	Pass	Elite Report No. 37485-01 Appendix D
RE 102	Radiated electric field emissions	10 kHz to 10 GHz	Pass	Elite Report No. 37485-01 Appendix E

These tests measured the conducted, magnetic field, or electric field radiated emissions from the enclosure and cables of the ALS test specimen over the specified frequency ranges. The NRC staff reviewed the test results and found that the test results did not meet the emissions requirements of IEEE TR-102323. The high-frequency conducted emissions (Test Method CE102 Run 9 in page B-8 of Elite Report No. 37485-01) showed higher emissions than the emissions limit curve of Figure 7-2 of IEEE TR-102323, Revision 2 (page 7-3) around 9 MHz during the test. However, all the four tests showed no radiated emissions exceeding the limits as specified in Regulatory Guide 1.180, Revision 1, Elite EMC emissions test requirements, and the EMC requirements in WCGS "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 16, 2009 (Reference 25), and, therefore, the NRC staff determined that reasonable assurance exists that the high-frequency conducted emissions from the MSFIS will not affect other equipment.

Based on the review, the NRC staff finds the ALS platform meets the requirements of Regulatory Guide 1.180 for conducted and radiated emission. This determination is not MSFIS-specific, and is suitable for reference when using the ALS platform for other safety-related uses in nuclear power plants. Any new design of boards intended for use in the ALS platform in safety-related applications would require equivalent conducted and radiated emission testing. Because the ALS platform meets the guidance in Regulatory Guide 1.180, the MSFIS is acceptable to operate at the WCGS control room regarding the EMC emissions.

3.3.1.4.2 EMC Susceptibility Testing

The objective of EMC susceptibility testing is to reasonably ensure that the equipment will function and operate as designed when installed in the industrial electromagnetic environment of a power plant.

Both conducted and radiated susceptibility testing was performed on the MSFIS in accordance with IEC 61000-4 test methods. In addition to IEC susceptibility tests, two MIL-STD-461E susceptibility tests, CS101 and RS101, were performed. The following table lists the EMC susceptibility tests (excluding surge withstand tests) and the testing results of the MSFIS system.

EMC Test	Description	Range	Result	Document
CS101	Low-frequency conducted susceptibility	30 kHz to 150 kHz	Pass	Elite Report No. 37485-01 Appendix C
RS101	Radiated magnetic field susceptibility	30 Hz to 100 kHz	Pass	Elite Report No. 37485-01 Appendix F
IEC 61000-4-3	Radiated electric field susceptibility	26 MHz to 10 GHz	Pass	Elite Report No. 37485-01 Appendix G
IEC 61000-4-6	Disturbances induced by radio-frequency fields conducted susceptibility	10 kHz to 200 MHz	Pass	Elite Report No. 37485-01 Appendix J
IEC 61000-4-8	Radiated magnetic field susceptibility	50 Hz and 60 Hz	Pass	Elite Report No. 37485-01 Appendix K
IEC 61000-4-9	Radiated magnetic field susceptibility	50/60 Hz to 50 kHz	Pass	WCGS ET-08-0035 (Reference 21)
IEC 61000-4-10	Radiated magnetic field susceptibility	100 Hz and 1 MHz	Pass	WCGS ET-08-0035 (Reference 21)

These tests determined whether the MSFIS test specimen continues to operate as designed under the specified test ranges. IEC 61000-4-3 test verifies the ability of equipment to withstand radiated electric fields over the frequency range from 26 megahertz (MHz) to 10 gigahertz (GHz). When this test was run, during the initial sweep from 26 MHz to 80 MHz, the alarm light-emitting diode (LED) on the MS rack illuminated, the full capability operation LED extinguished, and the reduced capability operation LED illuminated. Subsequently, the grounding strap for the unit was changed from a 12-gauge wire to a tinned copper braided strap, re-routed the J4 wires behind the table, and re-ran the test. The test showed no response to the radiated emissions after the modification.

The NRC staff reviewed the test results and noted that the frequency range applied for IEC 61000-4-9 tests do not cover the required test range as specified in Regulatory Guide 1.180, Revision 1 (50/60 Hz to 50 kilohertz (kHz)). However, Elite also performed RS101 test with frequency range from 10 Hz to 100 kHz. Because Elite RS101 test frequency range covers the required frequency range of IEC 61000-4-9 test, the NRC staff found the combination of Elite RS101 and IEC 61000-4-9 provides reasonable assurance that the ALS platform meets the EMC susceptibility requirements in Regulatory Guide 1.180, Revision 1.

The NRC staff reviewed Elite test report No. 37485-01 (Reference 72), and found that all Elite EMC susceptibility tests showed no response for the specified test conditions, and meet the EMC susceptibility requirements in Regulatory Guide 1.180, Revision 1, Elite EMC susceptibility test requirements, and the EMC requirements in WCGS "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 16, 2009 (Reference 25).

Based on the review, the NRC staff finds the MSFIS system meets the requirements of Regulatory Guide 1.180, and, therefore, is acceptable to operate at the WCGS control room regarding the EMC susceptibility. This determination is not MSFIS-specific, and is suitable for reference when using the ALS platform for other safety-related uses in nuclear power plants. Any new design of boards intended for use in the ALS platform in safety-related applications would require equivalent conducted and radiated susceptibility testing.

3.3.1.4.3 Surge Withstand Testing

The objective of surge withstand testing is to verify the ability of the equipment to withstand high-energy overvoltage conditions on power and interconnection lines. Surge withstand testing was performed on the MSFIS system in accordance with IEC 61000-4 test methods as listed in the following table.

EMC Test	Description	Range	Result	Document
IEC 61000-4-4	Electrical fast transient/burst immunity	2 kV	Pass	Elite Report No. 37485-01 Appendix H
IEC 61000-4-5	Surge immunity	2 kV	Pass	Elite Report No. 37485-01 Appendix I
IEC 61000-4-12	Ring wave immunity	2 kV	Pass	Elite Report No. 37485-01 Appendix L
IEC 61000-4-16	Common-mode conducted immunity	0 Hz to 150 kHz	Pass	Elite Report No. 37485-01

Initially, the test was performed at the medium exposure level of 4 kV, but the main power fuses consistently blew at 4 kV level. During the EMC Surge Withstand Testing, Elite identified the following anomalies:

- EMC Test No. IEC 61000-4-4: When Elite conducted the initial electrical fast transient/burst immunity test at the medium-exposure level of 4 kV for data collection, the "FAIL" LED on various boards and alarm indications illuminated.
- EMC Test No. IEC 61000-4-5: At the 4 kV medium-exposure level, the main power fuses consistently blew.

Afterward, the manufacturer made the modifications that were described in Appendix I, Paragraph 6 of Elite Report No. 37485-01 (Reference 72). Appendix III of the same test report, "Records of Anomaly," ROA-148 also addresses the details of those anomalies and modifications.

After the modification, Elite did a review of EMC testing and concluded that IEC 61000-4-4, IEC 61000-4-5, and IEC 61000-4-12 tests need to be re-performed. By using the 2 kV

(low-exposure level) instead of 4 kV (medium-exposure level) surge input, Elite verified that these anomalies were confined to alarm indications and no change of solenoid state occurred. These alarms were part of the system design. When the unit detects anomalous inputs, such as voltage surges, the system is designed to generate an alarm. Therefore, Elite considered these responses were acceptable. Elite also verified the operation of the unit by post-test operation, as described in its test report Elite Report No. 37485-01.

Having reviewed the Elite test report, the NRC staff accepts those test results and concludes that the tested MSFIS system with the modification complies with the surge withstand requirements of Regulatory Guide 1.180, Revision 1. This determination is not MSFIS-specific, and is suitable for reference when using the ALS platform for other safety-related uses in nuclear power plants. Any new design of boards intended for use in the ALS platform in safety-related applications would require equivalent surge withstand testing. Because the ALS platform meet the guidance in Regulatory Guide 1.180, the MSFIS is acceptable to operate at the WCGS control room regarding surge withstand testing.

3.3.1.4.4 Electrostatic Discharge (ESD) Withstand Testing

The objective of ESD withstand testing is to verify the ability of the equipment to withstand electrostatic discharge. EPRI TR-102323 specifies IEC 61000-4-2 "ESD Withstand Testing" as an optional test, because electrostatic discharge is not considered a common-mode failure mechanism for safety-related system.

CS Innovations has designed ALS boards and racks to meet IEC 61000-4-2 (ESD Immunity Test) Level 3 (8 kV air discharge/4 kV contact discharge) requirement. CS Innovations ran the ESD test using IEC 61000-4-2 method with 15 kV air discharge and 4 kV contact discharge on the ALS handles, rails, switches, lamps, and connectors. The test results are documented in CS Innovations 6002-00207, "CSI ESD Test Report," Revision 0, dated January 15, 2009 (Reference 74).

Having reviewed the new test results, the NRC staff found the 4 kV contact discharge is lower than the requirement 8 kV specified in the EPRI TR-102323, and MSFIS system does not meet the guidance of TR-102323. However, these tests are optional and the MSFIS system exceeded the IEC 61000-4-2 Level 3 by using a 15 kV air discharge instead of the required 8 kV. The NRC staff reviewed these tests, and determined that the test results provide reasonable assurance that the ALS platform meets the ESD withstand testing requirements of EPRI TR-102323 and is, therefore, acceptable. This determination is not MSFIS-specific, and is suitable for reference when using the ALS platform for other safety-related uses in nuclear power plants. Any new design of boards intended for use in the ALS platform in safety-related applications would require equivalent ESD withstand testing.

Because IEC 61000-4-2 "ESD Withstand Testing" is an optional test per EPRI TR-102323, and the EDS testing performed meets the CS Innovations ALS design specification, the NRC staff found that MSFIS system is acceptable to operate at the WCGS control room.

3.3.1.4.5 Class 1E to Non-1E Isolation Testing

Clause 7.2.2.1 of IEEE 384 (Reference 102) provides the guidance for Class 1E to Non-1E isolation, that includes the use of isolation devices so that (a) the maximum credible voltage or current transient applied to the device's non-Class 1E side will not degrade the operation of the circuit connected to the device Class 1E or associated side below an acceptable level; and (b) shorts, grounds, or open circuits occurring in the non-Class 1E side will not degrade the circuit connected to the device Class 1E or associated side below an acceptable level.

The ALS platform design incorporates advanced failure detection and isolation techniques. All I/O boards incorporate dedicated I/O channels that typically include opto-coupler, transient voltage suppressors, and metal oxide varistors devices for isolation and protection.

Both input and output channels are divided into groups - typically one to four groups. Each group uses a common ground and has isolation from the other groups, as well as the digital portions of the board. The CS Innovations stated that the isolation is able to withstand 1500 VAC. The input channels on the ALS boards are based on isolated solid-state devices, where opto-isolators provide isolation. The output channels are protected against ESD and surge voltages using metal oxide varistors.

The licensee stated that the ALS platform-based MSFIS will be installed in the existing Group 1 and Group 4 cabinets, maintaining the current safety group separations. New switches installed on the operator control panel to control both divisions include physical barriers that meet the requirements of IEEE Standard 384-1992. Because no interface design changes between the existing MSFIS system and other systems, the physical separation, electrical isolation, physical barriers, and the effect of single random failure in other systems remain the same.

The NRC staff reviewed CS Innovations documents, Reference 32, Reference 33, and Reference 30, and determined that the MSFIS system design has adequate electrical isolation between Class 1E and Non-1E equipment, which is consistent with the guidelines as specified in Section 7.2.2 of IEEE 384. Therefore, the NRC staff found that the MSFIS system is suitable for safety-related use in the WCGS control room. This determination is, however, MSFIS-specific and, therefore, is not suitable for reference when using the ALS platform for other safety-related uses in nuclear power plants.

The licensee had incorporated the modifications made in EMC IEC 61000-4-3 test into manufacturer installation instructions, and the modifications made in EMC IEC 61000-4-5 test into manufacturer design documents for all future board and panel revisions. The licensee had reviewed and found all anomalies noted during testing to be acceptable, and the modified MSFIS system performed satisfactory.

The NRC staff reviewed these documents, and determined that the EMC tests demonstrated that the replacement MSFIS system, when properly installed, meet the EMC requirements of Regulatory Guide 1.180, Revision 1, for safety-related devices located in a low EMI exposure environment, as defined by RG 1.180. Therefore, the NRC staff concludes that MSFIS system is acceptable to operate at the WCGS control room.

3.3.1.5 Seismic Withstand Testing

Clause 4 of IEEE Standard 344-1987 states that the seismic qualification of Class 1E equipment should demonstrate an equipment's ability to perform its safety function during and after the time it is subjected to the forces resulting from one Safe Shutdown Earthquake (SSE). In addition, the equipment must withstand the effects of a number of Operating Basis Earthquakes (OBEs) prior to the application of an SSE.

To demonstrate that the MSFIS system will function under seismic motion conditions, the test system was subjected to a series of seismic simulation tests using a tri-axial seismic simulator shake table. These tests included resonance search tests and RMF tests in accordance with Nutherm Seismic Test Procedure S-128P, Revision 2, and IEEE 344-1975.

The acceptance criteria for the seismic tests are that there is no loss of safety function under OBE/SSE testing. Loss of function included (a) loss of output, such as open or short circuit, and (b) structural failure, such as broken or loosened parts. Also, output discontinuities or contact chatter greater than two milliseconds shall be recorded and results included in the report.

Prior to the seismic test, MSFIS system components were mounted to test fixtures to simulate the actual in-service configurations. Then the test fixtures were mounted to a tri-axial seismic simulator table such that the principal axes of the specimens were collinear with the input excitations of the test table. Control accelerometers were also mounted to the test table, the rack assembly, and the fuse block panel, and digital data acquisition system was used to record the output of those accelerometers.

3.3.1.5.1 Pre-seismic Inspection and Operability Check

The test specimens were examined upon their arrival at the test facility to verify that no damage had occurred during shipping and handling; and "ON-OFF" type operability checks were conducted before testing. The specimens passed the pre-seismic inspection and operational check.

3.3.1.5.2 Resonance Search Test

The MSFIS components were subjected to a resonance search test and conducted a low-level (0.2 g horizontally and vertically) single-axis sine sweep in each of the three orthogonal axes. Wyle performed sine sweeps from 1 Hz to 100 Hz at a sweep rate of one octave per minute. The test response spectra (TRS) of those tests in each of the three orthogonal axes demonstrated no resonance conditions below 33 Hz.

Clause 3.1 of IEEE 344-1987 described that the earthquake ground motion is typically broadband random, and produces potentially damaging effects over a frequency range of 1 Hz to 33 Hz. Having reviewed the test results, the NRC staff concludes that the results of those sine-sweep tests are acceptable.

3.3.1.5.3 Qualification-level Multiple-Frequency Tests

After the single-axis resonance search test, a tri-axial RMF seismic simulation tests was performed. The test specimen was subjected to 30-second duration tri-axial multiple-frequency random motion, that was amplitude-controlled in one-third of octave bandwidths, spaced one-third of an octave apart over the 1 Hz to 100 Hz frequency range. Three simultaneous, but independent, random signals were used as the excitation to produce phase-incoherent motions in the vertical and the two horizontal axes. The amplitude of each one-third of an octave bandwidth in each of the three axes was independently adjusted until the TRS enveloped the required response spectra (RRS) within the test table limits. The qualifying SSE RMF test is based on RRS as specified in Specification No. 10466-J-820 Revision 1, Figure 3 in Attachment D of WCGS "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 16, 2009 (Reference 25), as modified by WCGS. Figures 2 and 3 on pages 8 and 9 of Nutherm S-128P, "Seismic Test Procedure," Revision 2 (Reference 72), show the SSE horizontal and SSE vertical RRSs at 3 percent damping with 10 percent margin. The values of acceleration g's plus 10 percent margin range from 1.24 to 7.42 for the SSE horizontal RRS and from 0.26 to 0.89 for the SSE vertical RRS at 3 percent damping (Table 2 and Table 3 of Nutherm S-128P, Revision 2, pages 14 and 15). Figures 4 and 5 on pages 10 and 11 of Nutherm S-128P, Revision 2, show the OBE horizontal and OBE vertical RRS at 3 percent damping with 10 percent margin. The OBE test levels are two thirds of the SSE test levels.

By using a response spectrum analyzer, the resulting table motion at the test damping for the OBE and SSE tests were analyzed and plotted at one-sixth of octave intervals over the frequency range of 1 Hz to 100 Hz. These test levels include a 10 percent margin. OBE test levels are 2/3 of SSE RRS plus a 10 percent margin. The representative OBE and SSE tests used the damping values of 0.5 percent, 1 percent, 2 percent, 3 percent, and 5 percent.

The specimen was subjected to five OBE tests before it was applied the SSE test. The following list describes the seismic test runs for the test specimen of MSFIS system:

Test Run	Test Type	
1	sine sweep	Vertical
2	sine sweep	side/side
3	sine sweep	front/back
4	RMF	OBE-1
5	RMF	OBE-2
6	RMF	OBE-3
7	RMF	OBE-4
8	RMF	OBE-5
9	RMF	SSE-1
10	RMF	SSE-2

Approximately 15 seconds into the SSE test, the technician simultaneously pressed two of the four pushbuttons on the operator test panel to simulate an ESFAS signal. This action energized the appropriate load bank indicator lights. Wyle observed no structural damage or discontinuity of output in any of the identified tests.

3.3.1.5.4 Post-seismic Baseline Test and Operability Check

The test specimen was operated and visually examined at the conclusion of the seismic test and observed no structural anomalies. After completing the seismic testing, a baseline test was conducted on the test specimen. The test specimen passed the post-seismic baseline test. After the baseline test, the test specimen was inspected again, which did not find any anomalies. Finally, verification testing was conducted on all applicable boards, for information only, to compare them to the original manufacturer files. No changes in the FPGA files were noted.

Appendix V, "Seismic Test Data" of Nutherm Qualification Report, WCN-9175R, displayed the TRS plots and the TRS plots (with RRS comparison) of the seismic testing for representative OBE test runs and SSE test runs. The NRC staff reviewed those plots and found all the OBE and SSE TRS plots with RRS comparison enveloped the RRS over the test range of 1 Hz to 100 Hz.

On the basis of this review, the NRC staff found that the tested MSFIS system equipment, when properly installed and maintained, will meet the guidelines in Clause 10.2, "Specification Requirements" and Clause 10.3, "Seismic Qualification Report" of IEEE Standard 344-1987, and seismic qualification requirements in WCGS "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 16, 2009 (Reference 25). Based on the review, the NRC staff finds the MSFIS system is acceptable to operate at the WCGS control room with the mild environmental qualification. The test data is not MSFIS-specific, and is suitable for reference when using the ALS platform for other safety-related uses in nuclear power plants; however, the design basis earthquake and therefore the required seismic requirements are plant-specific, and it must be determined that the ALS platform qualifications exceed the specific plant's seismic requirements. In addition, any new design of boards intended for use in the ALS platform in safety-related applications would require seismic testing within an ALS platform-based system. Finally, for new uses with differing application-specific backplanes and differing functions that must continue to operate during the SSE, either seismic testing of the new ALS platform-based system or an appropriate qualification by similarity analysis should be provided.

3.3.2 Response Time

The accident analysis of design basis events at nuclear power plants includes a determination of how soon the protective actions are needed to mitigate those design basis events. The basis for this is contained in 10 CFR 50.55a, "Codes and Standards," of 10 CFR, "Domestic Licensing of Production and Utilization Facilities." This states that "protective systems must meet the requirements set forth in editions or revisions of the Institute of Electrical and Electronics Engineering Standard: 'Criteria for Protective Systems for Nuclear Power Generating Stations,' (IEEE-279)..." In addition, 10 CFR 50.36(c)(1)(ii)(A) requires inclusion in the TSs the limiting safety systems settings for nuclear reactors, those settings "so chosen that automatic protective action will correct the abnormal situation before a safety limit is exceeded." Once the total time required for a protective action has been determined, licensees allocate portions of that time to portions of the protective system (i.e., the time required for the sensors response to changes in

plant conditions, time required for the actuation logic, and the time required for a valve to close or a pump to start).

For MSFIS, WCGS "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 16, 2009 (Reference 25), requires, in Section 5.2.3, that "the overall response time of the Replacement MSFIS System specified herein shall be less than or equal to 100 milliseconds for an input signal step change." References 27 and 28 discuss MSFIS response time in Section 5.6. This section states that the worst case response time for the system will be 86 milliseconds. CS Innovations 6101-00004, "MSFIS System Test Plan," Revision 0.8, dated June 9, 2007, test requirement R-MSFIS.139 specified the test to measure the actual response time. The actual response of the system was tested by Nutherm test TPS-9064 and documented in Nutherm 9715-TR-01R, "Test, Inspection, and Quality Assurance Activities Report," Revision 0, dated February 29, 2008 (Reference 73), Appendix IV. The documentation shows that the test was run 13 times with an average measured response time of 89.75 milliseconds, and a maximum measured response time of 96.80 milliseconds.

Based on the specification, analysis, testing, and the test results for MSFIS response time performance, the NRC staff has determined that the MSFIS meets the WCGS response time requirements. Because the response time requirements, and the actual response time are MSFIS-specific, this determination is not suitable for reference in future uses of the ALS platform in safety-related applications at nuclear power plants.

3.3.3 Diversity and Defense-in-Depth

10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. Clause 5.1 of IEEE Standard 603-1991 requires in part that "safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures." In addition, 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram [ATWS]," requires in part various diverse methods of responding to ATWS; 10 CFR Part 50, Appendix A, General Design Criterion (GDC) 21, "Protection Systems Reliability and Testability," requires in part that "no single failure results in the loss of the protection system"; GDC 22, "Protection System Independence," requires in part "that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions ... not result in loss of the protection function ... Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function"; GDC 24, "Separation of Protection and Control Systems," requires in part that "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired"; and GDC 29, "Protection Against Anticipated Operational Occurrences," requires in part defense against anticipated operational transients "to assure an extremely high probability of accomplishing ... safety functions."

Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Safety Systems" (Reference 124), clarifies the application of the single-failure criterion (GDC 21) and endorses IEEE Standard 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems" (Reference 101). Clause 5.5 of IEEE Standard 379-2000 identifies diversity and D3 as a technique for addressing common-cause failure, and Clause 6.1 identifies logic failures as a type of failure to be considered when applying the single-failure criterion.

The Staff Requirements Memorandum on SECY 93-087, dated July 21, 1993 (Reference 88) describes the NRC position on D3 requirements to compensate for possible common cause programming failure. This requires that the applicant assess the defense-in-depth and diversity of the proposed instrumentation and control system, and if a postulated common-cause failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function.

Guidance on the evaluation of D3 is provided in SRP BTP 7-19. In addition, NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," dated December 31, 1994 (Reference 90), summarizes several D3 analyses performed after 1990 and presents a method for performing such analyses.

Additional guidance on evaluation of the need for D3, and acceptable methods for implementing the required D3 in digital I&C system designs is contained in "Interim Staff Guidance, Digital Instrumentation and Controls, DI&C-ISG-02 Task Working Group #2: Diversity and Defense-in-Depth Issues," September 26, 2007 (Reference 139).

CS Innovations 6002-00031, "ALS Diversity Analysis," Revision 0, dated January 13, 2009 (Reference 75), discusses the designed-in diversity of the ALS boards. The WCGS review of this diversity methodology is contained in WCGS "MSFIS D3 Assessment," Revision 2, dated January 9, 2009 (Reference 76).

Reference 75 states that each FPGA on each board associated with the safety signal path contains two sets of diverse hardware logic, each called a "core." This was performed by changing the logic implementation strategy used during synthesis process. The design process used to develop the FPGAs is described in Section 3.1.1.4.1.4.3 of this SE. After the HDL is developed by expanding the specification into formal language, the synthesis of that HDL is performed using one type of hierarchical structure, FSM encoding, and state decoding for one logic core, and a second type of hierarchical structure, FSM encoding, and state decoding for the other logic core. The two diverse core designs are tested on two diverse test benches, to determine that each core will adequately perform the required safety function. The two diverse cores then undergo the place and route process and are tested again to determine the proper operation of the safety application. The details on how the diversity between the two cores was achieved are in the proprietary ALS Diversity Analysis (Reference 75). The staff reviewed these design details, and the resulting internal diversity, and this review is discussed below.

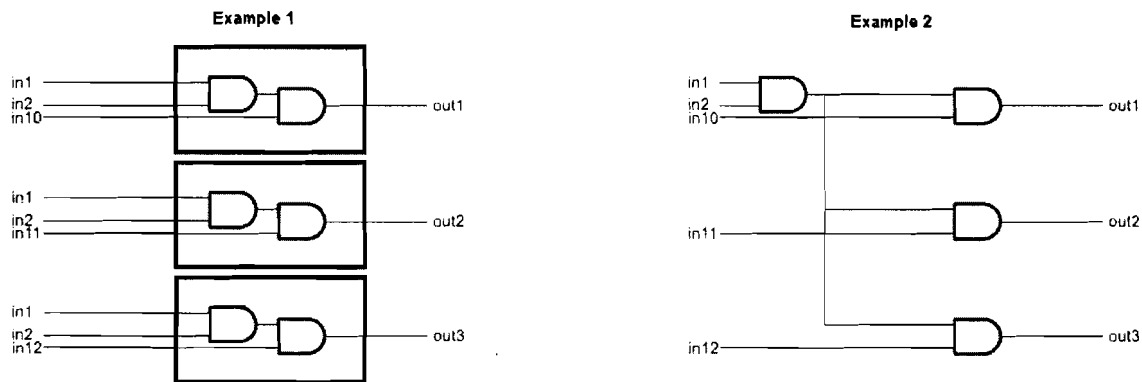


Figure 9 - Example of Diverse Logic Implementation

A very simple example of how two different logic methods can provide the same function is provided in Figure 9. As can be seen by this figure, in both examples 1 and 2, “int 1” and “int 2” are combined, and the resulting value is then combined with three other signals.

The diversity of the two cores is verified by using the synthesis tool to produce the netlist, a proposed schematic of the hardware circuit, for each core. The two schematics are compared by the V&V team to verify that the implementation of the function is different and diverse. In addition, each core is compared in the number and type of gates used for the core implementation.

As discussed in Section 3.0 of this SE, FPGA logic implementation is fundamentally different from that used by μ P-based systems. Because the complete sequence of gates used to perform a safety function is different, there is no programmed hardware that could cause a failure common to both cores. Unlike μ P-based systems, the actual logic schematics can be examined and signal flows can be traced through the schematics. The NRC staff did this on a sampling basis during the thread audit on May 12-15, 2008, at CS Innovations. FPGAs also do not use an operating system. The diversity of the two cores was reviewed by the NRC staff during the site visit to CS Innovations on December 10-11, 2008. The review included comparisons of the schematic diagrams showing the diverse implementation of selected functions in each of the cores.

For a μ P-based system to provide an equivalent level of diversity, the system would require two diverse μ Ps and two diverse operating systems, as well as diverse operational software performing the safety function. This type of diversity was proposed by B&W Nuclear Technologies in Topical Report BAW-10191, “STAR Systems Components for Reactor Protection System Digital Upgrades,” dated September 1994 (Reference 77), and approved by SE dated August 3, 1995 (Reference 78).

DI&C-ISG-02, Revision 1 (Reference 139), from NRC Task Working Group #2, “Diversity and Defense-in-Depth Issues,” issue 5, “Common Cause Failure Applicability,” contains NRC staff position 1. This NRC staff position states that if sufficient diversity exists in the protection system such that common cause failures within the channels can be considered to be fully addressed without further action, no additional diversity would be necessary in the safety system.

The NRC staff audited this diversity during a visit to CS Innovations on December 10-11, 2008. The details on the methodology used to design and verify the diversity are proprietary to CS Innovations, and will not be discussed in this SE. This information can be found in Reference 75. The NRC staff also took into consideration the low level of complexity of the MSFIS. The MSFIS is not a full trip or actuation system, but receives the trip signal from the SSPS, and upon receipt of that signal, provides opening signals to the individual valves. In addition, the MSFIS receives valve control signals from the operator control panel, and provides open or close signals to the individual valves. The received signals are binary (on/off) and not complex digital data. The staff determined that there is sufficient diversity within the programmable portion of the ALS platform such that common cause failures of that programming is adequately addressed and, therefore, the MSFIS design meets the intent of NRC staff position 1. This determination was based, in part, on the low level of complexity, and the resultant ability of the V&V group to compare the actual schematic diagrams of the two diverse cores to determine that the circuitry was actually diverse. The NRC staff notes that while the remaining analog portions of each board do not have diversity, because these portions are not subject to common cause software or programming error, diversity is not required for the analog portions of each board. The intent of requiring D3 as protection against common cause software failure or programming error is to ensure that the technology change from analog to digital does not introduce the new vulnerability into the protection systems. There has always been the possibility of a design deficiencies or manufacturing error in analog circuits, but these are specifically exempted by IEEE Standard 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," Clause 5.5, "Common-cause failures," from consideration when conducting the single-failure analysis. The NRC staff has determined that due to the MSFIS use of two diverse cores in each FPGA and the ability to examine the resultant circuitry to determine the actual diversity, there is reasonable assurance that the programmable nature of FPGAs as used in the MSFIS does not add any additional vulnerability over that found in non-programmable systems. The NRC staff therefore determined that for the MSFIS, the system meets the guidance provided in DC&I-ISG-02, and the MSFIS is acceptable for use in this safety-related application at WCGS. This determination is specific to the MSFIS design. Future and more complex uses of the ALS platform, such as for a system receiving sensor signals and making trip or actuation determinations, may require additional design diversity. An example of this additional design diversity may be to provide the independent development of diverse HDL code for each core. Any future determination of adequate diversity based on meeting DI&C-ISG-02, issue 5, staff position 1 will be based upon the application-specific use of the ALS platform.

3.3.4 Cyber Security

Guidance for cyber security measures of nuclear power plant safety systems is provided within Regulatory Guide 1.152. This states that security vulnerabilities should be addressed in each phase of the digital safety system life cycle. The interim NRC staff guidance within "Interim Staff Guidance, Digital Instrumentation and Controls, DI&C-ISG-01 Task Working Group #1: Cyber Security," December 31, 2007 (Reference 138), clarifies this guidance. The overall guidance provides that the basis for physical and logical access controls be established through the development process to consider the consequence to the nuclear power plant in combination with the susceptibility of a digital system to internal and external cyber-attack.

As discussed in Section 3.2.2.2 of this SE, the MSFIS application is not software driven while in operation. However, Reference 49 requires a line-by-line review of the HDL listings as part of the design and V&V activities described in Sections 3.1.1.4.1.4.3 and 3.1.1.4.1.5.1 of this SE, respectively. Also, as discussed in Section 3.2.2.4 of this SE, the NRC staff audited HDL listing to ensure the device programming was traceable to requirements. The FPGA design review and NRC staff audit are sufficient to determine the HDL listings are devoid of unwanted or malicious programming.

The MSFIS application of the ALS platform contains provisions to address cyber security. As described in Section 3.1.1.5.2 of this SE, a MSFIS rack contains a single connection, a USB 2.0 port, for use with an external computer, the ASU. There are no connections, permanent or temporary, to other installed plant equipment. The ASU is a dedicated PC used only for the test and troubleshooting of the ALS platform, is not used for any other purpose, and is not connected to other non-safety equipment at any time. As such, the MSFIS application of the ALS platform is not susceptible to external cyber-attack. Also, MSFIS application of the ALS platform provides security measures to address an internal cyber-attack. Internal cyber-attack security measures restrict access to and use of the USB port as follows: 1) the MSFIS rack communicates over this port using a proprietary protocol, 2) an active connection to this port is alarmed at the operator control panel, 3) the licensee has agreed to provide administrative controls that restrict connection of the ASU to this port, as described in Section 1.2.2 of Reference 50, 4) communications over this port, as limited by the safety-related MSFIS rack FPGA firmware, cannot modify the operational behavior of an installed MSFIS rack or otherwise impact the safety-signal path, and 5) the licensee has agreed to provide administrative controls that prohibit the plant from on-site possession of the special tooling needed to modify the operational behavior of an installed MSFIS rack, as described in the licensee's May 9, 2007, "Response to Request for Additional Information Relating to Replacement of the Main Steam and Feedwater Isolation System Controls" (Reference 3). The nature of FPGA-based equipment as implemented within the MSFIS does not allow reprogramming of the FPGA or NVM; therefore, no modification of the safety function without special tooling is possible. Furthermore, the safety-related MSFIS rack FPGA firmware verifies a valid configuration exists for the complete MSFIS rack, and if the configuration is invalid the MSFIS rack generates its alarm for indication at the operator control panel.

The NRC staff has reviewed the cyber security provisions of the MSFIS application of the ALS platform using the guidance provided by DI&C-ISG-01 (Reference 138) and Regulatory Guide 1.152, and determined that cyber security considerations have been satisfactorily addressed within the development. If future applications of the ALS platform maintain the same communication limitations, and future licensees also do not have the special tooling to allow local modifications of the FPGAs or NVMs, this determination can be used in future cyber security evaluations; however, if the communications is expanded in future uses of the ALS platform, or if licensees have the ability to modify the FPGA or NVM programming, this issue will need to be revisited.

3.3.5 Review of System and IEEE 603 Requirement

3.3.5.1 IEEE 603-1991 Clause 4 - Safety System Designation

Clause 4 of IEEE 603-1991 states that a specific basis shall be established for the design of each safety system of the nuclear power generating station. The sub clauses of this requirement include the following:

- Clause 4.1 - Identification of the Design Basis Events
- Clause 4.2 - Safety Functions and Corresponding Protective Actions
- Clause 4.3 - Permissive Conditions for Each Operating Bypass Capability
- Clause 4.4 - Identification of Variables Monitored
- Clause 4.5 - Minimum Criteria for Manual Initiation And Control Of Protective Actions
- Clause 4.6 - Identification of the Minimum Number And Location Of Sensors
- Clause 4.7 - Range Of Transient and Steady-State Conditions
- Clause 4.8 - Identification of Conditions Which May Degrade Performance
- Clause 4.9 - The Methods to Be Used To Determine Reliability
- Clause 4.10 - The Critical Points in Time After The Onset Of A Design Basis Event
- Clause 4.11 - The Equipment Protective Provisions
- Clause 4.12 - Any Other Special Design Basis

SRP Chapter 7, Appendix 7.1-C, Section 4, "Safety System Designation" provides acceptance criteria for these requirements.

The FPGA-based MSFIS controls system under discussion in this SE is a replacement for the existing system. The staff determined that the bases for the design of the MSFIS as described in Clauses 4.1 through 4.12 were not changed by use of a FPGA based MSFIS, and are the same as the existing system. In addition, no technical specification changes were needed to install the FPGA-based MSFIS, no modifications of the USAR were needed, and no new accident analysis was needed. For these reasons, the staff determined that no review is needed for Clause 4 of IEEE 603-1991.

3.3.5.2 IEEE 603-1991 Clause 5 - Safety System Criteria

3.3.5.2.1 IEEE 603-1991 Clause 5.1 - Single-Failure Criterion

Clause 5.1 of IEEE 603-1991 states that the safety systems meet the single failure criterion as defined by IEEE Standard 379-1988. SRP Chapter 7, Appendix 7.1-C, Section 5.1, "Single-Failure Criterion," provides acceptance criteria for the single-failure criterion. This section states that the applicant/licensee's analysis should confirm that the requirements of the single-failure criterion are satisfied.

WCGS submitted the MSFIS "System Reliability Analysis for Advanced Logic System, Revision 1, dated April 10, 2007 (Reference 79). This analysis includes a failure modes and effects analysis. The NRC staff has reviewed this FMEA, and agrees with the licensee determination that the FMEA provides reasonable assurance that the single-failure criterion is met for all creditable single failures and all failures caused by the single failure.

3.3.5.2.2 IEEE 603-1991 Clause 5.2 - Completion of Protective Action

Clause 5.2 of IEEE 603-1991 states that 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, and that deliberate operator action shall be required to return the safety systems to normal. SRP Chapter 7, Appendix 7.1-C, Section 5.2, "Completion of Protective Action," provides acceptance criteria for this requirement.

The MSFIS does not initiate the isolation function, but receives the isolation signal from the SSPS. MSFIS then performs the valve control function to close the required valves. During the May 12-15, 2008, Thread Audit at CS Innovations, the NRC staff specifically examined the valve close and open functions, and reviewed the logic responsible for these functions. The NRC staff determined that once the isolation signal is received from the SSPS or a manual close or open signal is received from the operator, the protective action is sealed-in, and will continue until completed. The NRC staff also determined that deliberate operator action was required to reset the MSFIS to automatic functionality. The NRC staff therefore concluded that the MSFIS meets this IEEE 603 requirement for completion of protective action.

3.3.5.2.3 IEEE 603-1991 Clause 5.3 – Quality

Clause 5.3 of IEEE 603-1991 states that the components and modules within the safety system be of a quality that is consistent with minimum maintenance requirements and low failure rates, and that safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. SRP Chapter 7, Appendix 7.1-C, Section 5.3, "Quality," provides acceptance criteria for the quality requirement. This acceptance criteria states that the quality assurance provisions of 10 CFR Part 50, Appendix B, apply to a safety system.

WCGS conducted a 10 CFR Part 50, Appendix B, audit of CS Innovations on September 10-13, 2007. The scope of the audit was "to evaluate the effectiveness and proper implementation of an acceptable QA Program for the supply of ALS Control Systems, including Engineering Design Analysis & Production of an FPGA Control and Signal Processing Application in support of nuclear safety-related work as it applies to 10 CFR Part 50, Appendix B, and 10 CFR Part 21 for the nuclear industry." The report on that audit was issued on November 21, 2007, and stated that CS Innovations is a WCGS qualified supplier for the audited scope. This determination meets the guidance acceptance criteria in SRP Chapter 7, Appendix 7.1-C, Section 5.3, "Quality."

3.3.5.2.4 IEEE 603-1991 Clause 5.4 - Equipment Qualification

Clause 5.4 of IEEE 603-1991 states that safety system equipment be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting the performance requirements as specified in the design basis. SRP Chapter 7, Appendix 7.1-C, Section 5.4, "Equipment Qualification" provides acceptance criteria for IEEE 603 Clause 5.4. This acceptance criteria states that the applicant/licensee should confirm that the safety system equipment is designed to meet the functional performance requirements over the range of normal environmental conditions for the area in which it is located. This clause of IEEE 603-1991 also states that qualification of

Class 1E equipment be in accordance with the requirements of IEEE Standard 323, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations" and IEEE Standard 627-1980, "IEEE Standard for Design Qualification of Safety Systems Equipment Used in Nuclear Power Generating Stations" (Reference 109). Regulatory Guide 1.89, Revision 1, endorses and provides guidance for compliance with IEEE Standard 323-1974.

A description of the equipment qualification is contained in Section 3.3.1 of this SE. The NRC staff has reviewed the equipment qualification, and has determined that the ALS platform environmental qualifications demonstrate that the MSFIS can meet its functional performance requirements over the range of normal and worst case accident environmental conditions for the WCGS control room, the area in which the MSFIS is located.

3.3.5.2.5 IEEE 603-1991 Clause 5.5 - System Integrity

Clause 5.5 of IEEE 603-1991 states that the safety systems be designed such that the system can accomplish its safety functions under the full range of applicable conditions enumerated in the design basis. SRP Chapter 7, Appendix 7.1-C, Section 5.5, "System Integrity," provides acceptance criteria for system integrity. This acceptance criteria states that the NRC staff should confirm that tests have been conducted on safety system equipment components and the system racks and panels as a whole to demonstrate that the safety system performance is adequate to ensure completion of protective actions over the range of transient and steady-state conditions of both the energy supply and the environment; that test shows that if the system does fail, it fails in a safe state, and that failures detected by self-diagnostics should also place a protective function into a safe state.

The CS Innovations equipment qualifications testing, discussed in Section 3.3 of this SE, provides reasonable assurance that the MSFIS system is capable of performing its safety function over the full range of environmental conditions that may exist during the worst case design basis event at WCGS during which the safety function is required and, therefore, satisfied this portion of the acceptance criteria.

The NRC staff review of the FMEA as discussed in Sections 3.2.1.9, 3.2.1.9.1, and 3.3.5.2.1 of this SE provides reasonable assurance that an input signal or system failure, including power supply or input power failure, will cause the MSFIS system to fail in the predefined safe state and annunciate that failure to the operators. It should be noted that the input sensors that feed the automatic isolation determination and the isolation determination itself are not part of the MSFIS, but are part of the SSPS. The MSFIS does not have any directly connected sensors, but does receive the isolations signals from the SSPS. Further, NRC staff review of the self diagnostic features and tests performed by the ALS platform will, for failures detected by self-diagnostics, place a MSFIS into a safe state and annunciate that failure to the operators. WCGS has defined the fail-safe output in WCGS "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 16, 2009 (Reference 25), Section 5.2.5, as maintaining the current output state when a failure is identified, and also has a requirement, in Section 5.6.7, to annunciate the failure to the operators. The NRC staff has therefore determined that there is reasonable assurance that the MSFIS system satisfied this portion of the acceptance criteria.

3.3.5.2.6 IEEE 603-1991 Clause 5.6 – Independence

Clause 5.6 of IEEE 603-1991 requires in part independence between 1) redundant portions of a safety system, 2) safety systems and the effects of design basis events, and 3) safety systems and other systems. SRP Chapter 7, Appendix 7.1-C, Section 5.6, "Independence" provides acceptance criteria for system integrity. This acceptance criteria states that three aspects of independence: 1) physical independence, 2) electrical independence, and 3) communications independence, should be addressed for each previously listed cases. Guidance for evaluation of physical and electrical independence is provided in Regulatory Guide 1.75, Revision 3, "Criteria for Independence of Electrical Safety Systems" (Reference 126), which endorses IEEE Standard 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits." The safety system design should not have components that are common to redundant portions of the safety system, such as common switches for actuation, reset, mode, or test; common sensing lines; or any other features that could compromise the independence of redundant portions of the safety system. Physical independence is attained by physical separation and physical barriers. Electrical independence should include the utilization of separate power sources. Transmission of signals between independent channels should be through isolation devices.

SRP Chapter 7, Appendix 7.1-C, Section 5.6, "Independence" provides additional acceptance criteria for communications independence. Section 5.6 states that where data communication exists between different portions of a safety system, the analysis should confirm that a logical or software malfunction in one portion cannot affect the safety functions of the redundant portions, and that if a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, a logical or software malfunction of the non-safety system must not be able to affect the functions of the safety system. Section 3.1.1.6 of this SE addresses additional evaluation of independence related to DI&C-ISG-04.

3.3.5.2.6.1 IEEE 603-1991 Clause 5.6.1 - Independence between Redundant Portions of a Safety System

Clause 5.6.1 of IEEE 603-1991 states that the safety systems be designed such that there is sufficient independence between redundant portions of a safety system such that the redundant portions are independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function. SRP Chapter 7, Appendix 7.1-C does not provide any additional acceptance criteria beyond that in Clause 5.6.1.

The NRC staff reviewed the independence between redundant portions of the MSFIS, and documented that review in Section 3.1.1.5.3 of this SE. Based on this review, the NRC staff determined that there is sufficient independence between redundant portions of the MSFIS such that the redundant portions are independent of and physically separated and, therefore, the MSFIS meets the requirements of Clause 5.6.1 of IEEE 603.

3.3.5.2.6.2 IEEE 603-1991 Clause 5.6.2 - Independence between Safety Systems and Effects of Design Basis Event

Clause 5.6.2 of IEEE 603-1991 states that the safety systems required to mitigate the consequences of a specific design basis event be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability to meet the requirements of this standard. Clause 5.6.2 further states that equipment qualification in accordance with 5.4 is one method that can be used to meet this requirement. SRP Chapter 7, Appendix 7.1-C does not provide any additional acceptance criteria beyond that in Clause 5.6.2.

The NRC staff reviewed the equipment qualifications of the MSFIS, and documented that review in Sections 3.2.1.10 and 3.3.1 of this SE. Based on this review, the NRC staff determined that the qualification of the system demonstrates that there is sufficient independence between the MSFIS and effects of design basis event for the MSFIS to be capable of mitigating the consequences of design basis events, and is sufficiently physically separated from the effects of the design basis events. Therefore, the MSFIS meets the requirements of Clause 5.6.2 of IEEE 603.

3.3.5.2.6.3 IEEE 603-1991 Clause 5.6.3 - Independence between Safety Systems and Other Systems

Clause 5.6.3 of IEEE 603-1991 states that the safety systems be designed such that credible failures in and consequential actions by other systems will not prevent the safety systems from meeting the requirements of this standard. This requirement is subdivided into requirements for interconnected equipment, equipment in proximity, and the effects of a single random failure. SRP Chapter 7, Appendix 7.1-C does not provide any additional acceptance criteria beyond that in Clause 5.6.3. Each of the subclauses will be addressed in the following paragraphs.

Clause 5.6.3.1 of IEEE 603, "Interconnected Equipment" states that equipment that is used for both safety and non-safety functions, as well as the isolation devices used to affect a safety system boundary, be classified as part of the safety systems. This clause further states that 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, and that a failure in an isolation device will be evaluated in the same manner as a failure of other equipment in a safety system.

The NRC staff reviewed the independence between MSFIS and other systems, and documented that review in Section 3.1.1.5.2 of this SE. Based on this review, the NRC staff determined that the only communications between MSFIS and non-safety systems is ASU. The ASU is not connected during operation of the MSFIS, and the boundary containing the isolation devices is contained within the safety-related ALS-201 board using a qualified isolation device. Therefore, the NRC staff has determined that the MSFIS meets the requirements of Clause 5.6.3.1 of IEEE 603.

Clause 5.6.3.2 of IEEE 603, "Equipment in Proximity," states that 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, will 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, and that physical separation may be achieved by physical barriers or acceptable separation distance. This clause states that the separation of Class 1E equipment shall be in accordance with the requirements of IEEE Standard 384-1981. This clause further states that the physical barriers used to effect a safety system boundary shall meet the requirements of 5.3, "Quality," 5.4, "Equipment Qualification" and 5.5, "System Integrity" for the applicable conditions specified in 4.7 and 4.8 of the design basis.

The MSFIS will be mounted in existing enclosures within the control room. There is no change to the equipment in proximity with the installation of the new MSFIS, and there is no change to the physical separation or separation distance. Therefore, the capability of the MSFIS to accomplish its safety functions in the event of the failure of non-safety equipment has not changed. For this reason, the NRC staff determined that MSFIS meets the requirements of Clause 5.6.3.2 of IEEE 603.

3.3.5.2.7 IEEE 603-1991 Clause 5.7 - Capability for Test and Calibration

Clause 5.7 of IEEE 603-1991 states that the safety system shall have the capability for test and calibration while retaining the capability to accomplish its safety function, and that this capability be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. This clause further states that the testing of Class 1E systems be in accordance with the requirements of IEEE Standard 338-1987 (Reference 98). 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; however, appropriate justification must be provided; acceptable reliability of equipment operation must be demonstrated; and the capability shall be provided while the generating station is shut down. SRP Chapter 7, Appendix 7.1-C, Section 5.7, "Capability for Test and Calibration," provides acceptance criteria for IEEE Clause 5.7. First, it states that guidance on periodic testing of the safety system is provided in Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions" (Reference 121), and in Regulatory Guide 1.118, Revision 3, "Periodic Testing of Electric Power and Protection Systems" (Reference 129), that endorses IEEE Standard 338-1987. Section 5.7 acceptance criteria states that periodic testing should duplicate, as closely as practical, the overall performance required of the safety system, and that the test should confirm operability of both the automatic and manual circuitry. This capability should be provided to permit testing during power operation and that when this capability can only be achieved by overlapping tests, the test scheme must be such that the tests do, in fact, overlap from one test segment to another. Section 5.7 further states that test procedures that require disconnecting wires, installing jumpers, or other similar modifications of the installed equipment are not acceptable test procedures for use during power operation. SRP Chapter 7, Appendix 7.1-C, Section 5.7 further states that for digital computer-based systems, test provisions should address the increased potential for subtle system failures such as data errors and computer lockup. SRP BTP 7-17 describes additional considerations in the evaluation of test provisions in digital computer-based systems.

The NRC staff review of References 27 and 28 showed that the MSFIS has a maintenance bypass function for each MSIV and MFIV. When one division is in bypass, the other division will still have the capability to perform the MSFIS safety function, thus allowing the bypassed

division to be tested. Because the MSFIS does not contain sensors, but receives the isolation actuation determination from the SSPS, and because the MSFIS is not analog, no calibration is required. The NRC staff has therefore determined that the MSFIS has the necessary capability for test and calibration while retaining the capability to accomplish its safety function.

3.3.5.2.8 IEEE 603-1991 Clause 5.8 - Information Displays

Clause 5.8 of IEEE 603-1991 has four subclauses, 5.8.1, "Displays for Manually Controlled Actions," 5.8.2, "System Status Indication," 5.8.3, "Indication of Bypasses," and 5.8.4, "Location." Appendix 7.1-C, Section 5.8, "Information Displays," provides acceptance criteria for IEEE 603, Clause 5.8. This guidance states that the information displays for manually controlled actions should include confirmation that displays will be functional, and that safety system bypass and inoperable status indication should conform to the guidance of Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems" (Reference 123).

3.3.5.2.8.1 IEEE 603-1991 Clause 5.8.1 - Displays for Manually Controlled Actions

Clause 5.8.1 states that display instrumentation provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions will be part of the safety systems and will meet the requirements of IEEE Standard 497-1981 (Reference 105). The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. SRP Chapter 7, Appendix 7.1-C, Section 5.8, "Information Displays," provides no further review guidance for IEEE 603 Clause 5.8.1.

The MSFIS does not have manually controlled actions for safety functions for which no automatic control is provided and, therefore, this clause of IEEE 603 is not applicable.

3.3.5.2.8.2 IEEE 603-1991 Clause 5.8.2 - System Status Indication

Clause 5.8.2 states that display instrumentation provide accurate, complete, and timely information pertinent to safety system status, and that this information shall include indication and identification of protective actions of the sense and command features and execute features. Clause 5.8.2 further states that the design minimize the possibility of ambiguous indications that could be confusing to the operator; however, the display instrumentation provided for safety system status indication need not be part of the safety systems. SRP Chapter 7, Appendix 7.1-C, Section 5.8, "Information Displays," provides no further review guidance for IEEE 603 Clause 5.8.2.

The NRC staff review of References 27 and 28, Section 2.3.4, "Operator Status Information" and review of the methods of implementation of this status information during the May 12-15, 2008, Thread Audit at CS Innovations showed that the information is displayed in simple status and alarm lights. The NRC staff therefore determined that the system status indication is accurate, complete, and timely, and meets the requirements of IEEE 603-1991 Clause 5.8.2.

3.3.5.2.8.3 IEEE 603-1991 Clause 5.8.3 - Indication of Bypasses

Clause 5.8.3 states that 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 be provided in the control room. Clause 5.8.3 further states that this display instrumentation need not be part of the safety systems, that this indication shall be automatically actuated if the bypass or inoperative condition is expected to occur more frequently than once a year, and is expected to occur when the affected system is required to be operable, that the capability shall exist in the control room to manually activate this display indication, and that the 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 effect the actions. SRP Chapter 7, Appendix 7.1-C, Section 5.8, "Information Displays," provides no further review guidance for IEEE 603 Clause 5.8.3.

The NRC staff review of References 27 and 28, Section 2.3.4, "Operator Status Information" and review of the methods of implementation of this status information during the May 12-15, 2008, Thread Audit at CS Innovations showed that the bypass status of each valve is indicated by the status light showing a red color. The NRC staff therefore determined that if part of a safety system has been bypassed or deliberately rendered inoperative, continued indication of this fact is provided in the control room in the manner stipulated by IEEE 603-1991 Clause 5.8.3. The MSFIS therefore meets the requirements of IEEE 603-1991 Clause 5.8.3.

3.3.5.2.9 IEEE 603-1991 Clause 5.9 - Control of Access

Clause 5.9 of IEEE 603-1991 states that the safety system be designed to permit administrative control of access to safety system equipment. SRP Chapter 7, Appendix 7.1-C, Section 5.9, "Control of Access," provides acceptance criteria for IEEE Clause 5.10. This acceptance criteria states that administrative control is acceptable to assure that the access to the means for bypassing safety system functions is limited to qualified plant personnel and that permission of the control room operator is obtained to gain access, and that digital computer-based systems need to consider controls over electronic access, including access via network connections and maintenance equipment, to safety system software and data.

Reference 50, Section 1.2.1 states that the equipment shall be located in the WCGS Control Building's Main Control Equipment Room, and that this room is secured by the plant security system in a manner that only allows authorized personnel access. This limits the means to bypass the MSFIS safety system functions, via access controls, to authorized plant personnel. As discussed in Section 3.1.1.5.2 of this SE, the operate/bypass switch for each valve within the specific ALS rack shall be placed into bypass prior to the connection of maintenance equipment to that ALS rack, and the MSFIS provides maintenance bypass indications, as well as an alarm due to active maintenance equipment, to the control room operator. The MSFIS does not provide any network connection. Therefore, the MSFIS as controlled by WCGS meets the requirements of IEEE 603-1991 Clause 5.9.

3.3.5.2.10 IEEE 603-1991 Clause 5.10 – Repair

Clause 5.10 of IEEE 603-1991 states that safety systems be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. SRP Chapter 7, Appendix 7.1-C, Section 5.10, "Repair" provides acceptance criteria for IEEE Clause 5.10. This acceptance criteria states that while digital safety systems may include self-diagnostic capabilities to aid in troubleshooting, the use of self-diagnostics does not replace the need for the capability for test and calibration systems as required by Clauses 5.7 and 6.5 of IEEE Standard 603-1991.

The NRC staff review of References 27 and 28 and review of the methods used for on-line continuous self-test, failure detection and isolation, and off-line diagnostic aids during the May 12-15, 2008, Thread Audit at CS Innovations showed that the MSFIS was designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment and, therefore, meets requirements of IEEE 603-1991 Clause 5.10.

3.3.5.2.11 IEEE 603-1991 Clause 5.11 – Identification

Clause 5.11 of IEEE 603-1991 states that safety system equipment be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Standard 384-1981 and IEEE Standard 420-1982 (Reference 103); that identification of safety system equipment shall be distinguishable from any identifying markings placed on equipment for other purposes; that identification of safety system equipment and its divisional assignment shall not require frequent use of Reference material; and that the associated documentation shall be distinctly identified in accordance with the requirements of IEEE Standard 494-1974 (R1990) (Reference 104); however, 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. SRP Chapter 7, Appendix 7.1-C, Section 5.11, "Identification," provides acceptance criteria for IEEE Clause 5.11. This acceptance criterion also identifies IEEE 384 as guidance.

The MSFIS is being installed into existing cabinets and uses existing wiring, and there is no change from the existing safety group identification using cabinet nameplates and color-coded wiring. Within the MSFIS, each rack and each board has a front panel that identifies the board type. Each board also contains a NVM device that is read by the FPGA and contains configuration data and board identification information. The setpoint information can also be read by the ASU. FPGA build information is created when the FPGA image is generated and is integral to the FPGA logic. This can be read from the Joint Test Action Group (JTAG) port associated with each FPGA on each board. The NRC staff has determined that this meets the requirements of IEEE 603-1991 Clause 5.11.

3.3.5.2.12 IEEE 603-1991 Clause 5.12 - Auxiliary Features

Clause 5.12 of IEEE 603-1991 states that auxiliary supporting features meet all requirements of this standard, and that auxiliary features that perform a function that is not required for the safety systems to accomplish their safety functions and are 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. SRP

Chapter 7, Appendix 7.1-C, Section 5.12, "Auxiliary Features," provides acceptance criteria for IEEE Clause 5.12. This acceptance criterion states SRP BTP 7-9 provides specific guidance for the review of anticipatory trips that are auxiliary features of a reactor protection system.

There are no auxiliary features within the MSFIS that perform a function not required for the MSFIS to accomplish its safety functions, which are either not isolated from the safety system or have been developed as non-safety functions; therefore, Clause 5.12 of IEEE 603 is not applicable.

3.3.5.2.13 IEEE 603-1991 Clause 5.13 - Multi-Unit Stations

Clause 5.13 of IEEE 603-1991 states that 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, and that guidance on the sharing of electrical power systems between units is contained in IEEE Standard 308-1980 (Reference 96), and guidance on the application of the single failure criterion to shared systems is contained in IEEE Standard 379-1988. SRP Chapter 7, Appendix 7.1-C, Section 5.13, "Multi-Unit Stations," provides acceptance criteria for IEEE Clause 5.13. This acceptance criterion states that the shared user interfaces must be sufficient to support the operator needs for each of the shared units.

WCGS is not a multi-unit station and, therefore, Clause 5.13 of IEEE 603 is not applicable.

3.3.5.2.14 IEEE 603-1991 Clause 5.14 - Human Factors Considerations

Clause 5.14 of IEEE 603-1991 states that human factors 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 operators and maintainers can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Standard 1023-1988 (Reference 115). SRP Chapter 7, Appendix 7.1-C, Section 5.14, "Human Factors Considerations," provides acceptance criteria for IEEE Clause 5.13, and states that safety system human factors design should be consistent with the applicant/licensee's commitments documented in Chapter 18 of the USAR.

The NRC staff reviewed the WCGS "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 16, 2009 (Reference 25); References 27 and 28; individual board specifications; and the methods used for design (May 12-15, 2008, Thread Audit at CS Innovations). This review has shown that human factors were considered at the initial stages and throughout the design process and, therefore, the MSFIS design and design methods meet the requirements of IEEE 603-1991 Clause 5.14.

3.3.5.2.15 IEEE 603-1991 Clause 5.15 – Reliability

Clause 5.15 of IEEE 603-1991 states that 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, and that IEEE Standard 352-1987 (Reference 100) and IEEE Standard 577-1976 (Reference 106) provide guidance for reliability analysis. SRP Chapter 7, Appendix 7.1-C, Section 5.15, "Reliability," provides acceptance criteria for IEEE 603 Clause 5.15. This acceptance criterion states that the

applicant/licensee should justify that the degree of redundancy, diversity, testability, and quality provided in the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed and that for computer systems, both hardware and software reliability should be analyzed. The acceptance criteria further states that software that complies with the quality criteria of IEEE 603 Clause 5.3 and that is used in safety systems that provide measures for defense against common-cause failures, as previously described for IEEE 603 Clause 5.1, are considered by the NRC staff to comply with the fundamental reliability requirements of GDC 21, IEEE Standard 279-1971 (Reference 95), and IEEE Standard 603-1991.

Appendix 7.1-C, Section 5.15 further states that the assessment of reliability should consider the effect of possible hardware and software failures and the design features provided to prevent or limit the effects of these failures, and that hardware failure conditions to be considered should include failures of portions of the computer itself and failures of portions of communication systems. Hard failures, transient failures, sustained failures, and partial failures should be considered. Software failure conditions to be considered should include, as appropriate, software common-cause failures, cascading failures, and undetected failures. SRP Chapter 7, Appendix 7.1-C, Section 5.15 also references SRP Chapter 7, Appendix 7.1-D, and points out that quantitative reliability goals are not sufficient as a sole means of meeting the NRC's regulations for the reliability of digital computers used in safety systems.

WCGS established a desired reliability goal of two years mean time between failures (MTBFs) for the existing MSFIS equipment. A reliability analysis (Reference 79) was performed in accordance with IEEE Standard 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems," and IEEE Standard 577-2004, "IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities" (Reference 107). This analysis used the calculation model from MIL-HDBK-217B (December 1974), "Reliability Stress and Failure Rate Data for Electromagnetic Equipment." This analysis did not consider software failure, because the FPGA-based system does not contain traditional software, as discussed in Section 3.0 of this SE. The analysis did consider individual component failures, including failure of components of the FPGA. This analysis showed a MTBF for a single cabinet containing a Main Steam and a Feedwater rack as being 3.28 years. The overall MTBF for a combination of both redundant cabinets and using an estimated mean time to repair of 12 hours, was calculated to be 3948 years.

The NRC staff has reviewed this reliability analysis, and has determined that the calculated MTBF exceeds the reliability goal of two years and, therefore, meets the requirements of IEEE 603 Clause 5.15.

3.3.5.3 IEEE 603-1991 Clause 6 - Sense and Command Features Functional and Design Requirements

3.3.5.3.1 IEEE 603-1991 Clause 6.1 - Automatic Controls

Clause 6.1 states that for each design basis event, all protective actions should automatically initiate without operator action, except as justified in IEEE 603 Clause 4.5. SRP Chapter 7, Appendix 7.1-C, Section 6.1, "Automatic Controls," provides acceptance criteria for IEEE Clause

6.1. The acceptance criterion states the automatic initiation should be precise and reliable, and the evaluation of the precision of the safety system should be addressed to the extent that setpoints, margins, errors, and response times are factored into the analysis. Section 6.1 also states that SRP BTP 7-12 discusses considerations for the review of the process for establishing instrument setpoints.

As described in Section 3.0 of this SE, the MSFIS does not initiate the protective actions. The protective action is initiated by the SSPS, and the isolation signal is received by the MSFIS from the SSPS and, therefore, Clause 6.1 of IEEE 603 is not applicable to the MSFIS.

3.3.5.3.2 IEEE 603-1991 Clause 6.2 - Manual Control

Clause 6.2 states that means be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions, and that the means will minimize the number of discrete operator manipulations and will depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1. Clause 6.2 also requires implementation of manual actions necessary to maintain safe conditions after the protective actions are completed as specified in 4.10, with the information provided to the operators, the actions required of these operators, and the quantity and location of associated displays and controls be appropriate for the time period within which the actions shall be accomplished and the number of available qualified operators, and in an environment suitable for the operator, and suitably arranged for operator surveillance and action. SRP Chapter 7, Appendix 7.1-C, Section 6.2, "Manual Control," provides acceptance criteria for IEEE Clause 6.2. This acceptance criterion states that features for manual initiation of protective action should conform to Regulatory Guide 1.62, "Manual Initiation of Protection Action" (Reference 125), and will be functional, accessible within the time constraints of operator responses, and available during plant conditions under which manual actions may be necessary.

The NRC staff has reviewed the design of the MSFIS system, and has determined that the capability for manual action exists, and is essentially unchanged from the existing system. The operator is capable of closing or opening all main steam or feedwater valves, or can individually open or close the valves. There are two paired-sets of "all close" switches, where one pair is for each division and each set is for either the main steam valves or the feedwater valves. There are two sets of four individual "open/close" switches, where each set is for either the main steam or feedwater valves. Each individual "open/close" switch controls both divisions via separate contact signals. The NRC staff has determined that these valves meet the IEEE 603 Clause 6.2 requirement for manual initiation. The NRC staff has also determined that these valves allow the operators to maintain safe conditions after the protective actions are completed. The NRC staff determined that the switches are functional, accessible within the time constraints of operator responses, and available during plant conditions under which manual actions may be necessary. The NRC staff therefore determined that the MSFIS meets the requirements of Clause 6.2 of IEEE 603.

3.3.5.3.3 IEEE 603-1991 Clause 6.3 - Interaction Between the Sense and Command Features and Other Systems

Clause 6.3 states that if a single credible event can both 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, either an alternate channel or alternate equipment not subject to this failure will be provided, or equipment not subject to failure caused by the same single credible event shall be provided. SRP Chapter 7, Appendix 7.1-C, Section 6.3, "Interaction Between the Sense and Command Features and Other Systems," provides acceptance criteria for IEEE Clause 6.3. This acceptance criterion states that if the event of concern is a single failure of a sensing channel shared between control and protection functions, isolating the safety system from the sensing channel failure by providing additional redundancy or isolating the control system from the sensing channel failure by using data validation techniques to select a valid control input are approaches that have been previously accepted.

As discussed in this SE in Section 3.1.1.5, Communications, and in Section 3.3.5.2.6 on independence, the NRC staff has determined that no single credible event can both cause a non-safety system action that results in a condition requiring protective action and can concurrently prevent the protective action. For this reason, Clause 6.3 of IEEE 603 is not applicable to the MSFIS.

3.3.5.3.4 IEEE 603-1991 Clause 6.4 - Derivation of System Inputs

Clause 6.4 states that, to the extent feasible and practical, sense and command feature inputs be derived from signals that are direct measures of the desired variables as specified in the design basis. SRP Chapter 7, Appendix 7.1-C, Section 6.4, "Derivation of System Inputs," provides acceptance criteria for IEEE Clause 6.4. This acceptance criterion states that if indirect parameters are used, the indirect parameter must be shown to be a valid representation of the desired direct parameter for all events, and that for both direct and indirect parameters, the characteristics of the instruments that produce the safety system inputs, such as range, accuracy, resolution, response time, and sample rate, are consistent with the analysis provided in Chapter 15 of the USAR.

As described in Section 3.1.1 of this SE, the MSFIS does not receive sensor inputs. The sensors provide input to the SSPS, the protective action is initiated by the SSPS, and the isolation signal is received by the MSFIS from the SSPS. For this reason, Clause 6.4 of IEEE 603 is not applicable to the MSFIS.

3.3.5.3.5 IEEE 603-1991 Clause 6.5 - Capability for Testing and Calibration

Clause 6.5 states that it must be possible to check, 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, including the availability of each sense and command feature required during the post-accident period. SRP Chapter 7, Appendix 7.1-C, Section 6.5, "Capability for Testing and Calibration," provides acceptance criteria for IEEE Clause 6.5. This acceptance criterion confirms that the operational availability can be checked by varying the input to the sensor or by cross checking between redundant channels. The acceptance criteria also states that when only two channels of readout are provided, the basis used to ensure that an operator will not take incorrect action when the two channel readouts differ must be stated. SRP Chapter 7, Appendix 7.1-C, Section 6.5 also states that SRP BTP 7-17 concerning sensor check and surveillance test provisions for digital computer I&C systems.

The MSFIS does not receive sensor inputs. The sensors provide input to the SSPS, the protective action is initiated by the SSPS, and the isolation signal is received by the MSFIS from the SSPS. For this reason, Clause 6.5 of IEEE 603 is not applicable to the MSFIS.

3.3.5.3.6 IEEE 603-1991 Clause 6.6 - Operating Bypasses

Clause 6.6 states that if the applicable permissive conditions are not met, a safety system must automatically prevent the activation of an operating bypass or initiate the appropriate safety function, and if plant conditions change so that an activated operating bypass is no longer permissible, the safety system must either remove the appropriate active operating bypass, restore plant conditions so that permissive conditions once again exist, or initiate the appropriate safety function(s). SRP Chapter 7, Appendix 7.1-C, Section 6.6, "Operating Bypasses," provides acceptance criteria for IEEE Clause 6.6. This acceptance criterion states that the requirement for automatic removal of operational bypasses means that the reactor operator may not have a role in such removal; however, the operator may take action to prevent the unnecessary initiation of a protective action.

The NRC staff reviewed References 27 and 28 and determined that there are no operating bypass functions within the MSFIS. For this reason, Clause 6.5 of IEEE 603 is not applicable to the MSFIS.

3.3.5.3.7 IEEE 603-1991 Clause 6.7 - Maintenance Bypass

Clause 6.7 states that the safety system be designed such that while sense and command features equipment is in maintenance bypass, the capability of a safety system to accomplish its safety function must be retained, and during such operation, the sense and command features must continue to meet the requirements of 5.1 and 6.3. SRP Chapter 7, Appendix 7.1-C, Section 6.7, "Maintenance Bypass," provides acceptance criteria for IEEE Clause 6.7. This acceptance criterion states that provisions for this bypass need to be consistent with the required actions of the plant TSs.

As discussed in Sections 3.0, 3.1.1.4.5, and 3.1.1.5.1.3 of this SE, for the MSFIS, if one of the redundant divisions is in maintenance bypass, the other division is capable of performing the safety function. For this reason, the NRC staff has determined that the MSFIS meets the requirements of Clause 6.7 of IEEE 603.

3.3.5.3.8 IEEE 603-1991 Clause 6.8 – Setpoints

Clause 6.8 states that the allowance for uncertainties between the process analytical limit documented in Clause 4.4 and the device setpoint must be determined using a documented methodology, and where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design must provide a positive means of ensuring that the more restrictive setpoint is used when required. SRP Chapter 7, Appendix 7.1-C, Section 6.8, "Setpoints," provides acceptance criteria for IEEE Clause 6.8. This acceptance criteria states that the setpoint analysis should confirm that an adequate margin exists between operating limits and setpoints, such that there is a low probability for inadvertent actuation of the system, and should confirm that an adequate margin exists between setpoints and safety limits, and that additional guidance on establishment of instrument

setpoints can be found in Regulatory Guide 1.105, Revision 3, "Instrument Setpoints for Safety Systems" (Reference 128), and SRP BTP 7-12, and in Regulatory Issue Summary 2006-17, "NRC Staff Position on the Requirements of 10 CFR 50.36, 'Technical Specifications,' Regarding Limiting Safety System Settings During Periodic Testing and Calibration of Instrument Channels" (Reference 137). SRP Chapter 7, Appendix 7.1-C, Section 6.8 further states that where it is necessary to provide multiple setpoints as discussed in Clause 6.8.2 of IEEE Standard 603-1991, the NRC staff interpretation of "positive means" is that automatic action is provided to ensure that the more restrictive setpoint is used when required, and that SRP BTP 7-3 provides additional guidance on multiple setpoints used to allow operation with reactor coolant pumps out of service.

As described in Section 3.1.1 of this SE, the MSFIS does not receive sensor inputs, and has no sensor setpoints. The sensors provide input to the SSPS, the protective action is initiated by the SSPS, and the isolation signal is received by the MSFIS from the SSPS. For this reason, Clause 6.4 of IEEE 603 is not applicable to the MSFIS.

3.3.5.4 IEEE 603-1991 Clause 7 - Execute Feature - Functional and Design Requirements

3.3.5.4.1 IEEE 603-1991 Clause 7.1 - Automatic Control

Clause 7.1 of IEEE 603-1991 states that the safety system will have the capability incorporated into the execute features to receive and act upon automatic control signals from the sense and command features consistent with 4.4 of the design basis. SRP Chapter 7, Appendix 7.1-C, Section 7.1, "Automatic Control," provides the same acceptance criteria for IEEE 603 Clause 7.1 as was provided for Clause 6.1.

The MSFIS received isolation signal from the SSPS, acts upon them to close the main steam and feedwater valves. The NRC staff has determined that the MSFIS meets the requirements of Clause 7.1 of IEEE 603.

3.3.5.4.2 IEEE 603-1991 Clause 7.2 - Manual Control

Clause 7.2 of IEEE 603-1991 states that if manual control of any actuated component in the execute features is provided, the additional features needed to accomplish such manual control shall not defeat the requirements of 5.1 and 6.2, and that any capability to receive and act upon manual control signals from the sense and command features is consistent with the design basis. SRP Chapter 7, Appendix 7.1-C, Section 7.2, "Manual Control," provides the same acceptance criteria for IEEE 603 Clause 7.2 as was provided for Clause 6.2.

The operator is capable of closing or opening all main steam or feedwater valves, or can individually open or close the valves. There are two paired-sets of "all close" switches, where one pair is for each division and each set is for either the main steam valves or the feedwater valves. There are two sets of four individual "open/close" switches, where each set is for either the main steam or feedwater valves. Each individual "open/close" switch controls both divisions via separate contact signals. The NRC staff has determined that meets the IEEE 603 Clause 7.2 requirement for manual control.

3.3.5.4.3 IEEE 603-1991 Clause 7.3 - Completion of Protective Action

Clause 7.3 of IEEE 603-1991 states that the design of the execute features be such that once initiated, the protective actions of the execute features shall go to completion; however, this requirement does not preclude the use of equipment protective devices identified in 4.11 of the design basis or the provision for deliberate operator interventions. In addition, when the sense and command features reset, the execute features shall not automatically return to normal, but shall require separate, deliberate operator action to be returned to normal. SRP Chapter 7, Appendix 7.1-C, Section 7.3, "Completion of Protective Action," provides acceptance criteria for IEEE Clause 7.3. This acceptance criterion states the review should include review of functional and logic diagrams, and that the seal-in feature may incorporate a time delay as appropriate for the safety function.

The MSFIS does not initiate the isolation function, but receives the isolation signal from the SSPS. MSFIS then performs the valve control function to close the required valves. During the May 12-15, 2008, Thread Audit at CS Innovations, the NRC staff specifically examined the valve close and open functions, and reviewed the logic responsible for these functions. The NRC staff determined that once the isolation signal is received from the SSPS or a manual close or open signal is received from the operator, the protective action is sealed-in, and will continue until completed. Once the valves are automatically closed, the valves cannot be opened via manual action until the ESFAS isolation signal is no longer present. The NRC staff also determined that deliberate operator action was required to reset the MSFIS to automatic functionality. The NRC staff therefore concluded that the MSFIS meets Clause 7.3 of IEEE 603 requirement for completion of protective action.

3.3.5.4.4 IEEE 603-1991 Clause 7.4 - Operating Bypasses

Clause 7.4 of IEEE 603-1991 has the same requirements as Clause 6.6. SRP Chapter 7, Appendix 7.1-C, Section 7.4, "Operating Bypass," provides the same acceptance criteria for IEEE 603 Clause 7.4 as was provided for Clause 6.6.

As was stated in this SE in Section 3.3.5.3.6, the MSFIS system has no operating bypass functions. For this reason, Clause 7.4 of IEEE 603 is not applicable to the MSFIS.

3.3.5.4.5 IEEE 603-1991 Clause 7.5 - Maintenance Bypass

Clause 7.5 of IEEE 603-1991 has similar requirements as Clause 6.7, but also states that portions of the execute features with a degree of redundancy of one must be designed such that when a portion is placed in maintenance bypass, the remaining portions provide acceptable reliability. SRP Chapter 7, Appendix 7.1-C, Section 7.5, "Maintenance Bypass," provides the same acceptance criteria for IEEE 603 Clause 7.5 as was provided for Clause 6.7.

Section 3.3.5.3.7 of this SE discussed the ability of the MSFIS to provide the protective action with one redundant cabinet, even if the other cabinet is in maintenance. Section 3.3.5.2.15 of this SE discussed reliability, and noted that the reliability goal for the MSFIS function was defined by WCGS as 2 years MTBF for the existing MSFIS equipment, and that the reliability analysis (Reference 79) determined that the MTBF for a single cabinet containing a Main Steam

and a Feedwater rack is 3.28 years. For these reasons, the NRC staff has determined that the MSFIS meets the requirements of Clause 7.5 of IEEE 603.

3.3.5.5 IEEE 603-1991 Clause 8 - Power Source Requirements

Clause 8 of IEEE 603-1991 states that 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, and that specific criteria unique to the Class 1E power systems can be found in IEEE Standard 308-1980. This clause also states that for power systems with a degree of redundancy, the safety functions and acceptable reliability must be retained while power sources are in maintenance bypass. SRP Chapter 7, Appendix 7.1-C, Section 8 does not provide acceptance criteria for IEEE Clause 8.

Power to the MSFIS is being supplied via the existing WCGS safety-related 125 volt DC power system. Each MSFIS rack has two redundant power supplies, each capable of independently providing full power for the entire rack when one of the power supplies had failed or been removed. These power supplies are discussed in Section 3.1.1.4.6 of this SE. The MSFIS power supplies were designed and built to the same quality standards as the rest of the MSFIS system, and power supply failure was considered for the reliability and MTBF determinations. The NRC staff has therefore determined that the MSFIS meets the requirements of Clause 8 of IEEE 603.

3.3.6 Review IEEE 7-4.3.2-2003 Requirements

3.3.6.1 IEEE 7-4.3.2 Clause 4 - Safety System Design Basis

Clause 4 of IEEE 7-4.3.2 (Reference 120) states that there are no requirements beyond those found in IEEE Standard 603-1991. The replacement MSFIS system does not change the design basis and, therefore, requires no review.

3.3.6.2 IEEE 7-4.3.2 Clause 5 - Safety System Criteria

3.3.6.2.1 IEEE 7-4.3.2 Clause 5.1 - Single-Failure Criterion

Clause 5.1 of IEEE 7-4.3.2 states that there are no requirements beyond those contained in IEEE Standard 603-1991. The single failure requirements are discussed in Section 3.3.5.2.1 of this SE.

3.3.6.2.2 IEEE 7-4.3.2 Clause 5.2 - Completion of Protective Action

Clause 5.2 of IEEE 7-4.3.2 states that there are no requirements beyond those contained in IEEE Standard 603-1991. The completion of protective action requirements are discussed in Section 3.3.5.2.2 of this SE.

3.3.6.2.3 IEEE 7-4.3.2 Clause 5.3 – Quality

Clause 5.3 of IEEE Standard 7-4.3.2 states that hardware quality is addressed in IEEE Standard 603-1991, and that software quality is addressed in IEEE/EIA Standard 12207.0-1996 (Reference 119) and supporting standards.

CS Innovations has established a QA program based on 10 CFR Part 50, Appendix B, and was designated a 10 CFR Part 50, Appendix B, supplier by WCGS. CS Innovations Procedure QCP-3, "Design Control" (Reference 55), is the top-level procedure describes the high level development process steps. QCP-3 references a lower tier procedure, 9002-00033, "Hardware Design Development Procedure" (Reference 48), for more details of the design development process. Furthermore, Procedure 9002-00033 references three lower tier procedures for specifics regarding the electrical wiring (9002-00034, Electrical Wiring Design Development Procedure [Reference 48] and 9002-00024, "Electrical Wiring Design Review," Revision 2, dated June 9, 2007 [Reference 49]), board design and development (9002-00035, "Board Design Development Procedure" [Reference 48], and 9002-00025, "Board Design Review Procedure," Revision 2, dated June 9, 2007 [Reference 49]), and FPGA design and development (9002-00036, "FPGA Design Development Procedure" [Reference 48] and 9002-00026, "FPGA Design Review Procedure," Revision 2, dated June 9, 2007 [Reference 49]).

The NRC staff reviewed the development and review processes of these documents and that review can be found in Section 3.1.1.4.1 for hardware development, Section 3.2 for the life cycle development process for the programming aspects of the FPGA, and Section 3.3.5.2.3 of this SE for IEEE 603-1991 compliance. The NRC staff found these development and review processes acceptable.

3.3.6.2.3.1 IEEE 7-4.3.2 Clause 5.3.1 - Software Development

Clause 5.3.1 requires an approved quality assurance (QA) plan consistent with the requirements of IEEE/EIA 12207.0-1996 for all software that is resident at run time. As discussed in Section 3.0 of this SE, the MSFIS has no software resident in the system, but does use software to program the system. The QA plan used for this effort was reviewed, and that review was discussed in Section 3.2.1.3 of this SE. The review showed that the QA plan was acceptable for development of FPGA-based safety-related applications for use in nuclear power plants.

3.3.6.2.3.1.1 IEEE 7-4.3.2 Clause 5.3.1.1 - Software Quality Metrics

Clause 5.3.1.1 of IEEE 7-4.3.2 states that the use of software quality metrics shall be considered throughout the software life cycle to assess whether software quality requirements are being met.

As discussed in Section 3.0 of this SE, the MSFIS is an FPGA-based system that does not use software in a traditional sense and, therefore, use of software quality metrics is not possible. Both CS Innovations and WCNOG did consider methods for assessing whether programming quality requirements are being met. Section 4, "Project Life Cycle" of Reference 31 includes the life cycle phase characteristics identified in IEEE 7-4.3.2, with exception of performance history,

and CS Innovations document 6002-00001, "ALS Quality Assurance Plan," Revision 2, dated July 29, 2008 (Reference 80), discussed the methods used to determine in each of the life cycle phases mentions what methods will be used to determine compliance with the quality requirements. CSI 6101-00008 and CSI 6101-00009, "MSFIS Quality Assurance Plan," Revision 0.5, dated June 9, 2007 (Reference 81), include the requirements to provide objective evidence and traceability of assessments performed throughout the MSFIS project's life cycle. This determination was programmatic, and no metrics were used.

Based on the review of these documents, and during the thread audit performed at CS Innovations on May 12-15, 2008, the NRC staff reviewed, on a sampling basis, the implementation of these methods used to assess programming quality requirements, and found them acceptable. The NRC staff notes, however, that no metrics were used during this assessment and, therefore, Clause 5.3.1.1 does not apply to the MSFIS development effort.

WCNOC maintenance program maintains performance history; however, the determination of the appropriateness and completeness of the actual data maintenance is beyond the scope of this SE.

3.3.6.2.3.2 IEEE 7-4.3.2 Clause 5.3.2 - Software Tools

Clause 5.3.2 of IEEE 7-4.3.2 states that software tools used to support software development processes and V&V processes shall be controlled under configuration management, and that the tools shall either be developed to a similar standard as the safety-related software, or that 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.

CS Innovations utilizes several software tools to achieve the final design of the ALS platform. The tools utilized in the development life cycle are configuration controlled and maintained with all files associated with the project by configuration management. CS Innovations performs a tool assessment and qualification to ensure that tools are capable of performing the particular design or verification activity to an acceptable level of confidence.

CS Innovations "6000-00010, 'ALS Design Tools,' Revision 0.95, dated August 30, 2007 (Reference 82), Chapter 2 describes the tool assessment and qualification. This document discusses the method of assessment and the experience with the software tools used in the development processes to provide additional confidence in the suitability of the tools. The NRC staff agrees that this tool assessment and qualification meets the intent of Sub-clause 5.3.2, to confirm the software tools are suitable for use in the ALS platform design. However, those software tools are not qualified as safety-related due to lack of full V&V information for those software tools in their development process.

Based on the review of the CS Innovations and Baseline Engineering V&V processes as described in Section 3.2.1.10 of this SE, and verified during the on-site audit, the NRC staff determined that the output of the tools used was subject to V&V which would detect any defects or errors caused by the usage of the tools, and the use of tools in the development of the MSFIS system is consistent with the of requirements in this section and is, therefore, is acceptable.

3.3.6.2.3.3 IEEE 7-4.3.2 Clause 5.3.3 – V&V

Clause 5.3.3 of IEEE 7-4.3.2 states that a V&V program exists throughout the system life cycle, and states that the software V&V effort be performed in accordance with IEEE Standard 1012-1998. Section 3.2.1.10 of this SE discusses the CS Innovations, WCGS and Baseline Engineering V&V activities and the NRC staff review of those activities, and determined that the V&V program existed throughout the system life cycle, that the effort was performed in accordance with IEEE Standard 1012-1998, and was appropriate for a safety-related system in a nuclear power plant and is, therefore, acceptable.

3.3.6.2.3.4 IEEE 7-4.3.2 Clause 5.3.4 - Independent V&V Requirements

Clause 5.3.4 of IEEE 7-4.3.2 defines the levels of independence required for the V&V effort, in terms of technical independence, managerial independence, and financial independence. The independence of the V&V effort was reviewed by the NRC staff, and a discussion of that review and the reasons for approval of the V&V effort can be found in Section 3.2.1.10 of this SE.

The CS Innovations stated that its V&V team is staffed with members familiar with all processes from design, to manufacturing, to final test procedures and execution of the test equipment. Because the CS Innovations is a small company, it has chosen to head the V&V team with the president of the company. This does not constitute independence between financial interests and the V&V effort, but it does emphasize the focus on the V&V effort. WCNOG and Nutherm International performed independent V&V oversight of CS Innovations design, processes, and V&V steps. The NRC staff determined that this level of independence was acceptable.

3.3.6.2.3.5 IEEE 7-4.3.2 Clause 5.3.5 - Software Configuration Management

Clause 5.3.5 of IEEE 7-4.3.2 states that Software configuration management shall be performed in accordance with IEEE Standard 1042-1987, and that IEEE Standard 828-1998 provides guidance for the development of software configuration management plans. IEEE Standard 828-1990 and IEEE Standard 1042-1987 are endorsed by Regulatory Guide 1.169.

CS Innovations "6101-00005, 'MSFIS Configuration Management Plan,' Revision 0.8," dated June 9, 2007 (Reference 83), is based on IEEE Standard 828 and the guidance in IEEE Standard 1042. The Configuration Management 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 Configuration Management Plan also includes detailed requirements for document and software identification, release, archiving and audits.

The configuration management used by CS Innovations and WCGS was reviewed by the NRC staff, and a discussion of that review and the reasons for approval of the configuration management can be found in Section 3.2.1.11 of this SE, and was determined to be acceptable.

3.3.6.2.3.6 IEEE 7-4.3.2 Clause 5.3.6 - Software Project Risk Management

Clause 5.3.6 of IEEE 7-4.3.2-2003 defines the RM required for a software project. SRP Chapter 7, Appendix 7.1-D, Section 5.3.6, "Software Project Risk Management" provides

acceptance criteria for software project RM. This section states that software project RM is a tool for problem prevention, and be performed at all levels of the digital system project to provide adequate coverage for each potential problem area. It also states that 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. Additional guidance on the topic of RM is provided in IEEE/EIA 12207.0-1996 and IEEE Standard 1540-2001, "IEEE Standard for Life Cycle Processes – Risk Management" (Reference 118).

As discussed in Section 3.0 of this SE, the MSFIS does not contain traditional computer software programming, but rather contains devices that are programmable (FPGAs and NVMs). This characteristic necessitates an appropriate tailoring of IEEE 7-4.3.2, "Software Risk Management" for applicability to the MSFIS and the ALS platform. The MSFIS program implements management plans that address development risks throughout the life cycle, and these plans include the development and use of the programmable devices. The licensee primarily credits the V&V plan in conjunction with the quality control corrective action plan as addressing RM life cycle needs.

Reference 80 provides that risks will be identified within individual plans rather than a dedicated RM plan, and that risks will be managed and discussed during regular program meetings. Both Reference 47 and CSI "6002-00002, 'ALS Configuration Management Plan.' Revision 1," dated February 21, 2008 (Reference 85), contain provisions for the identification and management of risks. Each CS Innovations product development and review procedure has risk identification and evaluation including the 9002-00036, "FPGA Design Development Procedure" (Reference 48), and its associated 9002-00026, "FPGA Design Review Procedure" (Reference 49).

Prototyping as a method of risk mitigation is introduced in Reference 31 and discussed in Section 3.1.1.4.1.2 of this SE. Documentation of prototyping as a risk mitigation tool is contained within Reference 30 for FPGA programming. For example, Reference 37, OR0319, optional requirement identifier, demonstrates that technical and cost risks are being considered within the requirements specifications.

The NRC staff has reviewed the RM plans and activities for the MSFIS development and finds that these plans and activities meet the requirements of IEEE 7-4.3.2 for the MSFIS programmable device development activities.

3.3.6.2.4 IEEE 7-4.3.2 Clause 5.4 - Equipment Qualification

Clause 5.4 of IEEE 7-4.3.2-2003 defines the Equipment Qualification required for a software project. SRP Chapter 7, Appendix 7.1-D, Section 5.4, "Equipment Qualification," provides acceptance criteria for equipment qualifications. This section of App. 7.1-D states that in addition to the equipment qualification criteria provided by IEEE Standard 603-1991 and Section 5.4 of SRP Chapter 7, Appendix 7.1-C, additional criteria, as defined in Sections 5.4.1 and 5.4.2, are necessary to qualify digital computers for use in safety systems. These sections are discussed in the following subsections of this SE.

3.3.6.2.4.1 IEEE 7-4.3.2 Clause 5.4.1 - Computer System Testing

Clause 5.4.1 of IEEE 7-4.3.2-2003 discusses the software that should be operational on the computer system while qualification testing is being performed. SRP Chapter 7, Appendix 7.1-D, Section 5.4.1, "Computer System Testing," provides acceptance criteria for equipment qualifications. This section states that computer system equipment qualification testing should be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation.

As discussed in Section 3.0 of this SE, the MSFIS is an FPGA-based system; therefore, the MSFIS does not use software in a traditional sense and, therefore, there is no software to run while the system is in test. However FPGA's are programmed, and that programming is performed in a manner similar to a traditional μ P-based software program development, with the similar versatility and potential weaknesses, and for this reason, the NRC staff determined that this requirement would be that the qualification testing should be performed while the system has the equivalent to operational programming installed and operational. CS Innovations has performed qualification testing on the ALS platform-based MSFIS per requirements in WCGS "Specification J-105A(Q) for Replacement MSFIS System," Revision 5, dated February 16, 2009 (Reference 25). The system tested included full ALS rack with all circuit cards installed, as well as software and diagnostics that are representative of the production assembly. CS Innovations has functionally tested the equipment before each test and after the completion of each test. These tests are described in Nutherm International Inc. document TSP-9059, "Technical Procedures: Baseline Testing for Main Steam and/or Feedwater Isolation System (MSFIS) Rack," Revision 0, and Revision 1 (Reference 72).

The NRC staff reviewed these test procedures, and based on the review, the NRC staff found that the testing performed on the representative MSFIS hardware, that included an operational system with the appropriate programming, meets the criterion in this section and is therefore acceptable.

3.3.6.2.4.2 IEEE 7-4.3.2 Clause 5.4.2 - Qualification of Existing Commercial Computers

Clause 5.4.2 of IEEE 7-4.3.2-2003 defines the Qualification of Existing Commercial Computers for use in safety-related applications in nuclear power plants. SRP Chapter 7, Appendix 7.1-D, Section 5.4.2, "Qualification of Existing Commercial Computers," provides acceptance criteria for equipment qualifications. This section states that EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications" (Reference 93), and EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants" (Reference 94), provide specific guidance for the evaluation of commercial grade digital equipment and existing programmable logic controllers (PLC).

The CS Innovations ALS platform was developed under a 10 CFR Part 50, Appendix B, program specifically for the nuclear power industry and is, therefore, not considered commercial grade digital equipment. This requirement is therefore not applicable for the review of the WCGS MSFIS equipment.

3.3.6.2.5 IEEE 7-4.3.2 Clause 5.5 - System Integrity

Clause 5.5 of IEEE 7-4.3.2 states that in addition to the system integrity criteria provided by IEEE Standard 603-1991, the digital system shall be designed for computer integrity, test and calibration, and fault detection and self-diagnostics activities. These attributes are further defined in IEEE 7-4.3.2 Clauses 5.5.1, "Design for computer integrity," Clause 5.5.2, "Design for test and calibration," and Clause 5.5.3, "Fault detection and self-diagnostics." There are no specific acceptance criteria shown in SRP Chapter 7, Appendix 7.1-D, Section 5.5, "System Integrity."

3.3.6.2.5.1 IEEE 7-4.3.2 Clause 5.5.1 - Design for Computer Integrity

Clause 5.5.1 of 7-4.3.2 states that the computer be designed to perform its safety function when subjected to conditions, external or internal, that have significant potential for defeating the safety function.

Chapter 7 of Reference 29 describes the modes and states of the ALS platform, classifications of failures and the effect on the system. Chapter 8 describes the ALS platform communications, which discusses critical aspects of the integrity of the ALS platform. The NRC staff reviewed those chapters, and has determined that CS Innovations has designed the ALS platform to handle several external or internal events or conditions placed upon the system while maintaining full system integrity. During the thread audit performed at CS Innovations on May 12-15, 2008, the NRC staff reviewed the implementation of these requirements on a sampling basis, and determined that the intended design was appropriately implemented. The NRC staff therefore determined that the MSFIS system meets the criterion in Sub-clause 5.5.1, "Design for computer integrity."

3.3.6.2.5.2 IEEE 7-4.3.2 Clause 5.5.2 - Design for Test and Calibration

Clause 5.5.2 of 7-4.3.2 states that test and calibration functions not adversely affect the ability of the computer to perform its safety function, and that it shall be verified that the test and calibration functions do not affect computer functions that are not included in a calibration change. The clause further states that V&V, configuration management, and QA be required for test and calibration functions on separate computers such as test and calibration computers that provide the sole verification of test and calibration data, but that V&V, configuration management, and QA is 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.

CSI 6000-00000 discussed the testability aspects of the ALS platform, and describes the self-test within the Core Logic Board, Service & Test Board, Input Board, Solid-State Output Board, and FET & Sensor Board. The ALS platform has several built-in self-test and manual test capabilities. A run-time test strategy is implemented in the ALS platform that provides self-testing to validate the system integrity. The on-line test capabilities of the ALS platform are contained within the ALS platform, thus no separate test systems are required. The specific concerns regarding the calibration and changing of setpoints do not apply to this review, because, as described in Section 3.1 of this SE the MSFIS receives the trip command from the SSPS, and does not contain the setpoint values. The NRC staff reviewed the self-test

capabilities of the MSFIS, and determined that self-testing will not adversely affect the ALS platform in performing its safety function and is therefore acceptable for this use at WCGS.

The NRC staff also reviewed the overall test and calibration functions of the ALS platform. The NRC staff determined that the design of the ALS platform is such that any setpoint data can be contained in the onboard NVM, a serial-flash device, and that this memory NVM cannot be written to or modified without the use of special tools that are available only to the vendor and not to the licensee. However, the programmable device configuration and version information is available to the ASU Service Unit in a read-only fashion.

The NRC staff review of the ALS platform determined that the ALS platform meets the IEEE 7-4.3.2 requirement for design for test and calibration, and because this determination is not MSFIS-specific, this determination is suitable for reference in future uses of the ALS platform in safety-related applications in nuclear power plants.

3.3.6.2.5.3 IEEE 7-4.3.2 Clause 5.5.3 - Fault detection and Self-diagnostics

Clause 5.5.3 of 7-4.3.2 discusses fault detection and self-diagnostics, and stated that if reliability requirements warrant self-diagnostics, then computer programs should contain functions to detect and report computer system faults and failures in a timely manner, and that these 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.

The ALS platform incorporates self-diagnostic features to provide a means to detect and alert any failure within the ALS platform. For each board, these self-diagnostic features are discussed in the hardware specification for that board (see Table 3 of this SE), and for the overall system, the ability for fault detection and self-diagnostics is discussed in the ALS Platform Specification (Reference 33). The NRC staff reviewed these self-diagnostic features, and determined that they will not impede the safety function of the system. The NRC staff also determined that CS Innovations built the self-diagnostics into the system and did not implement them as an add-on and, therefore, these functions were subject to the same high-quality design development process as the rest of the system. The self-diagnostics features are functional during all states of the system operation including power-up, operation, and bypass modes of operation. The NRC staff determined that the ALS platform meets the criterion in Sub-clause 5.5.3 for fault detection and self-diagnostics. Because this determination is not MSFIS-specific, this determination is suitable for reference in future uses of the ALS platform in safety-related applications in nuclear power plants.

3.3.6.2.6 IEEE 7-4.3.2 Clause 5.6 – Independence

Clause 5.6 of IEEE 7-4.3.2 states that, in addition to the requirements of IEEE Standard 603-1991, data communication between safety channels or between safety and non-safety systems shall not inhibit the performance of the safety function. SRP Chapter 7, Appendix 7.1-D, Section 5.6, "Independence" provides acceptance criteria for equipment qualifications. This section states 10 CFR Appendix A, GDC 24, "Separation of protection and control systems," states that the protection system be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control and

protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system, and that interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

The licensee stated that the ALS platform-based MSFIS will be installed in the existing Group 1 and Group 4 cabinets, maintaining the current safety group separations. New switches installed on the operator control panel to control both divisions include physical barriers that meet the requirements of IEEE Standard 384-1992. The NRC staff notes that verification of the actual installation is beyond the scope of this SE, and that the installation will be audited by the staff of the regional office during the installation. Because no interface design changes between the existing MSFIS system and other systems, the physical separation, electrical isolation, physical barriers, and the effect of single random failure in other systems remain the same. The licensee also stated that the only interconnection to non-safety equipment is with the ASU used for test and maintenance. The NRC staff review of the MSFIS verified this intent, but again, verification of the actual installation is beyond the scope of this SE, and that the installation will be audited by the staff of the regional office during the installation. Any valid communication connections via the ASU USB port are alarmed in the Control Room, and administrative controls prevent connection of the ASU unless the division is in a maintenance bypass. Having reviewed Sections 6.5, "ASU Test Mode," and 13.1, "ASU Interface," of Reference 51, the NRC staff concludes that the MSFIS meets the system independence requirement in this section.

Based on the review, the NRC staff found that the MSFIS system meets the criterion in this section and, therefore, is acceptable.

3.3.6.2.7 IEEE 7-4.3.2 Clause 5.7 - Capability for Test and Calibration

Clause 5.7 of IEEE 7-4.3.2 states that there are no requirements beyond those found in IEEE Standard 603-1991. This clause is redundant to Clauses 5.5.2 and 5.5.3 of IEEE 7-4.3.2, and the discussions on those sections are found in Sections 3.3.5.2.7 and 3.3.5.3.5 of this SE.

3.3.6.2.8 IEEE 7-4.3.2 Clause 5.8 - Information Displays

Clause 5.8 of IEEE 7-4.3.2 states that there are no requirements beyond those found in IEEE Standard 603-1991. However, in the past, information displays only provided a display function and, therefore, required no two-way communications. More modern display systems may also have included control functions and, therefore, the NRC staff reviewed the capacity for information displays to ensure that incorrect functioning of the information displays does not prevent the safety function from being performed when necessary. For the MSFIS, there are no changes from the existing MSFIS design, so the display for manually controlled action will not prohibit the MSFIS system to accomplish its safety functions. The ALS platform-based MSFIS includes a "Summary Trouble Alarm," that will activate on any system fault for each division on the operator control panel. The ALS platform-based MSFIS includes a status indicator that will indicate if any valve is in bypass mode, for each division on the operator control panel. These alarms and status indications are a one-way binary signal, and there is no data path back to the MSFIS. The NRC staff has determined that there is no ability of the information displays to affect the operation of the MSFIS and, therefore, this system is appropriate for use in this safety-related application at WCGS.

3.3.6.2.9 IEEE 7-4.3.2 Clause 5.9 - Control of Access

Clause 5.9 of IEEE 7-4.3.2 states that there are no requirements beyond those found in IEEE Standard 603-1991. For this reason, there is no additional guidance beyond that found in Section 5.9 of SRP Chapter 7, Appendix 7.1-C and Regulatory Guide 1.152, Revision 2. A discussion on control of access and the review can be found in Section 3.3.5.2.9 of this SE.

WCGS plant security controls MSFIS system physical access and administrative controls limit access when the ASU is connected. For these reasons, the NRC staff found that the MSFIS system meets the criterion in this section and, therefore, is acceptable.

3.3.6.2.10 IEEE 7-4.3.2 Clause 5.10 – Repair

Clause 5.10 of IEEE 7-4.3.2 states that there are no requirements beyond those found in IEEE Standard 603-1991. For this reason, there is no additional guidance in Section 5.10 of SRP Chapter 7, Appendix 7.1-C. A discussion on repair and the review can be found in Section 3.3.5.2.10 of this SE.

3.3.6.2.11 IEEE 7-4.3.2 Clause 5.11 – Identification

Clause 5.11 of IEEE 7-4.3.2 states that identification requirements specific to software systems (i.e., firmware and software) identification shall be used to assure the correct software is installed in the correct hardware component; means shall be included in the software such that the identification may be retrieved from the firmware using software maintenance tools; and physical identification requirements of the digital computer system hardware shall be in accordance with the identification requirements in IEEE Standard 603-1991. SRP Chapter 7, Appendix 7.1-D, Section 5.11, "Identification" provides acceptance criteria and adds that the identification should be clear and unambiguous. The identification should include the revision level, and should be traceable to configuration control documentation that identifies the changes made by that revision for equipment qualifications.

CS Innovations document 6101-00002, the ALS Level-1 System Specification, discussed programming information stored in each board's NVM device attached to the FPGA device. This information is local to each board, and contains local settings, such as channel setup, sequencer setup, timing setup, and build information, including the version and revision of the programming. FPGA build information is created when the FPGA image is generated and is integral to the FPGA logic. The information can be read by the ASU. The NRC staff reviewed the ALS Level-1 System Specification, and determined that the required identification requirements are met, and the ALS platform is in compliance with this requirement. Additional discussion on identification and review can be found in Section 3.3.5.2.11 of this SE.

3.3.6.2.12 IEEE 7-4.3.2 Clause 5.12 - Auxiliary Features

Clause 5.12 of IEEE 7-4.3.2 states that there are no requirements beyond those found in IEEE Standard 603-1991. For this reason, there is no additional guidance, and no review for compliance with IEEE 7-4.3.2 is required. A discussion on auxiliary features and the review can be found in Section 3.3.5.2.12 of this SE.

3.3.6.2.13 IEEE 7-4.3.2 Clause 5.13 - Multi-Unit Stations

Clause 5.13 of IEEE 7-4.3.2 states that there are no requirements beyond those found in IEEE Standard 603-1991. For this reason, there is no additional guidance, and no review for compliance with IEEE 7-4.3.2 is required. In addition, this clause is not applicable as WCGS is a single-unit facility. A discussion on multi-unit stations and the review can be found in Section 3.3.5.2.13 of this SE.

3.3.6.2.14 IEEE 7-4.3.2 Clause 5.14 - Human Factors Considerations

Clause 5.14 of IEEE 7-4.3.2 states that there are no requirements beyond those found in IEEE Standard 603-1991. For this reason, there is no additional guidance, and no review for compliance with IEEE 7-4.3.2 is required. A discussion on human factors considerations and the review can be found in Section 3.3.5.2.14 of this SE.

3.3.6.2.15 IEEE 7-4.3.2 Clause 5.15 – Reliability

Clause 5.15 of IEEE 7-4.3.2 states that, in addition to the requirements of IEEE Standard 603-1991, when reliability goals are identified, the proof of meeting the goals shall include the software. Guidance is provided in SRP Chapter 7, Appendix 7.1-C, Section 5.15.

In the case of the MSFIS, there is no software to include when determining reliability. The FPGA-based system is programmed, as discussed in Section 3.1.1.4.1.4.3 of this SE. This programming results in a hard-wired system consisting only of hardware items. Once V&V has determined the quality of the programming, and testing has determined that the programming functions correctly to perform the safety function, there is no software used during the operation of the system while performing its safety function and, therefore, there is no further contribution of software failure to the overall failure rate. The V&V and testing of the MSFIS are discussed in Sections 3.1.1.4.1.5, 3.1.1.4.1.6, 3.2.1.10, and 3.3.1 of this SE.

WCGS performed reliability and availability analysis for the MSFIS in accordance with IEEE Standard 352-1987 and IEEE Standard 577-1976. This analysis can be found in Reference 79. The analysis is based on the prediction data of MIL-HDBK-217B, "Reliability Stress and Failure Rate Data for Electromagnetic Equipment." The analysis determined that the calculated reliability and availability of the MSFIS system is 99.958 percent. The NRC staff reviewed this analysis, and agrees that the results of the reliability and availability prediction support use of the MSFIS system in this safety-related application. A discussion on reliability and the review can be found in Section 3.3.5.2.15 of this SE.

3.3.6.3 IEEE 7-4.3.2 Clause 6 - Sense and Command Features

Clause 6 of IEEE 7-4.3.2 states that there are no requirements beyond those found in IEEE Standard 603-1991. For this reason, there is no additional guidance, and no review for compliance with IEEE 7-4.3.2 is required. A discussion on sense and command features and the review can be found in Section 3.3.5.3 of this SE.

3.3.6.4 IEEE 7-4.3.2 Clause 7 - Execute Features

Clause 7 of IEEE 7-4.3.2 states that there are no requirements beyond those found in IEEE Standard 603-1991. For this reason, there is no additional guidance, and no review for compliance with IEEE 7-4.3.2 is required. A discussion on execute features and the review can be found in Section 3.3.5.4 of this SE.

3.3.6.5 IEEE 7-4.3.2 Clause 8 - Power Source Requirements

Clause 8 of IEEE 7-4.3.2 states that there are no requirements beyond those found in IEEE Standard 603-1991. For this reason, there is no additional guidance, and no review for compliance with IEEE 7-4.3.2 is required. A discussion on power source requirements and the review can be found in Section 3.3.5.5 of this SE.

4.0 NRC FINDINGS

4.1 Summary of Regulatory Compliance

This SE discussed the acceptability of the ALS platform as used in the MSFIS at WCGS. The GDC listed in 10 CFR Part 50 Appendix A establish minimum requirements for the design of nuclear power plants. IEEE 603-1991 is also incorporated in 10 CFR 50.55a(h). The regulatory guides and the endorsed industry codes and standards listed in NUREG-0800, SRP, Table 7-1, are the guidelines used as the basis for this evaluation.

The NRC staff concludes that the design of the MSFIS is acceptable and meets the relevant requirements of GDCs 1, 2, 4, 10, 13, 15, 16, 19-24, and 50.55a(a)(1), and 10 CFR 50.55a(h) as discussed below.

10 CFR 50.55a(a)(1), "Quality Standards for Systems Important to Safety," is addressed by conformance with the codes and standards listed in the SRP. CS Innovations used these codes and standards in the development of the ALS platform and, therefore, the ALS platform is in conformance with this requirement.

10 CFR 50.55a(h) endorses IEEE Standard 603-1991, that addresses both system level design issues and quality criteria for qualifying devices. WCGS and CS Innovations addressed these issues in the submitted documentation. In Section 3.3.5 of this SE, the NRC staff determined that the MSFIS meets the criteria of IEEE Standard 603, and in Section 3.3.6 of this SE, the supplemental standard IEEE Standard 7-4.3.2-2003. The NRC staff concludes, therefore, that the MSFIS is in compliance with this requirement.

The NRC staff has verified that the applicant has provided sufficient information and that the results of the review support the following:

1. The review of the instrumentation and control aspects of the MSFIS by the NRC staff determined that the MSFIS is intended to receive main steam and feedwater isolation signals from the SSPS or from manual initiation by the plant operators, and provide control of the main steam and feedwater isolation valves based upon these signals.

The NRC staff conducted a review of MSFIS for conformance to the guidelines in the regulatory guides, industry standards and BTPs applicable to these systems. Based upon the review of the MSFIS design for conformance to the guidelines, the NRC staff concludes that the MSFIS conforms to the guidelines applicable to the MSFIS. Therefore, the NRC staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met.

The review included the identification of those systems and components for the ESFAS and ESF control systems that are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles, and determined that MSFIS is among these systems. Section 3.3.1 of this SE addresses the qualification program to demonstrate the capability of these systems and components to survive the aforementioned effects. Therefore, the NRC staff finds that the identification of these systems and components satisfies the requirements of GDC 2 and 4.

Based on the review of MSFIS status information, manual initiation capabilities, control capabilities, and provisions to support safe shutdown, the NRC staff concludes that information is provided to monitor the system over the anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety. Appropriate controls are provided for manual initiation and control of MSFIS isolation functions. MSFIS controls appropriately support actions to operate the nuclear power unit safely under normal conditions and to achieve and maintain a safe condition under accident conditions. Therefore, the NRC staff finds that the MSFIS design satisfies the requirements of GDC 13 and 19.

Based on the review of MSFIS functions as documented in Section 3.3.5 of this SE, the NRC staff concludes that the MSFIS conforms to the requirements of IEEE Standard 603-1991. Therefore, the NRC staff finds that the MSFIS satisfies the requirements of GDC 20.

The MSFIS conforms to the guidelines for periodic testing in Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions," and Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems." The bypassed and inoperable status indication conforms to the guidelines of Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems." The MSFIS conforms to the guidelines on the application of the single-failure criterion in IEEE Standard 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," as supplemented by Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Safety Systems." Based on the review, the NRC staff concludes that the MSFIS satisfies the requirement of IEEE Standard 603-1991 with regard to the system reliability and testability. Therefore, the NRC staff finds that the MSFIS satisfies these requirements of GDC 21.

The MSFIS conforms to the guidelines in Regulatory Guide 1.75, "Criteria for Independence of Electrical Safety Systems," for the protection system independence. Based on the review, the NRC staff concludes that the MSFIS satisfies the requirement of IEEE Standard 603-1991 with regard to the system's independence. Therefore, the NRC staff finds that the MSFIS satisfies the requirements of GDC 22.

Based on the review of the failure modes and effects analysis for the MSFIS, the NRC staff concludes that the system is designed to fail into a safe state if conditions such as disconnection of the system, loss of energy, or a postulated adverse environment are experienced. Therefore, the NRC staff finds that the MSFIS satisfies the requirements of GDC 23.

Based on the review of the interfaces between the MSFIS and plant operating control systems, the NRC staff concludes that the system satisfies the requirements of IEEE Standard 603-1991 with regard to control and protection system interactions. Therefore, the NRC staff finds the MSFIS satisfies the requirements of GDC 24.

The conclusions noted are based upon the requirements of IEEE Standard 603-1991 with respect to the design of the MSFIS. Therefore, the NRC staff finds that the MSFIS satisfies the requirements of 10 CFR 50.55a(h).

In the review of the MSFIS, the NRC staff examined the dependence of this system on the availability of essential auxiliary systems. Based on this review, the NRC staff concludes that the design of the MSFIS is compatible with the functional requirements of auxiliary supporting features and other auxiliary features systems.

2. Based on the review of programming development plans and the development process and design outputs, the NRC staff concludes that the computer systems meet the guidance of Regulatory Guide 1.152. Therefore, the special characteristics of computer systems have been adequately addressed, and the NRC staff finds that the MSFIS satisfies these requirements of GDC 1 and 21.

Based on the review of the applicant/licensee's defense-in-depth and diversity analysis, the NRC staff concludes that the MSFIS complies with the criteria for defense against common-cause failure in digital instrumentation and control systems. Therefore, the NRC staff finds that adequate diversity and defense against common-cause failure have been provided to satisfy these requirements of GDC 21 and 22, and the Staff Requirements Memorandum on SECY-93-087.

4.2 Future Use of ALS Platform

4.2.1 ALS Process Documentation

The following generic ALS process documentation, in the revision listed, has been reviewed by the NRC staff and has been determined to be suitable for reference in future use of the ALS platform in safety-related applications in nuclear power plants. Modification of these documents to new revision levels will require review of the changes, to determine that those changes do not invalidate the NRC staff's acceptance. Process documents required for review of future uses of the ALS platform which are not contained in this list must be submitted on an application specific basis.

- 6000-00008, ALS Board Test Plan, Revision 0.8, dated June 9, 2007 (References 66 and 67)

- 6002-00002, ALS Configuration Management Plan, Revision 2, dated July 28, 2008 (Reference 63)
- 6002-00003, ALS VV Plan, Revision 1, dated January 5, 2009 (Reference 47)
- 6002-00004, ALS EQ Plan, Revision 2, dated February 20, 2009 (Reference 34)
- 6002-00031, ALS Diversity Analysis, Revision 0, dated January 13, 2009 (Reference 75)
- 9002-00024, Electrical Wiring Design Review, Revision 2, dated June 9, 2007 (Reference 49)
- 9002-00025, Board Design Review Procedure, Revision 2, dated June 9, 2007 (Reference 49)
- 9002-00026, FPGA Design Review Procedure, Revision 2, dated June 9, 2007 (Reference 49)
- 9002-00033, Hardware Design Development Procedure (Reference 48)
- 9002-00034, Electrical Wiring Design Development Procedure (Reference 48)
- 9002-00035, Board Design Development Procedure (Reference 48)
- 9002-00036, FPGA Design Development Procedure (Reference 48)
- 9006-00008, Return for Material Repair Procedure, Revision 0, dated January 16, 2009 (Reference 60)
- QCP-1, Quality Control Procedure, Revision 0, dated January 25, 2007 (Reference 55)

4.2.2 ALS Hardware and Programming Documentation

The following generic ALS hardware documentation, in the revision listed, has been reviewed by the NRC staff and has been determined to be suitable for reference in future use of the ALS platform in safety-related applications in nuclear power plants. Modification of these documents to new revision levels will require review of the changes, to determine that those changes do not invalidate the NRC staff's acceptance.

- 6000-00000, ALS Level-1 System Specification Revision 1.02, dated June 9, 2007 (Reference 51)
- 6002-00026, ALS Platform Overview, Revision 2, dated January 16, 2009 (Reference 29)
- 6002-00010, ALS Platform Requirements Specification, Revision 2, dated January 15, 2009 (Reference 32)
- 6002-00011, ALS Platform Specification, Revision 2, dated January 14, 2009 (Reference 33)

The following generic ALS hardware and FPGA programming, in the revision listed, has been reviewed by the NRC staff and has been determined to be suitable for use in future use of the ALS platform in safety-related applications in nuclear power plants. Modification of this

hardware of FPGA programming to new revision levels will require review of the changes, to determine that those changes do not invalidate the NRC staff's acceptance.

Item	Version	FPGA Version	Documentation
ALS-101 Core Logic Board	B	1.02	6002-10101 ALS-101 Requirements Specification (Reference 35) 6002-10102 ALS-101 Hardware Specification (Reference 36)
ALS-201 Service & Test Board	B	1.00	6002-20101 ALS-201 Requirements Specification (Reference 42) 6002-20102 ALS-201 Hardware Specification (Reference 44)
ALS-301 32-channel digital input board	B	1.01	6002-30101 ALS-301 Requirements Specification (Reference 37) 6002-30102 ALS-301 Hardware Specification (Reference 38)
ALS-401 16-channel output board	B	1.01	6002-40101 ALS-401 Requirements Specification (Reference 39) 6002-40102 ALS-401 Hardware Specification (Reference 40)
ALS-411 4-channel FET output board	B1	1.01	6002-41101 ALS-411 Requirements Specification (Reference 41) 6002-41102 ALS-411 Hardware Specification (Reference 42)
ALS-905 Power Supply Board	B3	N/A	6002-90501 ALS-905 Requirements Specification (Reference 45) 6002-90502 ALS-905 Hardware Specification (Reference 46)

Any new system or hardware developed in the future will require Reference to the development plans and procedures used are those previously approved and shown in Section 3.2.1 of this SE, and demonstration that those plans and procedures were used. Any plans or procedures which are required for NRC staff review which has not been previously approved shall be supplied prior to the NRC staff review of the new system or hardware. In addition, the new hardware and programming documentation must be as comprehensive as that shown above. At a minimum, any new use of the ALS platform will require review of the application-specific vendor and ALS requirements, the final V&V report, and the final test report; however, additional information and documentation may be required by the NRC staff. Any new hardware will require environmental, response time, and cyber security qualification as shown in Sections 3.3.1, 3.3.2, and 3.3.4 of this SE.

5.0 STATE CONSULTATION

In accordance with the Commission's regulations, the Kansas State official was notified of the proposed issuance of the amendment. The State official had no comments.

6.0 ENVIRONMENTAL CONSIDERATION

The amendment changes the requirements with respect to use of a facility component located within the restricted area as defined in 10 CFR Part 20. The NRC staff has determined that the amendment involves no significant increase in the amounts, and no significant change in the types, of any effluents that may be released offsite, and that there is no significant increase in

individual or cumulative occupational radiation exposure. The Commission has previously issued a proposed finding that the amendment involves no significant hazards consideration and there has been no public comment on such finding, published in the *Federal Register* on June 19, 2007 (72 FR 33785). Accordingly, the amendment meets the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(9). Pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendment.

7.0 CONCLUSION

The Commission has concluded, based on the considerations discussed herein, that (1) there is reasonable assurance that the health and safety of the public will not be endangered by use of the MSFIS in the proposed manner, (2) such use will be conducted in compliance with the Commission's regulations, and (3) the issuance of the amendment will not be inimical to the common defense and security or to the health and safety of the public.

8.0 REFERENCES

1. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-07-0004, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Revision 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),' March 14, 2007 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML070800193).
2. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-07-0008, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Supplemental Information on Main Steam and Feedwater Isolation System Controls Modification," April 18, 2007 (ADAMS Accession No. ML071160332).
3. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-07-0013, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Response to Request for Additional Information Relating to Replacement of the Main Steam and Feedwater Isolation System Controls," May 9, 2007 (ADAMS Accession No. ML071350247).
4. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-07-0022, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Supplemental Information on Main Steam and Feedwater Isolation System Controls Modification," June 15, 2007 (ADAMS Accession No. ML071770452).
5. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-07-0039, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Response to NRC Letter dated August 8, 2007, Regarding Main Steam and Feedwater Isolation System Controls Modifications," August 31, 2007 (ADAMS Accession No. ML072480530).
6. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-07-0040, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Response to Request for Additional Information Relating to Replacement of the Main Steam and Feedwater

Isolation Valves and Controls," September 12, 2007 (ADAMS Accession No. ML072620128).

7. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-07-0041, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Additional Response to NRC Letter dated August 8, 2007, Regarding the Main Steam and Feedwater Isolation System Controls Modification," September 20, 2007 (ADAMS Accession No. ML072700498).
8. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-07-0050, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Response to Request for Additional Information Relating to Replacement of the Main Steam and Feedwater Isolation Valves and Controls," October 16, 2007 (ADAMS Accession No. ML072970684).
9. Matthew W. Sunseri, Wolf Creek Nuclear Operating Corporation, WO-07-0028, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Response to Request for Additional Information Relating to Replacement of the Main Steam and Feedwater Isolation Valves and Controls," November 16, 2007 (ADAMS Accession No. ML073241402) (Withdrawn by letter dated February 17, 2009).
10. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-07-0060, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Response to Request for Additional Information Relating to Replacement of the Main Steam and Feedwater Isolation Valves and Controls," December 14, 2007 (ADAMS Accession No. ML073550325).
11. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-07-0062, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Response to Request for Additional Information Relating to Replacement of the Main Steam and Feedwater Isolation Valves and Controls," December 14, 2007 (ADAMS Accession No. ML080230167).
12. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-07-0052, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Response to Request for Additional Information Relating to Replacement of the Main Steam and Feedwater Isolation Valves and Controls," December 18, 2007 (ADAMS Accession No. ML073620328).
13. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-08-0004, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Additional Information Regarding Main Steam and Feedwater Isolation System (MSFIS) Controls Modification," January 18, 2008 (ADAMS Accession No. ML080250069).
14. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-08-0005, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Response to Request for Additional Information Relating to Replacement of the Main Steam and Feedwater

Isolation Valves and Controls," January 18, 2008 (ADAMS Accession No. ML080250061).

15. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-08-0008, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Additional Information Regarding Main Steam and Feedwater Isolation System (MSFIS) Controls Modification," January 31, 2008 (ADAMS Accession No. ML080390312).
16. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-08-0011, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Revisions to Proposed Changes to Technical Specification 3.7.3, 'Main Feedwater Isolation Valves (MFIVs)'," February 26, 2008 (ADAMS Accession No. ML080640632).
17. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-08-0014, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Additional Information Regarding Main Steam and Feedwater Isolation System (MSFIS) Controls Modification," February 28, 2008 (ADAMS Accession No. ML080940559).
18. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-08-0017, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Additional Information Regarding Main Steam and Feedwater Isolation System (MSFIS) Controls Modification," March 14, 2008 (ADAMS Accession No. ML080810088).
19. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-08-0026, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Withdrawal and Resubmission of Submittal Containing Additional Information Regarding Main Steam and Feedwater Isolation System (MSFIS) Controls Modification," April 26, 2008 (ADAMS Accession No. ML081290378).
20. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-08-0032, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Submittal of Additional Information Regarding Main Steam and Feedwater Isolation System (MSFIS) Controls Modification," May 14, 2008 (ADAMS Accession No. ML081420366).
21. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-08-0035, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Main Steam and Feedwater Isolation System (MSFIS) Controls Modification - Electromagnetic Compatibility Tests," June 19, 2008 (ADAMS Accession No. ML081790156).
22. Warren B. Wood, Wolf Creek Nuclear Operating Corporation, GC-08-0024, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Resubmittal of Information Regarding Main Steam and Feedwater Isolation System (MSFIS) Controls Modification," July 31, 2008 (ADAMS Accession No. ML082270296).
23. Stephen E. Hedges, Wolf Creek Nuclear Operating Corporation, WM-09-0001, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: NRC Request for Additional Information Regarding Main Steam and Feedwater Isolation System (MSFIS) Controls Modification," January 16, 2009 (ADAMS Accession No. ML090270824).

24. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-09-0005, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Submittal of Requested Information Regarding Main Steam and Feedwater Isolation System (MSFIS) Controls Modification," January 29, 2009 (ADAMS Accession No. ML090440051).
25. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-09-0008, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Additional Information Regarding Main Steam and Feedwater Isolation System (MSFIS) Controls Modification," February 17, 2009 (ADAMS Accession No. ML090630406).
26. Terry J. Garrett, Wolf Creek Nuclear Operating Corporation, ET-09-0011, letter to U.S. Nuclear Regulatory Commission, "Docket No. 50-482: Additional Information Regarding Main Steam and Feedwater Isolation System (MSFIS) Controls Modification," February 27, 2009 (ADAMS Accession No. ML090750080).
27. CS Innovations, LLC, "MSFIS System Specification Wolf Creek Generating Station," 6101-00002, Revision 0.98, Cover Page through Page 62 of 134, June 9, 2007 (ADAMS Accession No. ML071780282. *Proprietary information. Not publicly available.*).
28. CS Innovations, LLC, "MSFIS System Specification Wolf Creek Generating Station," 6101-00002, Revision 0.98, Page 63 of 134 through End, June 9, 2007 (ADAMS Accession No. ML071780296. *Proprietary information. Not publicly available.*).
29. CS Innovations, LLC, "CS Innovations Report 6002-00026, 'ALS Platform Overview,' Revision 2," January 16, 2009 (ADAMS Accession No. ML090270426).
30. CS Innovations, LLC, "CS Innovations Report 6101-00200, 'MSFIS V&V Report,' Revision 4," January 15, 2009 (ADAMS Accession No. ML090270466. *Proprietary information. Not publicly available.*).
31. CS Innovations, LLC, "CS Innovations Report 6101-00000, 'MSFIS Management Plan,' Revision 0.4," June 14, 2007 (ADAMS Accession No. ML071780233. *Proprietary information. Not publicly available.*).
32. CS Innovations, LLC, "CS Innovations Report 6002-00010, 'ALS Platform Requirements Specification,' Revision 2," January 15, 2009 (ADAMS Accession No. ML090270686. *Proprietary information. Not publicly available.*).
33. CS Innovations, LLC, "CS Innovations Report 6002-00011, 'ALS Platform Specification,' Revision 2," January 14, 2009 (ADAMS Accession No. ML090270687. *Proprietary information. Not publicly available.*).
34. CS Innovations, LLC, "CS Innovations Report 6002-00004, 'ALS EQ Plan,' Revision 2," February 20, 2009 (ADAMS Accession No. ML090750083. *Proprietary information. Not publicly available.*).

35. CS Innovations, LLC, "CS Innovations Report 6002-10101, 'ALS-101 Requirements Specification,' Revision 1," January 15, 2009 (ADAMS Accession No. ML090290653. *Proprietary information. Not publicly available.*).
36. CS Innovations, LLC, "CS Innovations Report 6002-10102, 'ALS-101 Hardware Specification,' Revision 1," January 15, 2009 (ADAMS Accession No. ML090270688. *Proprietary information. Not publicly available.*).
37. CS Innovations, LLC, "CS Innovations Report 6002-30101, 'ALS-301 Requirements Specification,' Revision 2," January 15, 2009 (ADAMS Accession No. ML090270706. *Proprietary information. Not publicly available.*).
38. CS Innovations, LLC, "CS Innovations Report 6002-30102, 'ALS-301 Hardware Specification,' Revision 1," January 15, 2009 (ADAMS Accession No. ML090270707. *Proprietary information. Not publicly available.*).
39. CS Innovations, LLC, "CS Innovations Report 6002-40101, 'ALS-401 Requirements Specification,' Revision 1," January 15, 2009 (ADAMS Accession No. ML090270954. *Proprietary information. Not publicly available.*).
40. CS Innovations, LLC, "CS Innovations Report 6002-40102, 'ALS-401 Hardware Specification,' Revision 1," January 15, 2009 (ADAMS Accession No. ML090270955. *Proprietary information. Not publicly available.*).
41. CS Innovations, LLC, "CS Innovations Report 6002-41101, 'ALS-411 Requirements Specification,' Revision 1," January 15, 2009 (ADAMS Accession No. ML090270956. *Proprietary information. Not publicly available.*).
42. CS Innovations, LLC, "CS Innovations Report 6002-41102, 'ALS-411 Hardware Specification,' Revision 1," January 15, 2009 (ADAMS Accession No. ML090270953. *Proprietary information. Not publicly available.*).
43. CS Innovations, LLC, "CS Innovations Report 6002-20101, 'ALS-201 Requirements Specification,' Revision 1," January 15, 2009 (ADAMS Accession No. ML090270689. *Proprietary information. Not publicly available.*).
44. CS Innovations, LLC, "CS Innovations Report 6002-20102, 'ALS-201 Hardware Specification,' Revision 1," January 15, 2009 (ADAMS Accession No. ML090270705. *Proprietary information. Not publicly available.*).
45. CS Innovations, LLC, "CS Innovations Report 6002-90501, 'ALS-905 Requirements Specification,' Revision 1," January 15, 2009 (ADAMS Accession No. ML090270957. *Proprietary information. Not publicly available.*).
46. CS Innovations, LLC, "CS Innovations Report 6002-90502, 'ALS-905 Hardware Specification,' Revision 0," December 9, 2008 (ADAMS Accession No. ML090270958. *Proprietary information. Not publicly available.*).

47. CS Innovations, LLC, "CS Innovations Report 6002-00003, 'ALS VV Plan,' Revision 1," January 5, 2009 (ADAMS Accession No. ML090270427. *Proprietary information. Not publicly available.*).
48. CS Innovations, LLC, "CS Innovations Procedures 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,'" May 13, 2007 (ADAMS Accession No. ML071780304. *Proprietary information. Not publicly available.*).
49. CS Innovations, LLC, "CS Innovations Procedures 9002-00024, 'Electrical Wiring Design Review,' 9002-00025, 'Board Design Review Procedure,' and 9002-00026, 'FPGA Design Review Procedure,'" June 9, 2007 (ADAMS Accession No. ML071780209. *Proprietary information. Not publicly available.*).
50. Wolf Creek Nuclear Operating Corporation, "Operation Plan," Revision 2, January 14, 2009 (ADAMS Accession No. ML090270823).
51. CS Innovations, LLC, "CS Innovations Procedures 6000-00000, 'ALS Level-I System Specification,' Revision 1.02," June 9, 2007 (ADAMS Accession No. ML071780268. *Proprietary information. Not publicly available.*).
52. CS Innovations, LLC, "CS Innovations Report 6101-00006, 'MSFIS Safety Assessment,' Revision 0.7, June 14, 2007 (ADAMS Accession No. ML071780261. *Proprietary information. Not publicly available.*).
53. Wolf Creek Nuclear Operating Corporation, "Main Steam & Feedwater Isolation System (MSFIS) Controls Replacement Project Plan," August 22, 2007 (ADAMS Accession No. ML072480533).
54. Wolf Creek Nuclear Operating Corporation, "Main Steam & Feedwater Isolation System (MSFIS) Quality Assurance Plan, Revision 0," September 16, 2006 (ADAMS Accession No. ML071160337).
55. CS Innovations, LLC, "CS Innovations, LLC Quality Assurance Manual and Implementing Quality Control Procedures, Revision 1," May 16, 2007 (ADAMS Accession No. ML071780230. *Proprietary information. Not publicly available.*).
56. Nutherm International Inc., "Quality Assurance Manual (QA-N-10179-5), Revision 5," March 8, 1993 (ADAMS Accession No. ML071770482).
57. Wolf Creek Nuclear Operating Corporation, "Installation Plan for the Replacement MSFIS Controls," Revision 1, May 29, 2007 (ADAMS Accession No. ML071770490).
58. Wolf Creek Nuclear Operating Corporation, "Maintenance Plan," Revision 1, January 21, 2008 (ADAMS Accession No. ML080940563).

59. CS Innovations, LLC, "CS Innovations Report 6101-00007, 'MSFIS Instruction, Operating & Maintenance Manual,' Revision 1," March 13, 2008 (ADAMS Accession No. ML080810093. *Proprietary information. Not publicly available.*).
60. CS Innovations, LLC, "CS Innovations Report 9006-00008, 'Return for Material Repair Procedure,' Revision 0," January 16, 2009 (ADAMS Accession No. ML090270962. *Proprietary information. Not publicly available.*).
61. Wolf Creek Nuclear Operating Corporation, Procedure "AP 05F-001, Design Verification," Revision 3, February 6, 2007 (ADAMS Accession No. ML071770461).
62. Wolf Creek Nuclear Operating Corporation, "Configuration Management Plan," Revision 2, February 16, 2008 (ADAMS Accession No. ML080940562).
63. CS Innovations, LLC, "CS Innovations Report 6002-00002, 'ALS Configuration Management Plan,' Revision 2," July 28, 2008 (ADAMS Accession No. ML082270303. *Proprietary information. Not publicly available.*).
64. CS Innovations, LLC, "CS Innovations Report 6002-00002, 'ALS Configuration Management Plan,' Revision 2," July 30, 2008 (ADAMS Accession No. ML082270298).
65. Wolf Creek Nuclear Operating Corporation, Procedure "AP 05-005, 'Design, Implementation and Configuration Control of Modifications,' Revision 11A," July 12, 2006 (ADAMS Accession No. ML071770460).
66. CS Innovations, LLC, "CS Innovations Document 6000-00008, 'ALS Board Test Plan (and Procedures),' Revision 0.8," Page 1 through Page 97, June 9, 2007 (ADAMS Accession No. ML071780199. *Proprietary information. Not publicly available.*).
67. CS Innovations, LLC, "CS Innovations Document 6000-00008, 'ALS Board Test Plan (and Procedures),' Revision 0.8," Page 98 through End, June 9, 2007 (ADAMS Accession No. ML071780204. *Proprietary information. Not publicly available.*).
68. CS Innovations, LLC, "CS Innovations Document 6101-00004, 'MSFIS System Test Plan,' Revision 0.8," June 9, 2007 (ADAMS Accession No. ML071780239. *Proprietary information. Not publicly available.*).
69. CS Innovations, LLC, CS Innovations Documents "ATU-101, 'Design Specification,' Revision 0, ATU-101, 'Design Specification,' Revision 0, and ATS-101, 'Software Specification,' Revision 0.2," June 9, 2007 (ADAMS Accession No. ML071780218. *Proprietary information. Not publicly available.*).
70. Wolf Creek Nuclear Operating Corporation, "ALS Architecture Evaluation," Revision 0, February 25, 2008 (ADAMS Accession No. ML080940569. *Proprietary information. Not publicly available.*).
71. Wolf Creek Nuclear Operating Corporation, "ALS Architecture Evaluation," Revision 0, February 25, 2008 (ADAMS Accession No. ML080940565.).

72. Nutherm Qualification Report "WCN-9715R, for CS Innovations Replacement MSFIS System," Revision 0, February 16, 2007 (ADAMS Accession No. ML071160369.).
73. Nutherm International Report "9715-TR-01R, 'Test, Inspection, and Quality Assurance Activities Report,' Revision 0," April 26, 2008 (ADAMS Accession No. ML081290379. *Proprietary information. Not publicly available.*).
74. CS Innovations, LLC, "CS Innovations Report 6002-00207, 'CSI ESD Test Report,' Revision 0," January 15, 2009 (ADAMS Accession No. ML090270961. *Proprietary information. Not publicly available.*).
75. CS Innovations, LLC, "6002-00031, 'ALS Diversity Analysis, Revision 0," January 13, 2009 (ADAMS Accession No. ML090270428. *Proprietary information. Not publicly available.*).
76. Wolf Creek Nuclear Operating Corporation, "MSFIS D3 Assessment," Revision 2, January 9, 2009 (ADAMS Accession No. ML090270825).
77. B&W Nuclear Technologies, Topical Report, "STAR System Components for Reactor Protection System Digital Upgrades," BAW-10191, September 1994 (ADAMS Legacy Library No. 9605010222).
78. Bruce A. Boger, U.S. Nuclear Regulatory Commission, to James H. Taylor, B&W Nuclear Technologies, "Safety Evaluation for Topical Report BAW-10191P, "STAR System Components for Reactor Protection System Digital Upgrades," August 3, 1995 (ADAMS Legacy Library No. 9508070177).
79. Wolf Creek Nuclear Operating Corporation, "System Reliability Analysis for Advanced Logic System," Revision 1, April 10, 2007 (ML071160381. *Proprietary information. Not publicly available.*).
80. CS Innovations, LLC, "CS Innovations Report 6002-00001, 'ALS Quality Assurance Plan,' Revision 2," July 28, 2008 (ADAMS Accession No. ML082270310. *Proprietary information. Not publicly available.*).
81. CS Innovations, LLC, "CS Innovations Document 6101-0009, 'MSFIS Quality Assurance Plan,' Revision 0.5, June 9, 2007 (ADAMS Accession No. ML071780226. *Proprietary information. Not publicly available.*).
82. CS Innovations, LLC, "6000-00010, 'ALS Design Tools,' Revision 0.95," August 30, 2007 (ADAMS Accession No. ML072480535. *Proprietary information. Not publicly available.*).
83. CS Innovations, LLC, "CS Innovations Document 6101-00005, 'MSFIS Configuration Management Plan,' Revision 0.8," June 9, 2007 (ADAMS Accession No. ML071780224. *Proprietary information. Not publicly available.*).

84. Wolf Creek Nuclear Operating Corporation, "Matrix of IEEE 7-4.3.2 Requirements to MSFIS Controls Design," Revision 0, November 16, 2007 (ADAMS Accession No. ML073241412. *Proprietary information. Not publicly available.*). (Withdrawn by letter dated February 17, 2009).
85. CS Innovations, LLC, "CS Innovations Report 6002-00002, 'ALS Configuration Management Plan,' Revision 1," February 21, 2008 (ADAMS Accession No. ML080940568. *Proprietary information. Not publicly available.*).
86. CS Innovations, LLC, "CS Innovations Report 6002-00026, 'ALS Platform Overview,' Revision 1," July 29, 2008 (ADAMS Accession No. ML082270301).
87. U.S. Nuclear Regulatory Commission, "NUREG-0800, Standard Review Plan (SRP) for the Review of Safety Analysis Reports for Nuclear Power Plants," Revision 5, March 2007 (ADAMS Package Accession No. ML070660036).
88. U.S. Nuclear Regulatory Commission, "SECY-93-087 - Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," Staff Requirements Memorandum, July 21, 1993 (ADAMS Legacy Library Accession No. 9308270107).
89. Lawrence Livermore Nuclear Laboratory, "NUREG/CR-6101, Software Reliability and Safety in Nuclear Reactor Protection Systems," November, 1993 (ADAMS Accession No. ML072750055).
90. Lawrence Livermore Nuclear Laboratory, "NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems," December, 1994 (ADAMS Accession No. ML071790509).
91. SoHaR Incorporated, "NUREG/CR-6463, Revision 1, Review Guidelines for Software Languages for Use in Nuclear Power Plant Safety Systems," October 31, 1997 (ADAMS Accession No. ML071790515).
92. Electric Power Research Institute (EPRI) Topical Report (TR)-102323, Revision 2, "Guidelines for Electromagnetic Interference Testing in Power Plants," November 2000.
93. Electric Power Research Institute (EPRI) Topical Report (TR)-106439, Revision 2, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications."
94. Electric Power Research Institute (EPRI) Topical Report (TR)-107330, Revision 2, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants."
95. Institute of Electrical and Electronics Engineers (IEEE) Standard 279-1971, "Criteria for Protection Systems for Nuclear Power Stations."

96. Institute of Electrical and Electronics Engineers (IEEE) Standard 308-1980, "IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations."
97. Institute of Electrical and Electronics Engineers (IEEE) Standard 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."
98. Institute of Electrical and Electronics Engineers (IEEE) Standard 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems."
99. Institute of Electrical and Electronics Engineers (IEEE) Standard 344-1987, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations."
100. Institute of Electrical and Electronics Engineers (IEEE) Standard 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems."
101. Institute of Electrical and Electronics Engineers (IEEE) Standard 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."
102. Institute of Electrical and Electronics Engineers (IEEE) Standard 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits."
103. Institute of Electrical and Electronics Engineers (IEEE) Standard 420-1982, "IEEE Standard for the Design and Qualification of Class 1E Control Boards, Panels, and Racks Used in Nuclear Power Generating Stations."
104. Institute of Electrical and Electronics Engineers (IEEE) Standard 494-1974, "IEEE Standard Methods for Identification of Documents Related to Class 1E Equipment and Systems for Nuclear Power Generating Stations."
105. Institute of Electrical and Electronics Engineers (IEEE) Standard 497-1981, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations."
106. Institute of Electrical and Electronics Engineers (IEEE) Standard 577-1976, "IEEE Standard Requirements for Reliability Analysis in the Design Operation of Safety Systems for Nuclear Power Generating Facilities."
107. Institute of Electrical and Electronics Engineers (IEEE) Standard 577-2004, "IEEE Standard Requirements for Reliability Analysis in the Design Operation of Safety Systems for Nuclear Facilities."
108. Institute of Electrical and Electronics Engineers (IEEE) Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

109. Institute of Electrical and Electronics Engineers (IEEE) Standard 627-1980, "IEEE Standard for Design Qualification of Safety Systems Equipment Used in Nuclear Power Generating Stations."
110. Institute of Electrical and Electronics Engineers (IEEE) Standard 828-1998, "IEEE Standard for Software Configuration Plans."
111. Institute of Electrical and Electronics Engineers (IEEE) Standard 829-1983, "IEEE Standard for Software Test Documentation."
112. Institute of Electrical and Electronics Engineers (IEEE) Standard 830-1993, "IEEE Recommended Practice for Software Requirements Specifications."
113. Institute of Electrical and Electronics Engineers (IEEE) Standard 1008-1987, "IEEE Standard for Software Unit Testing."
114. Institute of Electrical and Electronics Engineers (IEEE) Standard 1012-1998, "IEEE Standard for Software Verification and Validation."
115. Institute of Electrical and Electronics Engineers (IEEE) Standard 1023-1988, "IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities."
116. American Nuclear Standards Institute/Institute of Electrical and Electronics Engineers (ANSI/IEEE) Standard 1042-1987, "IEEE Guide to Software Configuration Management."
117. Institute of Electrical and Electronics Engineers (IEEE) Standard 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes."
118. Institute of Electrical and Electronics Engineers (IEEE) Standard 1540-2001, "IEEE Standard for Life Cycle Processes – Risk Management."
119. Institute of Electrical and Electronics Engineers (IEEE)/Electronic Industries Alliance (EIA) Standard 12207.0-1996, "IEEE/EIA Standard Industry Implementation of International Standard ISO/IEC 12207: 1995 (ISO/IEC 12207) Standard for Information Technology Software Life Cycle Processes."
120. Institute of Electrical and Electronics Engineers (IEEE) Standard 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."
121. U.S. Nuclear Regulatory Commission, "Periodic Testing of Protection System Actuation Functions," Regulatory Guide 1.22, Revision 0, February 1972 (ADAMS Accession No. ML083300530).

122. U.S. Nuclear Regulatory Commission, "Quality Assurance Program Requirements (Design and Construction)," Regulatory Guide 1.28, Revision 3, August 1985 (ADAMS Accession No. ML003739981).
123. U.S. Nuclear Regulatory Commission, "Bypassed and Inoperable Status Indication for Nuclear Plant Safety Systems," Regulatory Guide 1.47, May 1973 (ADAMS Accession No. ML003740127).
124. U.S. Nuclear Regulatory Commission, "Application of the Single-Failure Criterion to Safety Systems," Regulatory Guide 1.53, Revision 2, November 2003 (ADAMS Accession No. ML033220006).
125. U.S. Nuclear Regulatory Commission, "Manual Initiation of Protective Actions," Regulatory Guide 1.62, October 1973 (ADAMS Accession No. ML003740216).
126. U.S. Nuclear Regulatory Commission, "Criteria for Independence of Electrical Safety Systems," Regulatory Guide 1.75, Revision 3, February 2005 (ADAMS Accession No. ML043630448).
127. U.S. Nuclear Regulatory Commission, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," Regulatory Guide 1.89, Revision 1, June 1984 (ADAMS Accession No. ML031320126).
128. U.S. Nuclear Regulatory Commission, "Instrument Setpoints for Safety-Related Systems," Regulatory Guide 1.105, Revision 2, February 1986 (ADAMS Accession No. ML003740318).
129. U.S. Nuclear Regulatory Commission, "Periodic Testing of Electric Power and Protection System," Regulatory Guide 1.118, Revision 3, April 1995 (ADAMS Accession No. ML03739468).
130. U.S. Nuclear Regulatory Commission, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Regulatory Guide 1.152, Revision 2, January 2006 (ADAMS Accession No. ML053070150).
131. U.S. Nuclear Regulatory Commission, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Regulatory Guide 1.168, Revision 1, February 2004 (ADAMS Accession No. ML040410189).
132. U.S. Nuclear Regulatory Commission, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Regulatory Guide 1.169, September 1997 (ADAMS Accession No. ML003740102).
133. U.S. Nuclear Regulatory Commission, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Regulatory Guide 1.170, September 1997 (ADAMS Accession No. ML003740105).

134. U.S. Nuclear Regulatory Commission, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Regulatory Guide 1.172, September 1997 (ADAMS Accession No. ML003740094).
135. U.S. Nuclear Regulatory Commission, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Regulatory Guide 1.173, September 1997 (ADAMS Accession No. ML003740101).
136. U.S. Nuclear Regulatory Commission, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," Regulatory Guide 1.180, Revision 1, October 2003 (ADAMS Accession No. ML032740277).
137. U.S. Nuclear Regulatory Commission, Regulatory Issue Summary 2006-17, "NRC Staff Position on the Requirements of 10 CFR 50.36, 'Technical Specifications,' Regarding Limiting Safety System Settings During Periodic Testing and Calibration of Instrument Channels," August 24, 2006 (ADAMS Accession No. ML051810077).
138. U.S. Nuclear Regulatory Commission, "Interim Staff Guidance, Digital Instrumentation and Controls, DI&C-ISG-01 Task Working Group #1: Cyber Security," December 31, 2007 (ADAMS Accession No. ML072980159).
139. U.S. Nuclear Regulatory Commission, "Interim Staff Guidance, Digital Instrumentation and Controls, DI&C-ISG-02 Task Working Group #2: Diversity and Defense-in-Depth Issues," September 26, 2007 (ADAMS Accession No. ML072540118).
140. U.S. Nuclear Regulatory Commission, "Interim Staff Guidance, Digital Instrumentation and Controls, DI&C-ISG-04, Task Working Group #4, Highly-Integrated Control Rooms—Communications Issues (HICRc)," September 28, 2007 (ADAMS Accession No. ML072540138).
141. U.S. Nuclear Regulatory Commission, "NRC Presentation, Meeting on May 17, 2007, with Wolf Creek Nuclear Operating Corporation, Main Steam Feedwater Isolation System Upgrade," May 17, 2007 (ADAMS Accession No. ML071370364).
142. John W. Lubinski, U.S. Nuclear Regulatory Commission, letter to Rick A. Muench, Wolf Creek Nuclear Operating Corporation, "Wolf Creek Generating Station - Acceptance Review of Licensee's Application for Main Steam and Feedwater Isolation System Controls Modification (TAC No. MD4839)," May 29, 2007 (ADAMS Accession No. ML071380511).
143. Jack N. Donohew, U.S. Nuclear Regulatory Commission, letter to Rick A. Muench, Wolf Creek Nuclear Operating Corporation, "Wolf Creek Generating Station - Issuance of Amendment Re: Adoption of TSTF-491, Revision 2, Removal of Main Steam and Main Feedwater Valve Isolation Times (TAC No. MD5266)," Amendment No. 174, August 28, 2007 (ADAMS Accession No. ML072060324).

- 144. Jack N. Donohew, U.S. Nuclear Regulatory Commission, letter to Rick A. Muench, Wolf Creek Nuclear Operating Corporation, "Wolf Creek Generating Station - Issuance of Amendment Regarding Changes to Technical Specification Table 3.3.2-1 (TAC No. MD4839)," Amendment No. 175, March 3, 2008 (ADAMS Accession No. ML072970024).
- 145. Jack N. Donohew, U.S. Nuclear Regulatory Commission, letter to Rick A. Muench, Wolf Creek Nuclear Operating Corporation, "Wolf Creek Generating Station - Issuance of Amendment Re: Replacement of Main Steam and Main Feedwater Isolation Valves (TAC No. MD4840)," Amendment No. 176, March 21, 2008 (ADAMS Accession No. ML080650219).
- 146. Jack N. Donohew, U.S. Nuclear Regulatory Commission, letter to Rick A. Muench, Wolf Creek Nuclear Operating Corporation, "Wolf Creek Generating Station - Issuance of Amendment Re: Revision to Technical Specification 3.7.3, "Main Feedwater Isolation Valves," to Add Main Feedwater Regulating Valves (MFRV) and MFRV Bypass Valves (TAC No. MD4840)," Amendment No. 177, April 3, 2008 (ADAMS Accession No. ML080370117).
- 147. E-mail from Steven G. Wideman of Wolf Creek Nuclear Operating Corporation to Balwant K. Singal of NRC, dated March 5, 2009, "MSFIS Controls Implementation of Amendment," (ADAMS Accession No. ML090650056).
- 148. CS Innovations, LLC, "CS Innovations Report 6002-00206, 'NDT Temperature Test Report,' Revision 0," dated January 14, 2009 (ADAMS Accession No. ML090280445).

Principal Contributors: Paul Loeser
Bernard Dittman
Pong Chung

Date: March 31, 2009

March 31, 2009

Mr. Rick A. Muench
President and Chief Executive Officer
Wolf Creek Nuclear Operating Corporation
Post Office Box 411
Burlington, KS 66839

SUBJECT: WOLF CREEK GENERATING STATION - ISSUANCE OF AMENDMENT RE:
MODIFICATION OF THE MAIN STEAM AND FEEDWATER ISOLATION
SYSTEM CONTROLS (TAC NO. MD4839)

Dear Mr. Muench:

The U.S. Nuclear Regulatory Commission has issued the enclosed Amendment No. 181 to Renewed Facility Operating License No. NPF-42 for the Wolf Creek Generating Station. The amendment consists of changes to the licensing basis for the facility, in response to your application dated March 14, 2007, as supplemented by letters dated April 18, May 9, June 15, August 31, September 12 and 20, October 16, November 16, two letters dated December 14, and December 18, 2007; two letters dated January 18, January 31, February 26 and 28, March 14, April 26, May 14, June 19, and July 31, 2008; and January 16 and 29, and February 17 and 27, 2009.

The amendment revises the licensing basis for the Main Steam and Feedwater Isolation System (MSFIS) controls to incorporate field programmable gate array technology. Other related changes cited in your March 14, 2007, application were previously approved in Amendment No. 174, dated August 28, 2007, Amendment No. 175, dated March 3, 2008, Amendment No. 176, dated March 21, 2008, and Amendment No. 177, dated April 3, 2008.

A copy of our related Safety Evaluation is enclosed. The Notice of Issuance will be included in the Commission's next biweekly *Federal Register* notice.

Sincerely,
/RA/

Balwant K. Singal, Senior Project Manager
Plant Licensing Branch IV
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-482

Enclosures:

1. Amendment No. 181 to NPF-42
2. Safety Evaluation

cc w/encls: Distribution via Listserv

DISTRIBUTION:

PUBLIC

LPLIV r/f

RidsAcrsAcnw_MailCTR Resource

RidsNrrDirsltsb Resource

RidsNrrDorlDpr Resource

RidsNrrDorlLpl4 Resource

RidsNrrPMWolfCreek Resource

RidsNrrLAJBurkhardt Resource

RidsOgcRp Resource

RidsRgn4MailCenter Resource

PLoeser, NRR/DE/EICB

PChung, NRR/DE/EICB

BDittman, NRR/DE/EICB

ADAMS Accession No. ML090610317

*See previous concurrence

OFFICE	NRR/LPL4/PM	NRR/LPL4/LA	DIRS/ITSB/BC	DE/EICB/BC	OGC – NLO	NRR/LPL4/BC	NRR/LPLR/PM
NAME	BSingal	JBurkhardt	Not Required	WKemper *	DRoth *	MMarkley	BSingal
DATE	3/9/09	3/6/09	--	3/24/09	3/24/09	3/31/09	3/31/09

OFFICIAL RECORD COPY