US-APWR

Function Assignment Analysis for Safety Logic System

Non Proprietary Version

October 2009

© 2009 Mitsubishi Heavy Industries, Ltd.
All Rights Reserved

Revision History

Revision		Page	Description
0	October 2009	All	Original issued

© 2009
MITSUBISHI HEAVY INDUSTRIES, LTD.
All Rights Reserved

This document has been prepared by Mitsubishi Heavy Industries, Ltd. ("MHI") in connection with the U.S. Nuclear Regulatory Commission ("NRC") licensing review of MHI's US-APWR nuclear power plant design. None of the information in this document, may be disclosed, used or copied without written permission of MHI, other than by the NRC and its contractors in support of the licensing review of the US-APWR.

This document contains technological information and intellectual property relating to the US-APWR and it is delivered to the NRC on the express condition that it not be disclosed, copied or reproduced in whole or in part, or used for the benefit of anyone other than MHI without the express written permission of MHI, except as set forth in the previous paragraph.

This document is protected by the laws of Japan, U.S. copyright law, international treaties and conventions, and the applicable laws of any country where it is being used.

Mitsubishi Heavy Industries, Ltd.
16-5, Konan 2-chome, Minato-ku
Tokyo 108-8215 Japan

Abstract

This technical report is to justify the assignment of component control functions to each Safety Logic System (SLS) controller of the US-APWR, through a failure modes and effects analysis. SLS provides safety component controls in safety instrumentation and control (I&C) system in the US-APWR.

In the SLS, multiple component control functions are grouped within each controller. This analysis provided in this document ensures that each component control function is appropriately assigned to each controller so that spurious state changes of multiple components that may result from credible single failures cannot cause a plant transient, that is not bounded by the plant's safety analysis. Where concurrent spurious actuation of multiple components is determined to be unacceptable, these components are "separated" into different SLS controllers. In addition, this analysis identifies component control functions whose single spurious state change could lead to a plant trip. For these cases, the control function is "duplicated" using a 2-out-of-2 configuration, so that these single spurious state changes are precluded. The analysis in this document identifies the control functions that must be "duplicated" to preclude failures that can lead to spurious plant trip, and the control functions that must be "separated" to preclude failures that can lead to unanalyzed plant transients.

Table of Contents

List of Tables

List of Figures

List of Acronyms

APWR	advanced pressurized water reactor
AOO	anticipated operational occurrence
CCW	component cooling water
CCWS	component cooling water system
CPU	central processing unit
CSS	containment isolation system
CVCS	chemical and volume control system
DCD	Design Control Document
ECCS	emergency core cooling system
EFW	emergency feedwater
EFWS	emergency feedwater system
ESF	engineered safety feature
ESFAS	engineered safety feature actuation system
ESWS	essential service water system
FWS	feedwater system
FMEA	failure mode and effect analysis
HVAC	heating, ventilation, and air conditioning
IAS	instrument air system
I&C	instrumentation and control
I/O	input/output
MHI	Mitsubishi Heavy Industries, Ltd.
MSS	main steam supply system
NRC	U.S. Nuclear Regulatory Commission
PIF	power interface
PSMS	protection and safety monitoring system
PSS	process and post-accident sampling system
RCS	reactor coolant system
RCP	reactor coolant pump
RHRS	residual heat removal system
RPS	reactor protection system
SG	steam generator
SGBDS	steam generator blow down system
SIS	safety injection system
SLS	safety logic system
TT	turbine trip

1.0 INTRODUCTION

1.1 Purpose

This report describes the Failure Mode and Effect Analysis (FMEA) of SLS to justify the functional assignment of multiple plant components to each SLS controller.

1.2 Scope

The scope of this document is to ensure that there is no transient that is not bounded by the safety analysis in DCD Ch. 15 due to spurious state change of multiple components caused by a failure of a single SLS controller. Spurious state change means that a component that is normally energized becomes de-energized, or a component that is normally de-energized is erroneously energized to its alternate position. In performing this FMEA, the assignment to the SLS controller and duplication of SLS controllers are also considered. Components whose spurious state change can directly affect the critical safety functions considered in the safety analysis are considered in this duplication.

2.0 SLS Control Configuration

SLS provides safety component control in the safety I&C system, protection and safety monitoring system (PSMS), of the US-APWR. I&C overall architecture is shown in Figure 7.1-1 in DCD Ch.7. SLS in Train A and D have 3 controllers and SLS Train B and C have 2 controllers. Each controller has two parallel redundant Central Processing Unit (CPU)s and components are actuated through Power Interface (PIF) modules. The parallel CPUs are configured so that either CPU can position the component to its safe position as required by DCD Chapter 15 safety analysis. It is noted that the parallel CPU configuration is credited in this analysis to preclude spurious state change, since a failure of either CPU can cause spurious state changes of the components controlled by that CPU.

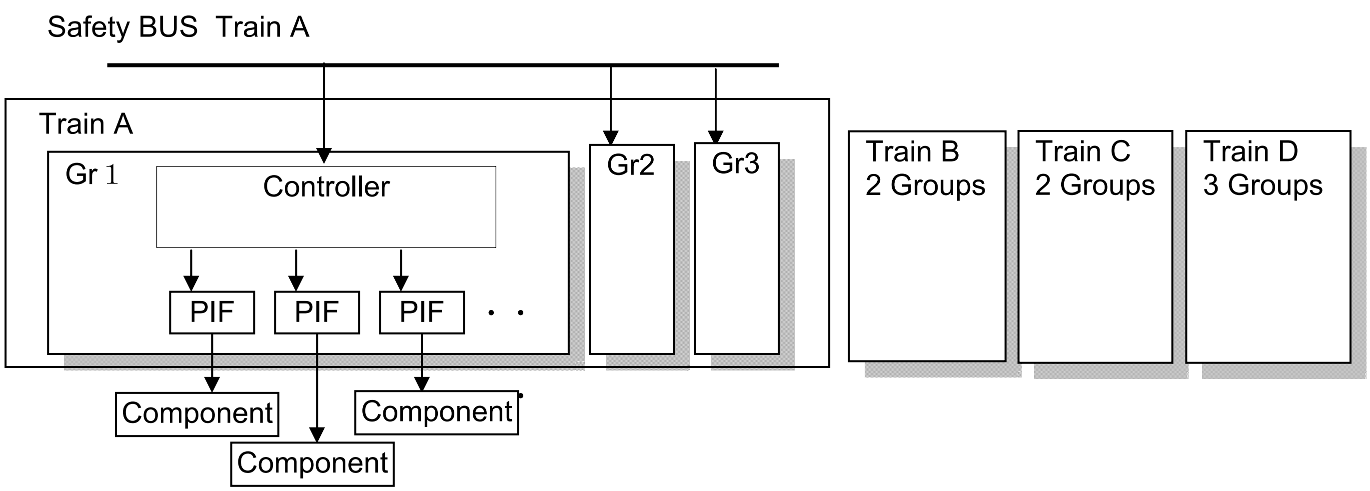

Figure 2.0-1 SLS Configuration

3.0 SLS Component Assignment

3.1 Basic Principle

Figure 3.1-1 Logic Duplication

3.2 Consideration

3.2.1 Scope of Controller Duplication

Table 3.2-1 Component Consideration for Duplication (1/2)

Table 3.2-1 Component Consideration for Duplication (2/2)

3.3 Scope of Controller Assignment

3.4 Result

Table 3.4-1 Component Assignment for Safety Train and Controller Group

Table 3.4-2 Controller Duplication Components

4.0 FMEA

4.1 Condition for the FMEA

4.2 Result and Summary

Table 4.1-1 FMEA for Gr.1 controller, SLS Train A (1/8)

Table 4.1-1 FMEA for Gr.1 controller, SLS Train A (2/8)

Table 4.1-1 FMEA for Gr.1 controller, SLS Train A (3/8)

Table 4.1-1 FMEA for Gr.1 controller, SLS Train A (4/8)

Table 4.1-1 FMEA for Gr.1 controller, SLS Train A (5/8)

Table 4.1-1 FMEA for Gr.1 controller, SLS Train A (6/8)

Table 4.1-1 FMEA for Gr.1 controller, SLS Train A (7/8)

Table 4.1-1 FMEA for Gr.1 controller, SLS Train A (8/8)

Table 4.1-2 FMEA for Gr.2 controller, SLS Train A (1/8)

Table 4.1-2 FMEA for Gr.2 controller, SLS Train A (2/8)

Table 4.1-2 FMEA for Gr.2 controller, SLS Train A (3/8)

Table 4.1-2 FMEA for Gr.2 controller, SLS Train A (4/8)

Table 4.1-2 FMEA for Gr.2 controller, SLS Train A (5/8)

Table 4.1-2 FMEA for Gr.2 controller, SLS Train A (6/8)

Table 4.1-2 FMEA for Gr.2 controller, SLS Train A (7/8)

Table 4.1-2 FMEA for Gr.2 controller, SLS Train A (8/8)

Table 4.1-3 FMEA for Gr.3 controller, SLS Train A (1/8)

Table 4.1-3 FMEA for Gr.3 controller, SLS Train A (2/8)

Table 4.1-3 FMEA for Gr.3 controller, SLS Train A (3/8)

Table 4.1-3 FMEA for Gr.3 controller, SLS Train A (4/8)

Table 4.1-3 FMEA for Gr.3 controller, SLS Train A (5/8)

Table 4.1-3 FMEA for Gr.3 controller, SLS Train A (6/8)

Table 4.1-3 FMEA for Gr.3 controller, SLS Train A (7/8)

Table 4.1-3 FMEA for Gr.3 controller, SLS Train A (8/8)

Table 4.1-4 FMEA for Gr.1 controller, SLS Train B (1/7)

Table 4.1-4 FMEA for Gr.1 controller, SLS Train B (2/7)

Table 4.1-4 FMEA for Gr.1 controller, SLS Train B (3/7)

Table 4.1-4 FMEA for Gr.1 controller, SLS Train B (4/7)

Table 4.1-4 FMEA for Gr.1 controller, SLS Train B (5/7)

Table 4.1-4 FMEA for Gr.1 controller, SLS Train B (6/7)

Table 4.1-4 FMEA for Gr.1 controller, SLS Train B (7/7)

Table 4.1-5 FMEA for Gr.2 controller, SLS Train B (1/8)

Table 4.1-5 FMEA for Gr.2 controller, SLS Train B (2/8)

Table 4.1-5 FMEA for Gr.2 controller, SLS Train B (3/8)

Table 4.1-5 FMEA for Gr.2 controller, SLS Train B (4/8)

Table 4.1-5 FMEA for Gr.2 controller, SLS Train B (5/8)

Table 4.1-5 FMEA for Gr.2 controller, SLS Train B (6/8)

Table 4.1-5 FMEA for Gr.2 controller, SLS Train B (7/8)

Table 4.1-5 FMEA for Gr.2 controller, SLS Train B (8/8)

Table 4.1-6 FMEA for Gr.1 controller, SLS Train C (1/7)

Table 4.1-6 FMEA for Gr.1 controller, SLS Train C (2/7)

Table 4.1-6 FMEA for Gr.1 controller, SLS Train C (3/7)

Table 4.1-6 FMEA for Gr.1 controller, SLS Train C (4/7)

Table 4.1-6 FMEA for Gr.1 controller, SLS Train C (5/7)

Table 4.1-6 FMEA for Gr.1 controller, SLS Train C (6/7)

Table 4.1-6 FMEA for Gr.1 controller, SLS Train C (7/7)

Table 4.1-7 FMEA for Gr.2 controller, SLS Train C (1/8)

Table 4.1-7 FMEA for Gr.2 controller, SLS Train C (2/8)

Table 4.1-7 FMEA for Gr.2 controller, SLS Train C (3/8)

Table 4.1-7 FMEA for Gr.2 controller, SLS Train C (4/8)

Table 4.1-7 FMEA for Gr.2 controller, SLS Train C (5/8)

Table 4.1-7 FMEA for Gr.2 controller, SLS Train C (6/8)

Table 4.1-7 FMEA for Gr.2 controller, SLS Train C (7/8)

Table 4.1-7 FMEA for Gr.2 controller, SLS Train C (8/8)

Table 4.1-8 FMEA for Gr.1 controller, SLS Train D (1/8)

Table 4.1-8 FMEA for Gr.1 controller, SLS Train D (2/8)

Table 4.1-8 FMEA for Gr.1 controller, SLS Train D (3/8)

Table 4.1-8 FMEA for Gr.1 controller, SLS Train D (4/8)

Table 4.1-8 FMEA for Gr.1 controller, SLS Train D (5/8)

Table 4.1-8 FMEA for Gr.1 controller, SLS Train D (6/8)

Table 4.1-8 FMEA for Gr.1 controller, SLS Train D (7/8)

Table 4.1-8 FMEA for Gr.1 controller, SLS Train D (8/8)

Table 4.1-9 FMEA for Gr.2 controller, SLS Train D (1/9)

Table 4.1-9 FMEA for Gr.2 controller, SLS Train D (2/9)

Table 4.1-9 FMEA for Gr.2 controller, SLS Train D (3/9)

Table 4.1-9 FMEA for Gr.2 controller, SLS Train D (4/9)

Table 4.1-9 FMEA for Gr.2 controller, SLS Train D (5/9)

Table 4.1-9 FMEA for Gr.2 controller, SLS Train D (6/9)

Table 4.1-9 FMEA for Gr.2 controller, SLS Train D (7/9)

Table 4.1-9 FMEA for Gr.2 controller, SLS Train D (8/9)

Table 4.1-9 FMEA for Gr.2 controller, SLS Train D (9/9)

Table 4.1-10 FMEA for Gr.3 controller, SLS Train D (1/8)

Table 4.1-10 FMEA for Gr.3 controller, SLS Train D (2/8)

Table 4.1-10 FMEA for Gr.3 controller, SLS Train D (3/8)

Table 4.1-10 FMEA for Gr.3 controller, SLS Train D (4/8)

Table 4.1-10 FMEA for Gr.3 controller, SLS Train D (5/8)

Table 4.1-10 FMEA for Gr.3 controller, SLS Train D (6/8)

Table 4.1-10 FMEA for Gr.3 controller, SLS Train D (7/8)

Table 4.1-10 FMEA for Gr.3 controller, SLS Train D (8/8)

Table 4.1-11 Effect Analysis of Spurious State Actuation, Train A

Table 4.1-12 Effect Analysis of Spurious State Actuation, Train B

Table 4.1-13 Effect Analysis of Spurious State Actuation, Train C

Table 4.1-14 Effect Analysis of Spurious State Actuation, Train D