

Enclosure II to WM 09-0001

**WCNOC MSFIS D3 Assessment, Rev. 2,
Non-proprietary**

**ADVANCED LOGIC SYSTEM
(ALS)
CLASS 1E CONTROLS**



MSFIS D3 ASSESSMENT

REVISION 2

**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 discrete safety path(s), full testability of safety path(s), and failure detection of all faults with immediate alert of the fault. Removed discussion regarding existing system (CCC). Removed discussion regarding quality of design process.
2	GWC	1/9/2009	Modified complete document based on built-in diversity approach by CS Innovations within the ALS platform.

Table of Content

REVISION 2..... 1

1 Introduction 4

1.1 Purpose..... 4

1.2 References..... 4

 1.2.1 USNRC, DI&C-ISG-02, “Task Working Group #2: Diversity and Defense-in-Depth Issues” 4

 1.2.2 CS Innovations, 6101-00002, “MSFIS System Specification” 4

 1.2.3 CS Innovations, 6002-00031, “ALS Diversity Analysis” 4

 1.2.4 WCGS, Updated Safety Analysis Report (USAR), Section 15..... 4

2 MSFIS Description and Design Basis..... 5

2.1 MSFIS Description 5

2.2 MSFIS Design Bases 6

3 Transients and Accidents Associated with MSFIS Controls..... 10

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 discuss the internal diversity attributes of the ALS platform and how they apply to the transient and accidents conditions which assume either a mainsteam isolation valves or a feedwater isolation valves as the ESF equipment required for the ESF function.

1.2 References

- 1.2.1** USNRC, DI&C-ISG-02, "Task Working Group #2: Diversity and Defense-in-Depth Issues"
- 1.2.2** CS Innovations, 6101-00002, "MSFIS System Specification"
- 1.2.3** CS Innovations, 6002-00031, "ALS Diversity Analysis"
- 1.2.4** WCGS, Updated Safety Analysis Report (USAR), Section 15

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 Solid State Protection System (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 slave 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**
- MSFIS Channel IV (Separation Group 4) located in MSFIS Cabinet **SA075B**

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. Figure 2-3 provides an overview of the valve logic finite state machine.

2.2 MSFIS Design Bases

The WCGS USAR Section 7.3.7 describes two design bases 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.

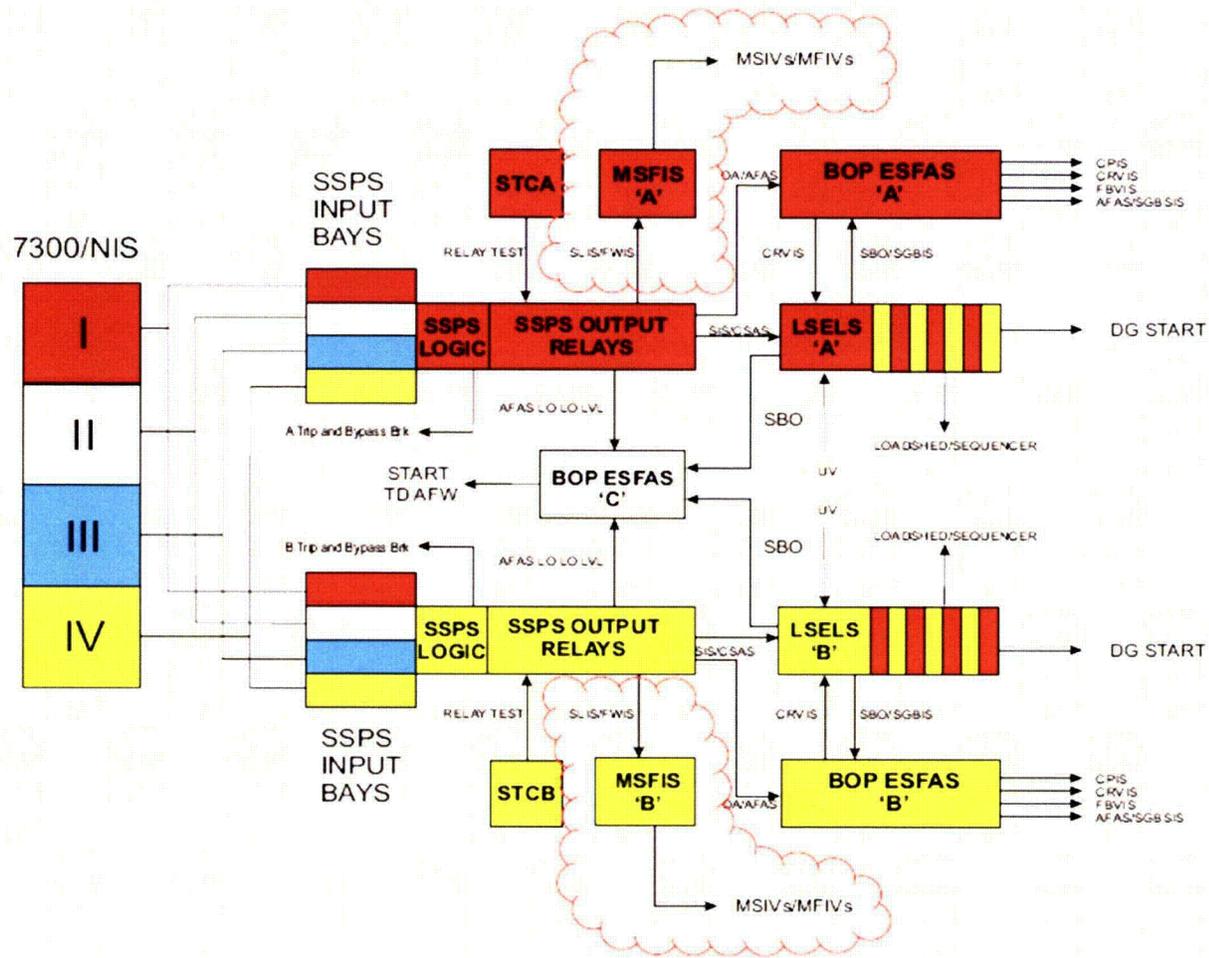


Figure 2-1: WCGS Safety Related Instrumentation and Controls Architecture w/ MSFIS Highlighted

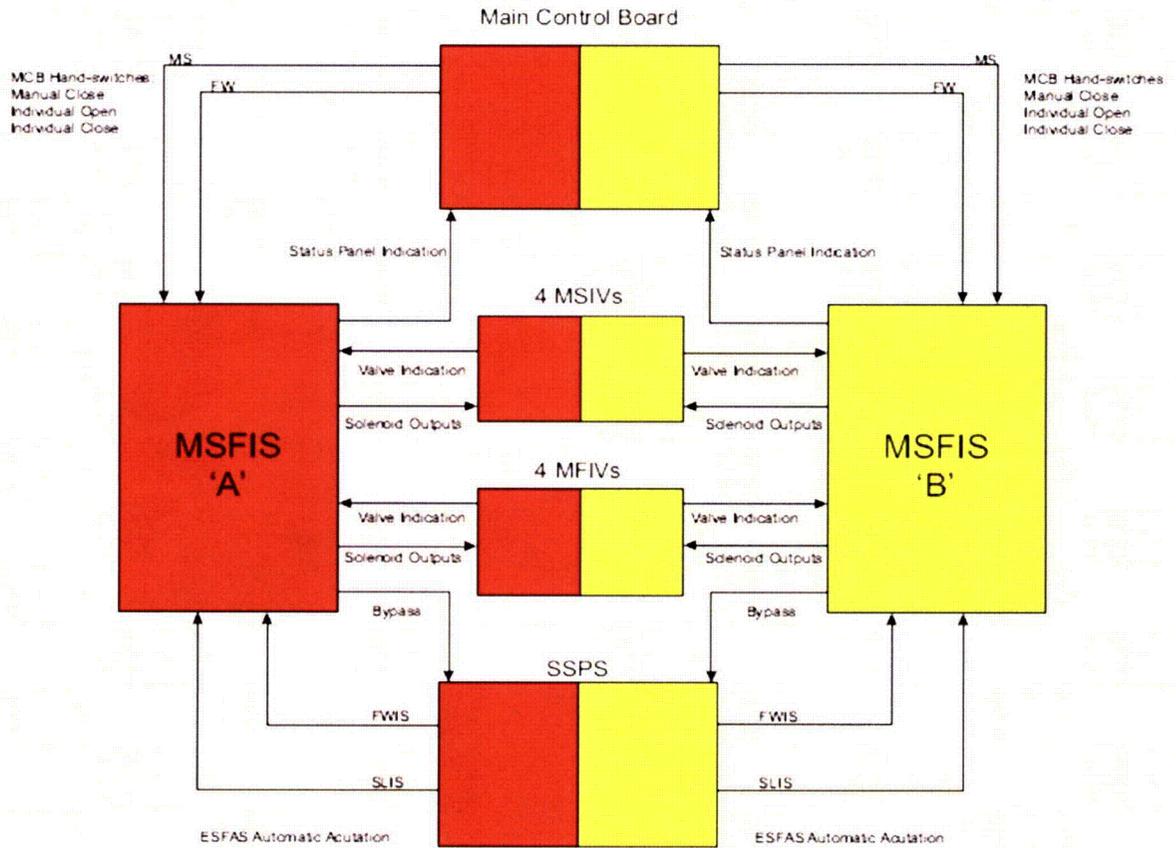


Figure 2-2: MSFIS Input and Output Overview

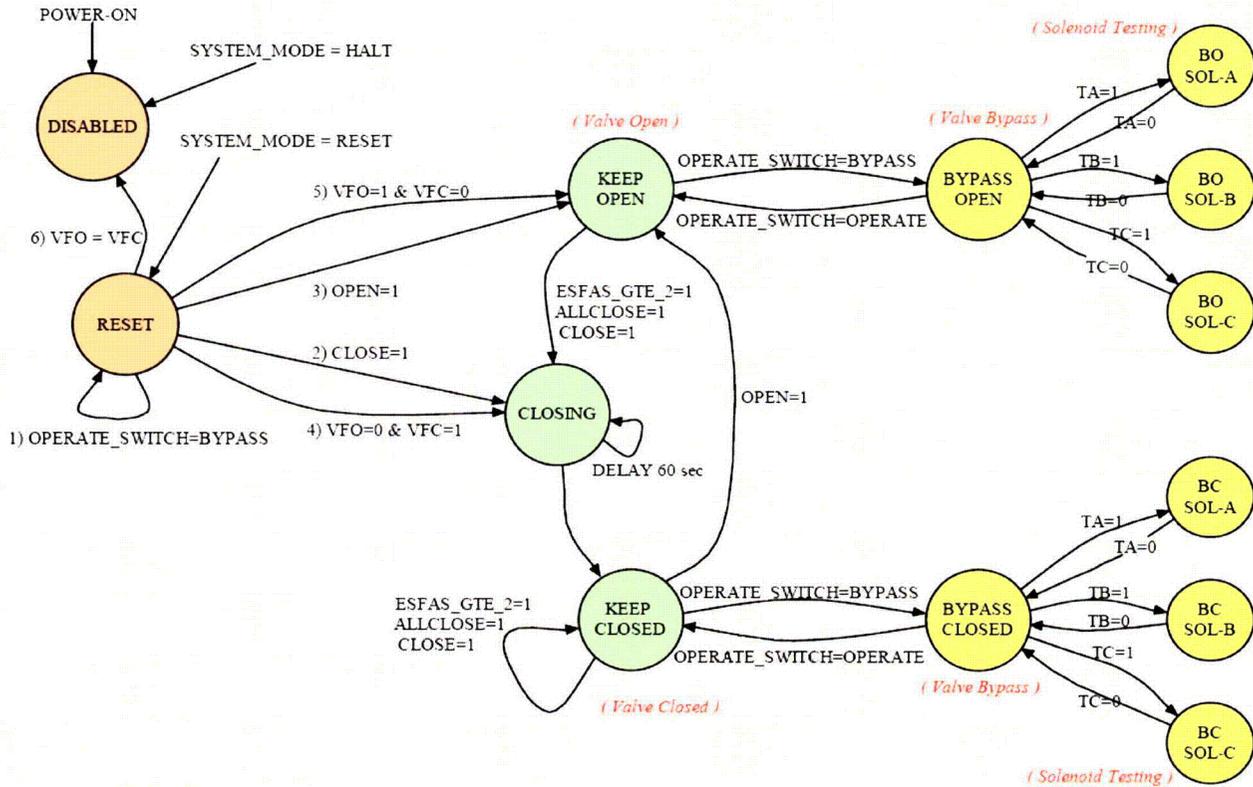


Figure 2-3: Valve Logic Finite State Machine

3 Transients and Accidents Associated with MSFIS Controls

The transients and accidents which assume a MSIV or a MFIV as the “Other Equipment” required for the ESF Function to mitigate the incident are listed in the Table 3-1 below. The information in Table 3-1 was extracted from WCGS USAR Table 15.0-6. The transients and accidents were evaluated and the conclusion was reached that as the MSFIS Controls continue to provide both automatic actuation and manual actuation of the MSIV and MFIV the current licensing-basis USAR Safety Analyses continues to be met.

The ALS platform provides internal diversity which is described in detail in the CS Innovations document number 6002-00031, ALS Diversity Analysis. This ALS Diversity Analysis discusses the inherent diversity within each of the ALS boards. Each FPGA on each board contains two sets of diverse hardware logic, called cores. This was achieved by changing the logic implementation strategy used during the synthesis process. Prior to the synthesis process the hardware is formally described in HDL. The HDL description is a formal representation of the written specification from the design process. After the HDL description is developed, the synthesis of that HDL is performed using one method of hierarchical structure, Finite State Machine (FSM) encoding, and state decoding for one logic core, and a second method of hierarchical structure, FSM encoding, and state decoding for the other logic core. The two diverse logic cores are tested on two diverse test benches using two different simulation tools and two diverse sets of test vectors to determine that each core will adequately perform the required safety function. The diverse test benches and test vectors were developed by different personnel and are verified to be diverse by the CS Innovations V&V group.

The two diverse logic cores then undergo the place and route process and are tested again to determine the proper operation of the safety application.

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

Interim Staff Guidance, revision 1, from NRC Task Working Group #2, “Diversity and Defense-in-Depth Issues”, issue 5, “Common Cause Failure Applicability,” staff position 1 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. WCNOG has concluded 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 ALS platform design meets the intent of the interim staff guidance. WCNOG’s conclusion is based on the review of the CS Innovations detailed methodology used to design and verify the built-in diversity within the ALS.

Incident	Reactor Trip Functions	ESF Actuation Functions	Other Equipment
Feedwater system malfunctions that result in an increase in feedwater flow	Source range high flux, intermediate range high flux, power range high flux, low-low steam generator level, manual overpower delta T, over-temperature delta T, turbine trip	High-high SG level produced feedwater isolation and turbine trip	Feedwater isolation valves
Inadvertent opening of a steam generator atmospheric relief or safety valve	Manual, SIS, power range high flux, overpower delta T	Low pressurizer pressure, low compensated steam line pressure high negative steam pressure rate	Feedwater isolation valves, steam line isolation valves
Steam system piping failure	Power range high flux, pressure, manual, SIS, overpower delta T	Low pressurizer pressure, low compensated steam line pressure, hi-1 containment pressure, hi-2 containment pressure, high negative steam pressure rate, SIS, high-high SG level, low-low SG level, manual	Feedwater isolation valves, steam line isolation valves
Feedwater system pipe break	Low-low SG level, high pressurizer pressure, SIS, manual, overtemperature delta T	Hi-1 containment pressure, low-low SG level, low compensated steam line pressure SIS, loss of offsite power, manual	Steam line isolation valves, feedline isolation, pressurizer safety valves, steam generator safety valves
Steam generator tube rupture	Low pressurizer pressure, SIS, manual, overtemperature delta T	Low pressurizer pressure manual	Essential service water system, component cooling water system, steam generator safety and/or atmospheric relief valves, steam line isolation valves

Table 3-1: Table of Transients and Accidents Assuming Steam Line and Feedwater Isolation