US-APWR Technical Report

FMEA of Control Rod Drive Mechanism Control System

December 2007

Revision History

Revision	Date	Page	Description
0	December 2007	All	Original issued

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

Abstract

This report describes Failure Mode and Effect Analysis (FMEA) of Control Rod Drive Mechanism Control System (CRDMCS) for the US-APWR.

The report provides a description and the configuration of the CRDMCS for FMEA. The FMEA tables provide a description of failure mode, method of failure detection, local failure effect and effect on protective function for each component consisted in CRDMCS. This analysis demonstrates the achievement of safety function during the each component failure of CRDMCS.

Table of Contents

List of Tables
List of Figures
List of Acronyms

1.0 INTRODUCTION 1
1.1 Purpose 1
1.2 Scope 1
2.0 SYSTEM DESCRIPTION 2
3.0 FMEA METHOD 3
4.0 FMEA ANALYSIS 4
5.0 REFERENCES 8

List of Tables

Table 4-1 FMEA of CRDMCS ...5

List of Figures

Figure 4-1 CRDMCS Configuration ...4

List of Acronyms

COLA	Combined License Application
CRDM	Control Rod Drive Mechanism
CRDMCS	Control Rod Drive Mechanism Control System
DAS	Diverse Actuation System
DCD	Design Control Document
D/O	Digital Output
ESF	Engineered Safety Feature
FMEA	Failure Mode and Effect Analysis
HSI	Human System Interface
HSIS	Human System Interface System
I&C	Instrumentation and Control
MCCB	Molded Case Circuit Breaker
M/G	Movable Gripper
MHI	Mitsubishi Heavy Industries, Ltd.
NRC	Nuclear Regulatory Commission
PCMS	Plant Control and Monitoring System
PSMS	Protection and Safety Monitoring System
RPIS	Rod Position Indication System
RT	Reactor Trip
RTB	Reactor Trip Breaker
S/G	Stationary Gripper

1.0 INTRODUCTION

1.1 Purpose

The purpose of this technical report is to describe the Mitsubishi Heavy Industries' (MHI's) Failure Modes and Effects Analysis (FMEA) for Control Rod Drive Mechanism Control System (CRDMCS) in Instrumentation and Control (I&C) system for US-APWR. FMEA method is described herein to clarify the purpose and the contents of FMEA tables.

The system descriptions, FMEA method and FMEA analysis are applicable to the US-APWR.

1.2 Scope

FMEA of CRDMCS is described in this report. The safety I&C system, non-safety I&C system and diverse I&C system described in this report are referred to as the Protection and Safety Monitoring System (PSMS), Plant Control and Monitoring System (PCMS) and the Diverse Actuation System (DAS), respectively. The CRDMCS is defined as part of PCMS in the I&C system. The overall architecture of the I&C system with PSMS, PCMS and DAS is briefly described to aid in understanding the MHI's I&C system.

This document can be referred from Plant Licensing Documentation of the US-APWR such as Design Control Document (DCD) and Combined License Application (COLA).

2.0 SYSTEM DESCRIPTION

Nuclear power plant instrumentation senses various plant parameters and transmits appropriate signals to the control systems during normal operation, and to the Reactor Trip (RT) and Engineered Safety Feature (ESF) systems during abnormal and accident conditions. I&C systems provide protection against unsafe reactor operation during steady-state and transient power operation. The primary purpose of the I&C systems is to provide automatic initiating signals, automatic and manual control signals, and monitoring displays to mitigate the consequences of faulted conditions.

The Overall I&C System of the US-APWR consists of the following four echelons.

a. Human System Interface System (HSIS)
b. Protection and Safety Monitoring System (PSMS)
c. Plant Control and Monitoring System (PCMS)
d. Diverse Actuation System (DAS)

The PSMS and PCMS are microprocessor based digital systems that offer high reliability. The HSIS encompasses the Human System Interface (HSI) provided by the PSMS, PCMS and DAS. The CRDMCS is defined as a part of PCMS, and the CRDMCS is connected to the Reactor Control System via point to point data link.

Detail descriptions of the PSMS, PCMS, DAS and HSIS are provided in Topical Reports. [Reference 1, 2, 3, 4]

The CRDMCS in the PCMS adjusts the position of the control rod banks in the reactor core. Each control rod bank is divided into two or more groups to obtain smaller incremental reactivity changes per step. The control rod groups within the same bank are moved such that the relative position of the groups does not differ by more than one-step. Each control rod in a group is paralleled so that rods of the same group move simultaneously.

Power to the Control Rod Drive Mechanisms (CRDMs) is supplied by motor-generator sets. AC power is distributed to the CRDMCS Power Cabinet through Reactor Trip Breakers (RTBs) and CRDM Distribution Panel. The CRDMCS consists of a Logic Cabinet and Power Cabinet. The PCMS controller group of the CRDM control system is located within the Logic Cabinet. The Logic Cabinet consists of microprocessor-based digital systems with redundant controllers. The controller group controls solid-state CRDM power supplies that are located in the Power Cabinet. The mechanical part of the CRDM, which consists of Stationary Gripper (S/G), Movable Gripper (M/G) and LIFT mechanism, is actuated by the coil current generated from the control signals from the CRDMCS through S/G coil, M/G coil and LIFT coil. These mechanical parts adjust the control rods directly.

More detailed information about the CRDM and CRDMCS is provided in the US-APWR DCD. [Reference 5]

3.0 FMEA METHOD

This section describes the FMEA method. The method and contents of the tables are described in the Safety I&C Topical Report. [Reference 1] In addition, the FMEA of CRDMCS demonstrates that:

- No credible single failure of CRDMCS will prevent PSMS actuation.
- No credible single failure of CRDMCS will result in spurious PSMS actuation.

Thus FMEA of CRDMCS demonstrates the PSMS can achieve the safety function in the case of failure each individual component of CRDMCS.

The failure mode, method of failure detection, local failure effect, and effect on protective function or plant for each component in the CRDMCS are described in the FMEA tables. One block diagram and one table are prepared for each system. The columns in the table are explained as follows:

Component
The component being analyzed is identified by functional description. Where there are multiple similar components additional descriptive information is added to ensure an unambiguous identification.

Failure Mode
The failure modes of the component are defined in the terms of the component's output interface to other downstream components. Typical failure modes include high, low and as-is. One row is included in the table for each credible failure mode.

Method of Failure Detection
The means by which the failure will come to the attention of the plant operation/maintenance staff are identified. This could be by automatic detection or manual testing.

Local Failure Effect
The consequent effect(s) of the failure on the component or on its adjunct components are described. Symptoms and local effects including dependent failure are also provided.

Effect on Protective Function or Plant
The effect of the failure on the ability to complete the protective function or spurious actuation of the protective function is described, including identification of any degradation in performance or degree of redundancy.

4.0 FMEA ANALYSIS

This section provides FMEA for the CRDMCS. Figure 4-1 shows the configuration of system diagram for CRDMCS. Table 4-1 shows the FMEA tables for CRDMCS.

The CRDMCS is divided into several parts for the analysis in these figures and tables. These divisions are defined as the Logic Cabinet (processing part and output part), the Power Cabinet (transformer part, Molded Case Circuit Breaker [MCCB] part, current control unit part) and the Coils (S/G coil, M/G coil, LIFT coil).

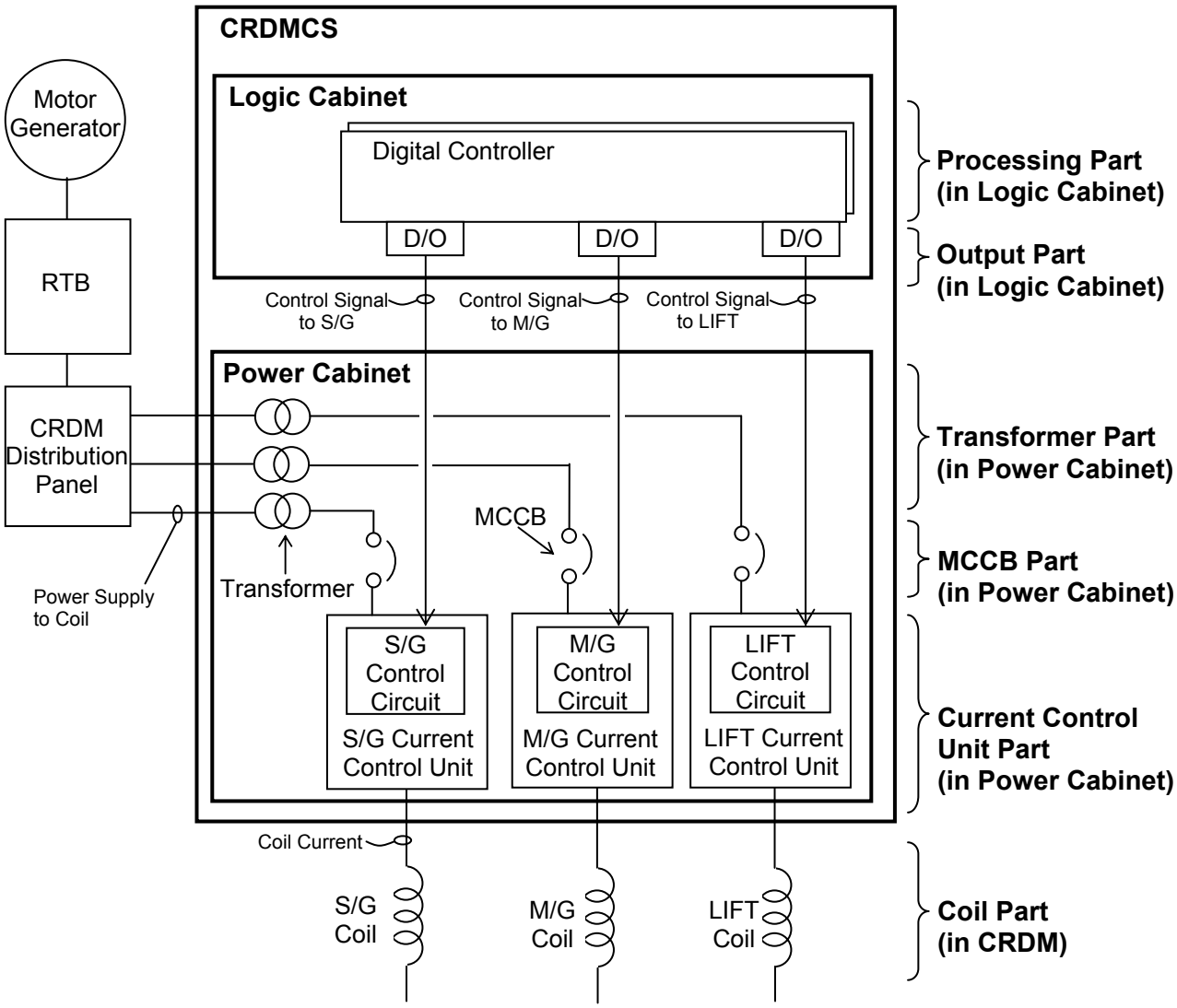

Figure 4-1 CRDMCS Configuration

Table 4-1 FMEA of CRDMCS (1/3)

Component	Failure Mode	Method of Failure Detection	Local Failure Effect	Effect on Protective Function
Logic Cabinet Processing Part	Fail to no data output	Self-diagnostic alarm.	Processing Part consists of two digital controllers. One operates in Control Mode while the other operates in Standby Mode. One digital controller operating in Standby Mode will automatically switch to Control Mode due to its Redundant Standby Controller Configuration.	Redundant Standby Controller Configuration in the digital controller can achieve the control function. PSMS can achieve the reactor trip function during this failure.
Logic Cabinet Output Part to S/G Coil	Fail ON	Self-diagnostic alarm.	S/G coils are ON state; this causes S/G latches of one group to be closed.	Control rods are out of control. PSMS can achieve the reactor trip function during this failure.
	Fail OFF	Self-diagnostic alarm. Alarms from RPIS due to control rods drop.	S/G coils are OFF state; this causes control rods drop due to S/G latches of one group being open when control rods are operating.	Control rods are out of control. Reactor trips due to control rods drop. PSMS can achieve the reactor trip function during this failure.
Logic Cabinet Output Part to M/G Coil	Fail ON	Self-diagnostic alarm.	M/G coils are ON state; this causes M/G latches of one group to be closed.	Control rods are out of control. PSMS can achieve the reactor trip function during this failure.
	Fail OFF	Self-diagnostic alarm. Alarms from RPIS due to control rods drop.	M/G coils are OFF state; this causes control rod drops due to M/G latches of one group being open when control rods are operating.	Control rods are out of control. Reactor trips due to control rods drop. PSMS can achieve the reactor trip function during this failure.
Logic Cabinet Output Part to LIFT Coil	Fail ON	Self-diagnostic alarm.	LIFT coils are maintained their hold-up state; this causes control rods of one group to be inoperable.	Control rods are out of control. PSMS can achieve the reactor trip function during this failure.
	Fail OFF	Self-diagnostic alarm.	LIFT coils will be inoperable; this causes control rods of one group to be inoperable when control rods are operating.	Control rods are out of control. PSMS can achieve the reactor trip function during this failure.

Table 4-1 FMEA of CRDMCS (2/3)

Component	Failure Mode	Method of Failure Detection	Local Failure Effect	Effect on Protective Function
Power Cabinet Transformer for S/G Coil	Fail to disconnection or short circuit	Alarms from failure detection circuit. Alarms from RPIS due to control rods drop.	Rod drops due to S/G latches of one cabinet (three groups) being open when control rods are operating.	Control rods are out of control. Reactor trips due to control rods drop. PSMS can achieve the reactor trip function during this failure.
Power Cabinet Transformer for M/G Coil	Fail to disconnection or short circuit	Alarms from failure detection circuit. Alarms from RPIS due to control rods drop.	Control rod drops due to M/G latches of one cabinet (three groups) being open when control rods are operating.	Control rods are out of control. Reactor trips due to control rods drop. PSMS can achieve the reactor trip function during this failure.
Power Cabinet Transformer for M/G Coil	Fail to disconnection or short circuit	Alarms from failure detection circuit.	Control rods of one cabinet (three groups) are inoperable when control rods are operating.	Control rods are out of control. PSMS can achieve the reactor trip function during this failure.
Power Cabinet MCCB for S/G Current Control Unit	Fail to breaking or overcurrent	Alarms from failure detection circuit. Alarms from RPIS due to control rods drop.	Control rod drops due to S/G latches of one cabinet (three groups) being open when control rods are operating.	Control rods are out of control. Reactor trips due to control rods drop. PSMS can achieve the reactor trip function during this failure.
Power Cabinet MCCB for M/G Current Control Unit	Fail to breaking or overcurrent	Alarms from failure detection circuit. Alarms from RPIS due to control rods drop.	Control rod drops due to S/G latches of one cabinet (three groups) being open when control rods are operating.	Control rods are out of control. Reactor trips due to control rods drop. PSMS can achieve the reactor trip function during this failure.
Power Cabinet MCCB for LIFT Current Control Unit	Fail to breaking or overcurrent	Alarms from failure detection circuit.	Related control rods of the selected group are inoperable.	Control rods are out of control. PSMS can achieve the reactor trip function during this failure.

Table 4-1 FMEA of CRDMCS (3/3)

Component	Failure Mode	Method of Failure Detection	Local Failure Effect	Effect on Protective Function
Power Cabinet S/G Current Control Unit	Fail to spurious actuation	Alarms from failure detection circuit. Alarms from RPIS due to control rods drop.	S/G latches of one group are closed, or control rods drop due to S/G latches of one group being open when control rods are operating.	Control rods are out of control. Reactor trips if control rods drop. PSMS can achieve the reactor trip function during this failure.
	Fail to inoperable	Alarms from failure detection circuit.	S/G latches of one group are inoperable.	Control rods are out of control. PSMS can achieve the reactor trip function during this failure.
Power Cabinet M/G Current Control Unit	Fail to spurious actuation	Alarms from failure detection circuit. Alarms from RPIS if control rods drop.	M/G latches of one group are closed, or control rods drop due to M/G latch of one group being opened when control rods are operating.	Control rods are out of control. Reactor trips if control rods drop. PSMS can achieve the reactor trip function during this failure.
	Fail to inoperable	Alarms from failure detection circuit.	M/G latches of one group are inoperable.	Control rods are out of control. PSMS can achieve the reactor trip function during this failure.
Power Cabinet LIFT Current Control Unit	Fail to spurious actuation	Alarms from failure detection circuit.	Related control rods of the selected group are inoperable.	Control rods are out of control. PSMS can achieve the reactor trip function during this failure.
	Fail to inoperable	Alarms from failure detection circuit.	Related control rods of the selected group are inoperable.	Control rods are out of control. PSMS can achieve the reactor trip function during this failure.
Coil S/G Coil	Fail to disconnection or short circuit	Alarms from failure detection circuit. Alarms from RPIS if control rods drop.	Control rods drop due to S/G latch of the related control rods being open.	Related control rod is out of control. PSMS can achieve the reactor trip function during this failure.
Coil M/G Coil	Fail to disconnection or short circuit	Alarms from failure detection circuit. Alarms from RPIS if control rods drop.	Control rods drop due to M/G latch of the related control rods being open.	Related control rods are out of control. PSMS can achieve the reactor trip function during this failure.
Coil LIFT Coil	Fail to disconnection or short circuit	Alarms from failure detection circuit.	Related control rods are inoperable.	Related control rods are out of control. PSMS can achieve the reactor trip function during this failure.

5.0 REFERENCES

1. “Safety I&C System Description and Design Process”, MUAP-07004, MHI Topical Report.
2. “Safety System Digital Platform - MELTAC-“, MUAP-07005, MHI Topical Report.
3. “Defense-in-Depth and Diversity”, MUAP-07006, MHI Topical Report.
4. “HSI System Description and HFE Process”, MUAP-07007, MHI Topical Report.
5. “US-APWR Design Control Document”, MHI DCD for US-APWR.