Enclosure XV to ET 08-0014

WCNOC MSFIS D3 Assessment, Rev. 1, Non-Proprietary

ADVANCED LOGIC SYSTEM

(ALS)

CLASS 1E CONTROLS

MSFIS D3 ASSESSMENT

REVISION 1

PROJECT MANAGER - GREGG CLARKSON
MANAGEMENT SPONSOR - PATRICK GUEVEL
EXECUTIVE SPONSOR - TERRY GARRETT

Wolf Creek Nuclear Operating Corporation
PO Box 411
1550 Oxen Lane, NE
Burlington, KS 66839

Revision Control

Rev #	Approval	Approval Date	Description of Change(s)
0	GWC	6/14/2007	**Initial Revision**
1	GWC	2/23/2008	**Revised to discuss [** **]**^{c,d} **Removed discussion regarding existing system (CCC). Removed discussion regarding quality of design process.**

Table of Content

1 Introduction

WCNOC plans to replace the existing Main Steam and Feedwater Isolation System (MSFIS) controls with a new control system. The new control system is based on the Advanced Logic System (ALS) from CS Innovations. The installation of the ALS MSFIS is scheduled for Refueling Outage 17, fall 2009. The MSFIS Controls Replacement Project is one aspect of an overall project to replace the existing Main Steam Isolation Valve (MSIV) bodies and actuators as well as the Main Feedwater Isolation Valve (MFIV) bodies and actuators. The existing MSFIS controls do not support the operation of the replacement MSIV and MFIV actuators. A modified or replacement controls system is required to operate the new valve actuators. In addition to the lack of capability, the existing MSFIS controls are based on obsolete technology and that has become less reliable as the system ages. A recent plant trip (August 2003) was due to a failed circuit card in the existing MSFIS control. Several single points of failure exist in the existing MSFIS controls.

1.1 Purpose

The purpose of this Diversity and Defense-in-Depth Assessment is to present the ALS as implemented for the MSFIS replacement at WCGS. The intent of this assessment is to describe the design attributes of the ALS which are sufficient to eliminate consideration of Common Cause Failure (CCF).

Section 2 provides a description of the MSFIS and its design basis at WCGS. Section 3 provides an overview of the ALS architecture. Section 4 discusses the key design attributes of the ALS which are sufficient to eliminate consideration of Common Cause Failure (CCF). Section 5 describes key analyses employed to ensure integrity and robustness of the ALS design. Section 6 provides a conclusion for the consideration of CCF.

1.2 References

1.2.1 USNRC, DI&C-ISG-02, "Task Working Group #2: Diversity and Defense-in-Depth Issues"

1.2.2 [ ]^{c,d}

1.2.3 [ ]^{c,d}

1.2.4 [ ]^{c,d}

1.2.5 [ ]^{c,d}

1.2.6 CS Innovations, 6101-00002, "MSFIS System Specification"

1.2.7 CS Innovations, 6101-00004, "MSFIS System Test Plan"

1.2.8 CS Innovations, 6101-00006, "MSFIS Safety Assessment"

1.2.9 TPS-9064, "Final Acceptance Testing for Main Steam and Feedwater Isolation System (MSFIS) Rack"

1.2.10 WCNOC, WCGS Updated Safety Analysis Report (USAR), Section 7

1.2.11 WCNOC, "System Reliability Analysis for Advanced Logic System"

1.2.12 MIL-HDBK-217B, "Reliability Stress and Failure Rate Data for Electromagnetic Equipment"

2 MSFIS Description and Design Basis

2.1 MSFIS Description

The MSFIS is a second tier Engineered Safety Features Actuation System, as can be seen in Figure 2-1. The MSFIS is a two channel valve control system. The MSFIS does not make the determination as to whether the MSIVs and/or MFIVs are to be closed or open. The MSFIS receives either an automatic signal or a manual signal to close the valves. The signals that initiate automatic closure of the MSIV and MFIV valves are generated in the ESFAS. This ESFAS functionality is contained in the SSPS which can also be seen in Figure 2- 1. The MSFIS is a sub-system of the ESFAS. The MSFIS is essentially the valve operator for the MSIVs and MFIVs. The MSFIS will cause the MSIVs and MFIVs to close automatically upon receipt of an automatic close signal from the SSPS. The automatic close signal for the MSIVs is the Steam Line Isolation Signal (SLIS) and for the MFIVs is the Feedwater Isolation Signal (FWIS). The SSPS provides the SLIS and FWIS by means of slaves relay contacts, which are input to the MSFIS. A manual close function for the valves is also provided by a hand-switch on the MCB. In addition to the manual and automatic closure modes of operation, manual valve control is provided by separate hand-switches on the MCB which allow for the opening and closing of each valve independently. The MSFIS is implemented with a two channel separation scheme. Two redundant, independent, and equivalent MSFIS subsystems are located in separate cabinets:

- MSFIS Channel I (Separation Group 1) located in MSFIS Cabinet **SA075A** – also referred to as train A.
- MSFIS Channel IV (Separation Group 4) located in MSFIS Cabinet **SA075B** – also referred to as train B.

Within a particular separation train the MSFIS functionally is divided into 2 independent functions:

- **MSIV control** - The MSIV control receives the automatic actuation SLIS to close the MSIVs. Main Steam line isolation minimizes the uncontrolled cool down of the Reactor Coolant System (RCS) that would result from a main steam line rupture. Input signals pass from the detectors through the SSPS to the MSFIS cabinet where the output signal is generated to close the valves.
- **MFIV control** - The MFIV control receives the automatic actuation FWIS to close the MFIVs. The feedwater isolation minimizes the potential for excessive post-trip cool down of the RCS due to overfilling the steam generators. It also prevents moisture carryover caused by high steam generator levels, and isolates normal feedwater in the event of a High Energy Line Break inside containment. Input signals pass from the detectors through the SSPS to the MSFIS cabinet where the output signal is generated to close the valves.

The MSFIS provides the control logic for a total of 8 valves:

- 4 Main Steam Isolation Valves (MSIV#1-4): **AB-HV-14, AB-HV-17, AB-HV-20, AB-HV-11**.
- 4 Main Feedwater Isolation Valves (MFIV#1-4): **AE-FV-39, AE-FV-40, AE-FV-41, AE-FV-42**.

The MSFIS is provided with operator inputs from MCB switches, ESFAS actuation signals from SSPS, and valve position switches. The MSFIS provides outputs to the valve solenoids, a bypass to the SSPS to permit ESFAS testing, and status panel indications to the MCB. Figure 2-2 provides an overview of the inputs and outputs for the MSFIS.

2.2 MSFIS Design Bases

The WCGS USAR describes two design basis for the MSFIS: 1) the system shall isolate the Main Steam and Feedwater when required. 2) No single failure can prevent any valve from performing its required design basis safety function, which is to isolate the Main Steam or Feedwater when required. As stated above the MSFIS does not make the determination as to when the MSIVs or MFIVs are to close, that determination is made by the SSPS.

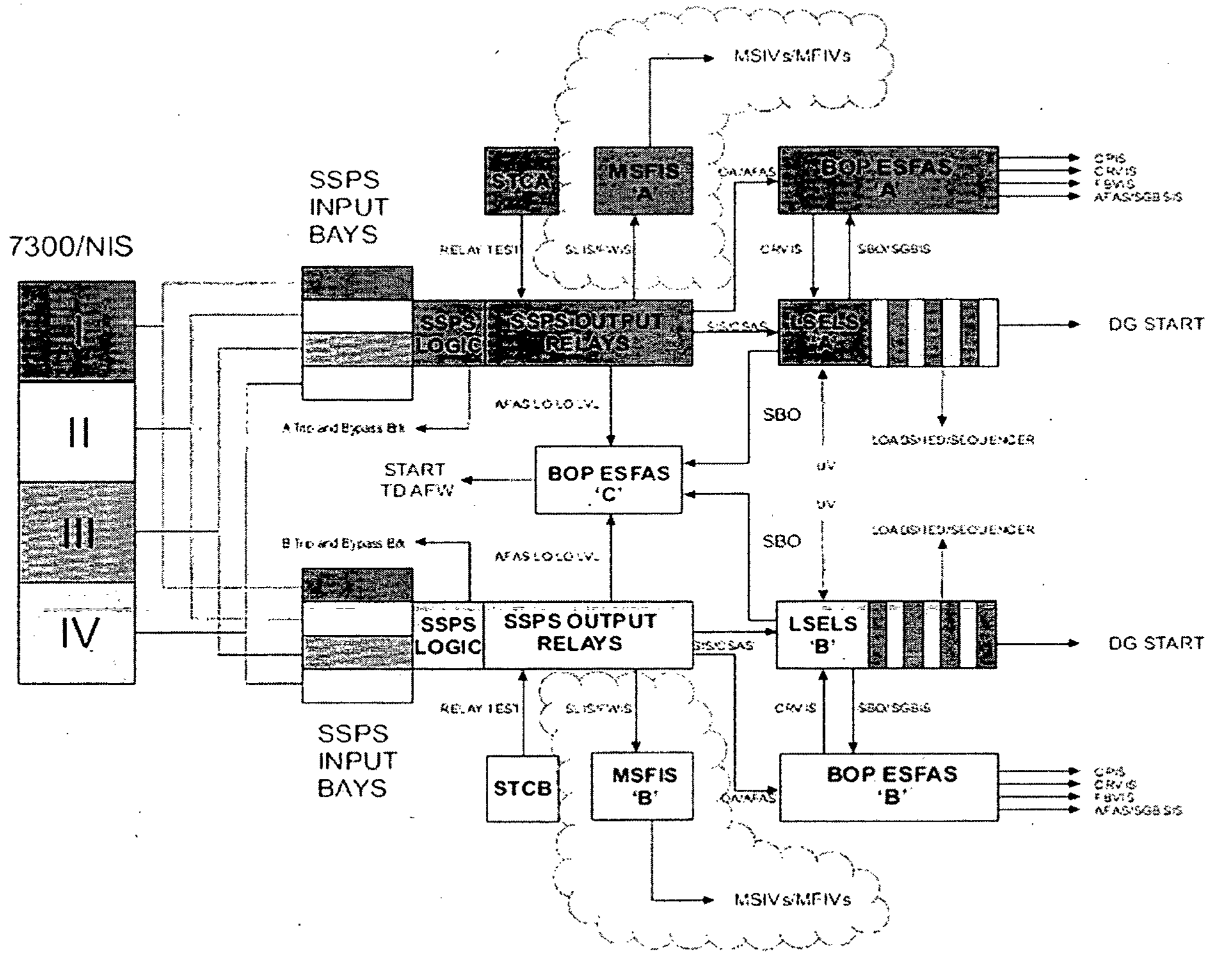

Figure 2-1: WCGS Safety Related Instrumentation and Controls Architecture w/ MSFIS Highlighted

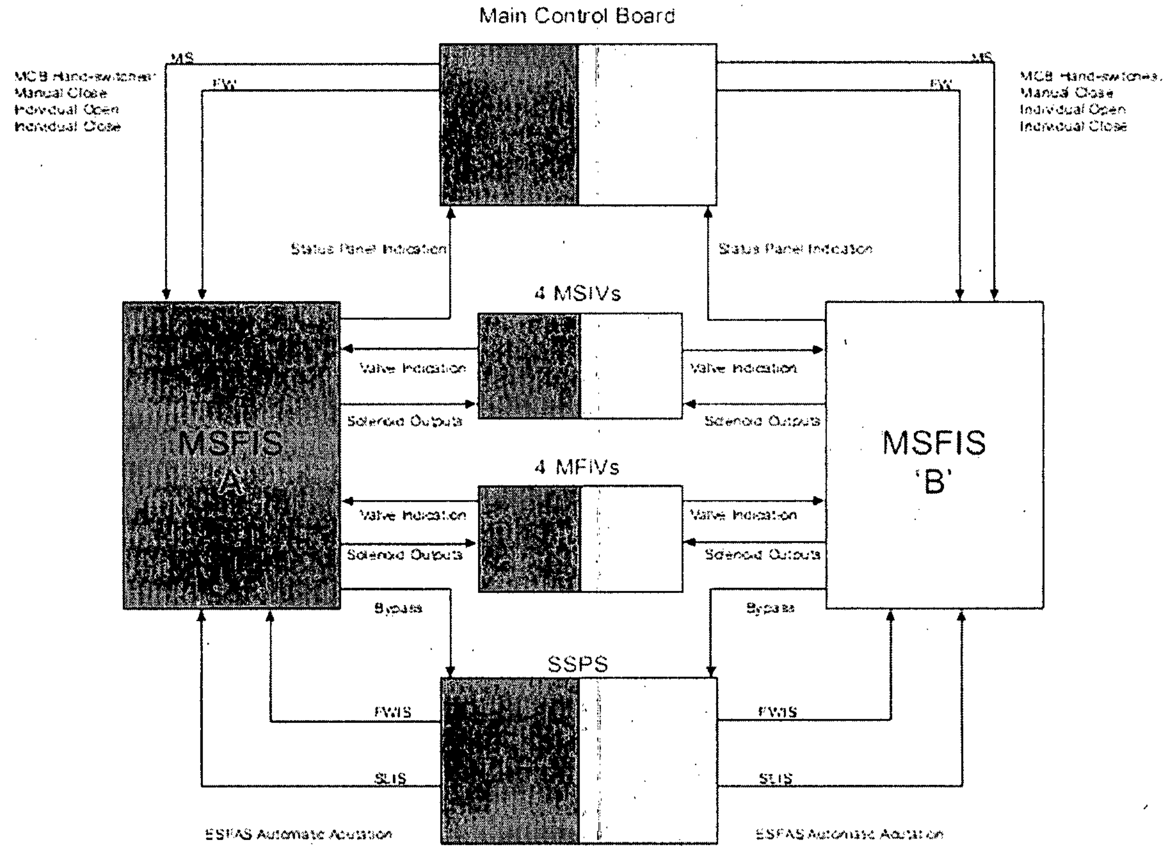

Figure 2-2: MSFIS Input and Output Overview

3 Advanced Logic System (ALS) Overview

c,d

c,d

c,d

c,d

c,d

c,d

c,d

c,d

c,d

4 ALS Design Attributes

c,d

c,d

c,d

c,d

c,d

5 ALS Design Analyses

This section describes the System Reliability Analysis (SRA), Failure Modes and Effects Analysis (FMEA), as well as the [ ]c,d performed on the ALS as implemented for MSFIS.

5.1 System Reliability Analysis (SRA)

The purpose of a SRA is to identify weak spots or imbalances within a design as presented in design documents and to assess the relative importance of all identified failures. The SRA for the ALS MSFIS implementation provides both a qualitative and quantitative analysis of the equipment reliability and availability.

Largely due to the simplistic nature as well as the inherent aspects of the ALS architecture the system achieves a very high calculated Mean Time Between Failure (MTBF) of ~10 years. The calculated MTBF is based on MIL-HDBK-217 prediction data and the MIL-HDBK-217 FN2 calculation model. Details of the SRA can be found in the WCNOC document "System Reliability Analysis for Advanced Logic System".

5.2 Failure Modes and Effects Analysis (FMEA)

An FMEA is a systematic method of identifying and preventing errors before they occur FMEAs are focused on preventing defects, enhancing safety, and increasing overall system functionality. FMEAs are conducted in the design and/or development stage to help ensure the overall correctness of the design.

The ALS MSFIS has been subjected to both a system level FMEA as well as a component level FMEA. These detailed FMEAs were performed during the design stage of the overall system development.

A system level FMEA was performed by both CS Innovations as well as WCNOC. For details of the CS Innovations FMEA refer to [ ] c,d For details of the WCNOC system level FMEA refer to WCNOC document "System Reliability Analysis for Advanced Logic System".

As stated above there was a component level FMEA performed on the complete ALS. This component level FMEA can be found within the CS Innovations individual board hardware specification,[ ] c,d

5.3 [ ] c,d

c,d

[

]

6 Conclusion

The ALS architecture implements key design attributes (see list below) which are sufficient to eliminate the consideration of Common Cause Failure (CCF). This conclusion is based on the guidance provided in U.S. NRC document DI&C-ISG-02 "Task Working Group #2: Diversity and Defense-in-Depth Issues" Revision 1, dated September 26th, 2007.

DI&C-ISG-02 states in section 5 "There are two design attributes that are sufficient to eliminate consideration of CCF:" staff position 2 states "Testability-A system is sufficiently simple such that every possible combination of inputs, internal and external states, and every signal path can be tested; that is, the system is fully tested and found to produce only correct responses."

c,d

The ALS was subjected to multiple analyses during the design and development of the system. Results of these analyses were utilized to ensure the integrity and robustness of the design was sufficient for implementation of a safety related function. These analyses are briefly discussed in section 5. Further details of the analysis can be found in the individual reference documents.