US-APWR

Defense-in-Depth and Diversity Coping Analysis

December 2007

Revision History

Revision	Date	Page (Section)	Description
0	December 2007	All	Original issued

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

Abstract

This technical report describes Mitsubishi Heavy Industries' (MHI's) approach to demonstrate defense in depth and diversity (D3) coping analysis for the instrumentation and control (I&C) systems applied to US-APWR plant. This approach is based on the design information described in the MHI's topical reports for digital I&C systems and the Design Control Document (DCD) for the US-APWR design certification application. D3 coping analysis is conducted based on the U.S. Nuclear Regulatory Commission (NRC) requirements including acceptance criteria using best estimate manner for every anticipated operational occurrence (AOO) or a postulated accident (PA) analyzed in the DCD chapter 15 safety analysis. This report describes results of analysis how the diverse actuation system (DAS) cope with a common cause failure (CCF) in the digital safety system that occurs concurrent with each event.

In this analysis, all the safety functions of the digital safety system are assumed to be disabled by CCF. Also, mitigating function of the control systems that use the same digital platform are assumed to be disabled by the same CCF. On the other hand, the DAS provides diverse automatic reactor/turbine trip and diverse emergency feedwater actuation functions which are not impaired by the postulated CCF. The DAS also provide manual actuation functions and plant parameter monitoring functions which can be used to cope with CCFs. Available components and plant conditions assumed in this analysis are established in a best estimate manner considering beyond design basis situation.

The D3 coping analysis is performed to confirm that the US-APWR DCD chapter 15 safety analysis events (AOOs/PAs) are successfully mitigated by the DAS and related components even if a CCF occurs in the assumed plant conditions. The analysis/evaluation is conducted in terms of the pressure boundary integrity, the coolability and the radiation release based on the CCF acceptance criteria.

Table of Contents

List of Tables

List of Figures

List of Acronyms

AOO	anticipated operational occurrence
ATWS	anticipated transients without scram
BOC	beginning-of-Cycle
BTP	branch technical position
C/V	containment vessel
CCF	common cause failure
CRDM	control rod drive mechanism
D3	defense in depth and diversity
DAS	diverse actuation system
DCD	Design Control Document
DNB	departure from nucleate boiling
DNBR	departure from nucleate boiling ratio
ECCS	emergency core cooling system
EFW	emergency feedwater
EFWS	emergency feedwater system
EOC	end-of-cycle
ESF	engineered safety features
HFP	hot full power
HSIS	human-system interface system
HZP	hot zero power
I&C	instrumentation and control
LBLOCA	large break loss of coolant accident
LOCA	loss-of-coolant accident
M/G	motor generator
MHI	Mitsubishi Heavy Industries, Ltd
NRC	U.S. Nuclear Regulatory Commission
OLM	on-line maintenance
PA	postulated accident
PCMS	plant control and monitoring system
PRA	probabilistic risk assessment
PSMS	protection and safety monitoring system
RCCA	rod cluster control assembly
RCP	reactor coolant pump
RCS	reactor coolant system
RTDP	revised thermal design procedure
RTS	reactor trip system
SAR	safety analysis report
SRP	Standard Review Plan
VDU	visual display unit

1.0 INTRODUCTION

The purpose of this technical report is to describe the Mitsubishi Heavy Industries' (MHI's) approach to demonstrate defense in depth and diversity (D3) coping analysis of the instrumentation and control (I&C) systems of the US-APWR plant. MHI prepared this technical report to support D3 design information in the Design Control Document (DCD) for the US-APWR plant design certification application.

In corresponding to the defense in depth and diversity issue, system design approach to prevent common cause failures (CCFs) in the high integrity digital I&C system for the US-APWR plant, and analysis and design approach for the diverse actuation system (DAS) as the countermeasure for the effect of CCFs are described in the following documents.

Description, design basis and conformance to the requirements of the US-APWR digital I&C system is provided in the topical report "Safety I&C System Description and Design Process" (Reference-1)
Also, design concept and quality programs to achieve high integrity of the digital platform applied to the US-APWR I&C system is provided in the topical report "Safety System Digital Platform - MELTAC-" (Reference-2).
Based on these documents, conformance to the requirements for D3 and design and analysis method of the DAS is described in the topical report "Defense-in-Depth and Diversity" (Referece-3).

Based on the above documents, design information of the digital I&C systems and the DAS of the US-APWR plant is described in the DCD for the US-APWR Chapter 7 "Instrumentation and Control Systems".

This technical report shows performance analysis how functions of the DAS cope with CCF in the digital I&C system concurrent with an anticipated operational occurrence (AOO) or a postulated accident (PA) based on best-estimate assumptions.

Applicable codes and standards and conformance to them are described in section 2. Failure mode analysis of digital I&C systems and available DAS functions used in the coping analysis are described in section 3. Basis for the coping analysis including best-estimate assumptions and results of analysis for each event are described in section 4.

2.0 CODES AND STANDARDS

This section identifies compliance to applicable codes, standards and conformance with applicable U.S. Nuclear Regulatory Commission (NRC) guidance, as appropriate. Unless specifically noted, the latest version issued on the date of this document is applicable.

2.1 Code of Federal Regulations

(1) 10 CFR 50.62 “Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants”

The DAS has diverse turbine trip and emergency feedwater (EFW) actuation capability required for ATWS mitigation. The DAS also has a diverse reactor trip function which interrupt electrical power to the control rod control mechanism by tripping the motor-generator set. The DAS design is diverse from the protection system, with the exception of sensors, which are shared with the protection system. This report shows DAS can mitigate the anticipated operational occurrences assuming the safety system failed to trip the reactor.

2.2 Standard Review Plan

(1) Standard Review Plan, Branch Technical Position 7-19 “Guidance for Evaluation of Diversity and Defense in Depth in Digital Computer-Based Instrumentation and Control Systems”

The DAS design and analysis approach to comply with this standard review plan (SRP) branch technical position (BTP) is described in the topical report “Defense-in-Depth and Diversity” (Referece-3).
This technical report describes the best-estimate coping analysis required in this BTP for postulated AOOs and PAs in the safety analysis concurrent with a CCF based on acceptance criteria stated in the same BTP.

3.0 BASIS OF I&C SYSTEM DESIGN FOR D3 COPING ANALYSIS

3.1 Objective and General Consideration

Objective of this D3 coping analysis is to show that the DAS is able to mitigate the plant response against postulated events considering a CCF in the digital I&C system, and to meet the requirements of the BTP 7-19.

In the BTP 7-19, steps to demonstrate the vulnerability to the CCF before preparing countermeasures for the effect of the CCF are described as follows.

Point 1: The applicant/licensee should assess the D3 of the proposed I&C system to demonstrate that vulnerabilities to CCFs have been adequately addressed.

Point 2: In performing the assessment, the vendor or applicant/licensee should analyze each postulated CCF for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate or SAR Chapter 15 analysis methods. The vendor or applicant/licensee should demonstrate adequate diversity within the design for each of these events.“

In this report, the D3 coping analysis is conducted based on the above steps.

First, the evaluation of failure mode of digital systems and available diverse means assumed in the coping analysis are described in detail within subsections below. In these subsections, assumptions are established considering beyond-design-basis nature of the postulated events concurrent with a CCF.

Then, effects of CCF on plant safety for each postulated event are analyzed in the section 4 using best-estimate analysis assumptions, method and acceptance criteria assuming the DAS mitigating functions.

3.2 Failure Mode of the Digital I&C System

3.2.1 Effect of CCF in Digital Platform

Effect of a CCF on the digital platform MELTAC is discussed in the topical report ”Defense-in-Depth and Diversity” (Reference-3).

In the MELTAC digital platform, the highly conservative design approach is applied to realize high integrity of the software. Important characteristics are summarized as follows.

- No use of the commercial off the shelf software including the operating system.
- No use of software and hardware interrupt in software execution.
- All the software modules are executed during a fixed cycle time in the predefined order. This means that there is neither selection of executed modules nor change of order of execution

- No dynamic allocation of memories. This means that all the memories used to execute safety functions are accessed in every execution cycle

These design attributes show that MELTAC digital platform does not change its software execution path and memory access no matter how the plant condition is normal operation or accident conditions.

Therefore, most provable case which a CCF could occur is that hidden failures which disable the safety functions are accumulated among the redundant systems and finally loses entire safety function when it is required to actuate.

3.2.2 Failure Mode of the Protection and Safety Monitoring System

Based on the topical report “Defense-in-Depth and Diversity” (Reference-3), CCF may affect all the digital controllers in the protection and safety monitoring system (PSMS).
PSMS achieve various safety functions within the distributed digital system architecture.
But, obviously, from the point of ability to mitigate the abnormal plant conditions, it is most severe to assume that CCF disables all the safety functions in the PSMS.

According to the description about CCFs in the MELTAC digital platform in section 3.2.1, potential or hidden defects in the digital system could be a functional failure. But detectable failures that tends to actuate spurious signals can be adequately treated and repaired before all the redundant portion of the safety system are affected by the same or common cause.
Instead, undetectable failures by the same or common cause may remain inside the safety systems without any indication of malfunction. As the time proceeds, redundant portions of the safety system could be affected by the same or common cause, and finally the safety system lose its safety function to mitigate the event even though there are sufficient redundancy.

Although these scenarios are quite unlikely to occur, all the safety functions of the PSMS could be disabled by CCF in this way.

As a result, all the safety functions are assumed to be disabled in the D3 coping analysis before an event occurs.

On the other hand, spurious actuation of safety functions other than the initiating events in the chapter 15 safety analysis is not assumed in the D3 coping analysis, because type of software failures for spurious actuation is self-announcing and not activated by the plant accident conditions.

3.2.3 Failure Mode of the Plant Control and Monitoring System

The plant control and monitoring system (PCMS) consists of many subsystems which contain digital controller and have many kind of plant control functions which can be used to regulate the plant normal operation and can be used to mitigate the consequences of the transients.

In general, mitigating functions of these control system within non-safety PCMS is not assumed in the DCD chapter 15 safety analysis. However, in case of best-estimate analysis, available non-safety function can be assumed to mitigate the consequences of the events.
As the same digital platform MELTAC used in the PSMS is also applied to the PCMS, CCFs postulated in the PSMS could influence availability of the PCMS control functions.
From the point of understandable and comparable way, mitigation functions in the PCMS which are not usually activated during normal power operation are not assumed available in the D3 coping analysis because these are the stand-by functions similar to the safety functions in the PSMS.
On the other hand, normal regulation function of these control systems may be maintained in case of the CCF, and can be assumed available in the D3 coping analysis.
Availability of each control system in the D3 coping analysis is described below

(1) Rod control system

This control system has dead-band for reactor coolant system (RCS) temperature error signal to generate motion demand for the control rod. This means that CCF could affect the control function without any indication of plant malfunction. So it is not assumed to be used as mitigation in case of postulated CCF.
Also, rod stop interlocks which could inhibit inadvertent control rod withdrawal are assumed to be affected and disabled by the CCF.

(2) Pressurizer pressure control system

Pressurizer pressure control system continuously monitors the RCS pressure compared with the fixed reference pressure and continuously controls power to the proportional heater.
Pressurizer control system malfunctions induced by a CCF could immediately affect the pressurizer pressure control function and may cause plant transients. This will be detected because these types of failures are self-announcing.
But, other pressure control means such as pressurizer spray or backup heater are activated through dead-band for the pressure error signal.
So, as a totall, pressurizer pressure control function is not assumed to be maintained nor used as mitigation in case of postulated CCF.

(3) Pressurizer water level control system

Pressurizer water level control system continuously monitors the pressureizer water level compared with the programed reference water level and balance of charging and letdown flow. Deviation of these parameters continuously controls the charging flow control valve to regulate the pressurizer water level.
Pressurizer level control system malfunctions induced by a CCF could immediately affect the control function and may cause plant transients. This self announcing nature of this control function will be immediately detected by maintenance staff and system restore work will be started.
But, other relating means to keep pressurizer water level such as letdown isolation is a stand-by function which can not be assured to be operable.
So, as a totall, pressurizer level control function is not assumed to be maintained nor used as mitigation in case of postulated CCF.

(4) Steam generator water level control system

Steam generator water level control system continuously monitors the steam generator water level compared with the fixed reference water level and balance of feedawter and steam flow. Deviation of these parameters continuously controls feedwater regulation valves to keep steam generator water level.
Steam generator water level control system malfunctions induced by CCFs could immediately affect the regulation of the water level and may cause plant transients. These self announcing nature of this control system will be immediately detected by maintenance staff and system restore work will be started.
So, in the D3 coping analysis, the steam generator water level control system can be assumed to maintain water level control function except for each control malfunction as the initiating events in AOOs.
On the other hand, an interlock to prevent overfilling of the steam generator is not assumed to be available because this is a stand-by function.

(5) Turbine bypass control system

Turbine bypass control system continuously monitors the RCS temperature error signal and open the turbine bypass valves in case of the temperature error exceeds setpoints. This control system is the stand-by system during normal operation. So the turbine bypass control system is not assumed to be used as a mitigation in case of postulated CCF.

3.2.4 Failure Mode of Plant Monitoring Function

Plant monitoring function of the digital I&C system is categorized as continuous monitoring display and alarm system. Continuous display signals comes from various digital systems to the visual display units (VDUs) of the human system interface system (HSIS).

Safety portion of the HSIS consists of the MELTAC digital platform and may be affected by the postulated CCF. On the other hand, non-safety displays and computer systems consist of completely different computer system other than MELTAC. So the non-safety display capability can be assumed operable during postulated CCF. Exception to this in the non-safety HSIS is the alarm system. All the alarm status signals are gathered into the alarm process system which consists of MELTAC platform.

Considering about the availability of the monitoring function, information from the PSMS and alarm system is conservatively assumed not to be available because of their use of MELTAC platform and stand-by nature.

Instead, information display originating from the non-safety systems is assumed to be available because these non-safety control and monitoring functions are always running and malfunctions are self announcing.

In the assumptions to identify monitoring and decision making process for CCF situation, these non-safety originated display information can be used, but in case of an urgent situation diverse information displayed on the DAS has much priority.

3.3 Diverse Actuation System Functions

The DAS has following functions to provide diverse means to cope with CCF.

- Diverse automatic actuation
- Diverse manual actuation
- Diverse monitoring

Detailed functions and design information are described in the topical report “Defense-in-Depth and Diversity "(Referece-3) and the DCD chapter 7 for the US-APWR.

The DAS has diverse automatic actuation functions to shutdown the reactor and to achieve secondary system core heat removal.

(1) Diverse reactor trip

The following initiation signals trip the reactor by tripping the motor-generator set to interrupt electrical power to the control rod drive mechanism (CRDM) coils. Turbine trip and all of the main feedwater regulation valve closure are also actuated by the same signals.

- High pressurizer pressure
  (2-out-of-4 voting logic of the 4 pressurizer pressure channel signals)
- Low pressurizer pressure
  (2-out-of-4 voting logic of the 4 pressurizer pressure channel signals)
- Low steam generator water level
  (2-out-of-4 voting logic from the one channel signal per steam generator of steam generator water level.)

(2) Diverse emergency feedwater actuation

Following initiation signal automatically actuate all of the EFW pumps. The steam generator blow down isolation valves are closed by the same signal to ensure sufficient EFW flow to steam generators.

- Low steam generator water level
  (2-out-of-4 voting logic from the one channel signal per steam generator of steam generator water level.)

The DAS contains conventional switches in the main control room for manual actuation of the systems and the components which is required to cope with CCF.

- Manual reactor trip / Turbine trip / Main feedwater isolation: 1 switch
  (manually actuate diverse reactor trip function descried above)
- Manual emergency feedwater actuation: 1 switch

(manually start all the emergency feedwater pumps)

- Manual emergency core cooling system (ECCS) actuation: 1 switch
  (manually start all the safety injection pumps)
- Manual containment vessel (C/V)isolation: 1 switch
  (manually close major containment isolation valves at once)
- Manual operation of emergency feedwater control valves 4 switches
  (manually control a emergency feedwater control valve for each steam generator)
- Manual operation of main steam depressurization valves: 4 switches
  (manually control a main steam depressurization valve for each steam generator)
- Manual operation of pressurizer depressurization valve: 1 switch
  (manually control a pressurizer depressurization valve)

Long-term manual operation after the DAS actuation to maintain the plant in safe, keep hot-standby and achieve cold shutdown (containment splay, main steam isolation, residual heat removal system, etc.) can be operated by controls in the main control room or local controls other than digital I&C portion

The DAS contains conventional indicators and alarms located in the main control room for monitoring plant parameter and initiate operator action to cope with CCF.
Monitored valiables are as follows.

- Wide-range neutron flux
- Pressurizer pressure
- RCS pressure wide range
- RCS cold leg temperature (Tcold) (for each loop)
- Pressurizer water level
- Steam generator water level (for each steam generator)
- Main steam line pressure (for each steam generator)
- Containment pressure

Also following alarms are used to initiate operator action in the case of events with CCF.

- Diverse reactor trip actuation (with first hit indication)
- Diverse emergency feedwater actuation
- Diverse RCS leak detection

3.4 Operator Actions

This section summarizes the design basis events which require the operator actions when a CCF occurs, and the operator actions required to mitigate these events. The operator actions required in the event assuming CCF occurrence are categorized as follows.

- The operator actions assumed in the safety analyses discussed in the DCD chapter 15
- The operator actions including isolation of the EFW supplied to a faulted steam generator and actuation of the ECCS

The first category above is the operator actions assumed in the analysis of the design basis events. These operator actions are designed to be available when an event with a CCF occurs. The second category is the operator actions uniquely required to mitigate the event with a CCF, which include the isolation of the EFW supplied to a faulted steam generator at the on-line maintenance (OLM), and the actuation of the ECCS. Following sections discuss the events with a CCF occurrence which require the operator actions and identify the operator actions required in these events as categorized above.

3.4.1 Operator Actions Assumed in the Safety Analyses

The events which require the operator actions assumed in the safety analyses discussed in the DCD chapter 15 are as follows.

- Inadvertent Decrease in Boron Concentration in Reactor Coolant System
- Chemical and Volume Control System Malfunction that Increases Reactor Coolant Inventory
- Radiological Consequences of Steam Generator Tube Failure
- Spectrum of Rod Ejection Accidents
- Radiological Consequences of the Failure of Small Lines Carrying Primary Coolant Outside Containment

Note that the operator actions required to operate long term cooling and achieve a cold shutdown condition are out of scope of this evaluation as described in subsection 4.1.

The DAS and PCMS have capability to detect and identify the above events. Table 3.4-1 describes operator actions applicable to the events.

3.4.2 Operator Actions Including Isolation of the EFW and Actuation of the ECCS

The injection of EFW and ECCS which remove the core decay heat are designed to require following operator actions.

- Isolation of the EFW supplied to a faulted steam generator when a rupture of the secondary system piping (including a main steam line break and a main feedline break) occurs
- Actuation of the ECCS when a small break loss-of-coolant accident (LOCA) occurs

In the rupture of the secondary system piping accidents analysis discussed in the DCD chapter 15, the EFW supplied to the faulted steam generator are automatically isolated by detecting the decrease of the pressure in the faulted steam generator. Without assuming OLM, feedwater is supplied to the intact steam generators and the event is mitigated without any operator actions, which is applicable to the event with a CCF. When an OLM at which the tie-line opens is assumed and therefore one train of the emergency feedwater system (EFWS) is unavailable, it is required to manually isolate the emergency feedwater supply to the faulted steam generator in order to establish the emergency feedwater supply to the intact steam generators and remove the core decay heat. This procedure should also be available when a CCF occurs. Identification of the faulted steam generator and judgment of the event are achieved, for example, by monitoring the decrease of the pressure in the faulted steam generator.

In the small break LOCA analysis discussed in the DCD chapter 15, ECCS is automatically actuated by detecting the decrease of the pressure in the RCS and therefore the core coolability is achieved. When a CCF occurs, the core coolability is achieved by manually actuating all of the ECCS. Identification and judgment of the LOCA are achieved, for example, by monitoring the decrease of the pressure in the RCS.

Table 3.4-1 List of Monitoring and Control Actions for CCF

Events	Credited Manual Action
Inadvertent Decrease in Boron Concentration in Reactor Coolant System	• Termination of charging flow of primary makeup water
Chemical and Volume Control System Malfunction that Increases Reactor Coolant Inventory	• Termination of charging flow
Radiological Consequences of Steam Generator Tube Failure	• Reactor trip • Isolation of Affected steam generator • Cooldown of Primary coolant system • Pressure equalization between primary and secondary coolant system • Termination of Injection from ECCS
Spectrum of Rod Ejection Accidents	• Actuation of C/V spray system • Actuation of annulus emergency exhaust system
Radiological Consequences of the Failure of Small Lines Carrying Primary Coolant Outside Containment	• Isolation of C/V

4.0 D3 COPING ANALYSIS AND RESULTS

4.1 Best Estimate Assumptions of the Plant System Conditions

To perform D3 coping analysis, assumptions of plant and equipment conditions should be established.
In case of DCD chapter 15 safety analysis, conservative assumptions are made to assure safety of the plant for design basis events. But in case of D3 coping analysis, BTP 7-19 permits best-estimate analysis which does not require conservative assumptions such as single failure of a mitigating system.

Followings are the assumptions used in the D3 coping analysis. Performing the D3 coping analysis, these relaxed assumptions can be used.

(1) Reactor Operating Mode

In the D3 coping analysis, plant is assumed to be operated at rated power. This assumption covers most of the operational time interval of the plant which means this assumption covers most provable plant condition.
Also, in the D3 coping analysis, there is no limitation of core cycle during power operation, which means this covers entire 24 months core operation cycle.

(2) Single Failure

In the D3 coping analysis, no single failure is assumed for the structure, system and components used to mitigate the consequences of the postulated events. This means that in the best estimate analysis, extremely low probability of a event concurrent with a CCF and additional single failure of a required mitigating equipment is not need to be considered.
Despite this, in the D3 coping analysis, planned maintenance of such equipment during power operation is assumed because the on-line maintenance of the safety equipment is allowed by the Technical Specifications.

(3) Power Source

In the D3 coping analysis, off site electrical power sources are assumed to be available during mitigating period of the events except for the loss of offsite power as an initiating event.

(4) External Hazards

In the D3 coping analysis, no external hazards such as earthquake, fire and natural phenomena is assumed to occur concurrent with the events.

(5) Administrative operational control mode

In some cases to test the plant system or components during plant operation, operating mode of each I&C function may be changed to unusual mode under administrative control by plant operators. For example, rod control system may be in manual control

mode during power operation for nuclear instrumentation calibration or secondary system operational test. In this case, time duration of these specific operation is controlled to a limited time, and the condition of the plant and operation of I&C systems are carefully monitored by the plant operator.
In case of events with CCF during these administrative operation modes will be easily detected and operator can take mitigation action.
So, in the D3 coping analysis, administrative operation modes especially for the plant control systems are excluded for the evaluation.

(6) Long-term manual operation

Long-term manual operation after the DAS actuation to maintain the plant in safe and achieve cold shutdown can be operated by hardwired switches in the main control room or local controls other than digital I&C portion. Also, some digital portion may be restored from CCF by restarting the system in a short time period. So details of long-term manual operation are not discussed in this coping analysis

4.2 Events to be Analyzed

Based on the BTP 7-19, all the postulated events including both AOOs and PAs are considered as the events to be analyzed in the D3 coping analysis.

Events can be grouped into some categories and detailed evaluation can be implemented for some representative cases which have specific characteristics or most severe results.

In this D3 coping analysis, the large break loss of coolant accident (LBLOCA) is considered to be mitigated based on early detection of small leaks in the RCS and manual operator actions that ensure the plant is shutdown so that small leaks can be repaired before they can become large breaks. Plant procedures and Technical Specifications enforce these manual operator actions. So, the D3 coping analysis described in section 4 of this report does not discuss about plant behavior for LBLOCA with CCF.

This method of coping with a LBLOCA and concurrent CCF in the PSMS is based on the following:

- The probabilistic risk assessment (PRA) identifies LBLOCA as an accident with extremely low probability of occurrence.
- The staff requirements memoranda to SECY 93-087 identifies a CCF as a beyond design basis event based on its extremely low probability of occurrence.
- The combined probability of a LBLOCA with a CCF is even more remote. This is because there is a single software trajectory within the PSMS, which means the CCF in the PSMS cannot be triggered by the LBLOCA. Therefore LBLOCA and CCF are completely random events.

Objective of the D3 assessment is to show that total plant risk is not affected by CCFs in the digital I&C system. In terms of this objective, LBLOCA with CCF has less significance for the plant risks. PRA described in the DCD chapter 19 shows that above approach is acceptable to limit plant risk within the design goal.

4.3 Acceptance Criteria

The BTP 7-19 describes the following acceptance criteria for AOO/PA in CCF.

- The integrity of the RCS pressure boundary should not be violated for AOO. And the integrity of the containment should not be violated for PA.
- Radiation release should not be exceeding 10 percent of 10 CFR 100 guideline value for AOO. And radiation release should not be exceeding the 10 CFR 100 guideline value for PA.

Table 4.3-1 summarizes the CCF acceptance criteria.

The SRP 15.8 ATWS describes the following acceptance criteria for ATWS.

- The RCS pressure shall not exceed ASME Service Level C limits (approximately 22 MPa or 3200 psig)
- Peak cladding temperature shall not to exceed 2200°F. The maximum cladding oxidation shall not to exceed 17% the total cladding thickness before oxidation. And the maximum hydrogen generation shall not to exceed 1% of the maximum hypothetical amount if all the fuel cladding had reached to produce hydrogen.

Table 4.3-2 summarizes the ATWS acceptance criteria.

Table 4.3-3 shows the acceptance criteria in this report. For the integrity of the RCS pressure boundary, the ATWS criterion is applied in this report. The RCS pressure boundary integrity can be considered to be maintained if the ATWS criterion is met. As described in subsection 3.3 and 3.4, the DAS and the EFS equipment are designed to be maintained the integrity of the containment in the DCD chapter 15 events assuming a CCF. The ATWS criteria for the coolability is not necessary to apply for the D3 coping analysis, however, conservatively adopted as the criteria in this report.

The D3 coping analysis for the RCS pressure boundary integrity is described in subsection 4.5. The analysis for the coolability is described in subsection 4.6. And subsection 4.7 describes the evaluation for the radiation release.

Table 4.3-1
CCF Acceptance Criteria (BTP 7-19)

	RCS pressure	Coolability	Radiation release
AOO	RCS pressure boundary should not be violated	N/A	Should not be exceeding 10 percent of 10 CFR 100 guideline value
PA	Containment Integrity should not be violated	N/A	Should not be exceeding the 10 CFR 100 guideline value

Table 4.3-2
ATWS Acceptance Criteria (SRP 15.8)

	RCS pressure	Coolability	Radiation release
AOO	Shall not exceed ASME Service Level C limits (approximately 22 MPa or 3200 psig)	- Peak cladding temperature < 2200°F - the maximum cladding oxidation < 17% - the maximum hydrogen generation <1%	N/A
PA	N/A	N/A	N/A

Table 4.3-3
Acceptance Criteria in this Report

	RCS pressure	Coolability	Radiation release
AOO	Shall not exceed ASME Service Level C limits (approximately 22 MPa or 3200 psig)	- Peak cladding temperature < 2200°F - the maximum cladding oxidation < 17% - the maximum hydrogen generation <1%	Should not be exceeding 10 percent of 10 CFR 100 guideline value
PA	Same above (Conservatively use except for low frequency accidents) AND Containment Integrity should not be violated	Same above (Conservatively use except for low frequency accidents)	Should not be exceeding the 10 CFR 100 guideline value

4.4 Diverse Actuation System Assumed in the D3 Coping Analysis

The diverse automatic actuation functions of the DAS to shutdown the reactor and to achieve secondary system core heat removal following initiation signals. The detailed functions are described in subsection 3.3. Table 4.4-1 summarizes the diverse reactor trip and diverse emergency feedwater actuation analytical limit and delay times for functions used in the D3 coping analysis.

(1) Diverse reactor trip

- High pressurizer pressure
- Low pressurizer pressure
- Low steam generator water level

(2) Diverse emergency feedwater actuation

- Low steam generator water level

Table 4.4-1
DAS Actuation Analytical Limit and Time Delays
Assumed for D3 Coping Analysis

Actuation Signal	Analytical Limit	Time Delay (sec)
1. Diverse reactor trip		
High pressurizer pressure	2440 psia	10
Low pressurizer pressure	1840 psia	10
Low steam generator water level	7% of span	10
2. Diverse emergency feedwater actuation		
Low steam generator water level	7% of span	10

4.5 Analysis for Reactor Coolant System Pressure Boundary Integrity

The capacity of the pressurizer safety valve is designed that this valve is able to release the maximum surge flow to the pressurizer assuming a turbine trip without a reactor trip, as far as steam generator secondary side have sufficient water inventory. The trip function of the DAS includes the low steam generator water level signal, thus the reactor trips from this signal before the steam generator dry-out assuming CCF. Therefore, the RCS pressure increase is mitigated by the DAS the pressurizer safety valve which is not affected by CCF in the DCD chapter 15 safety analysis events assuming CCF. In this subsection, the representative D3 coping analysis is conducted in the loss of load event to assure that the RCS pressure increase can be successfully mitigated by the pressurizer safety valve and the DAS.

4.5.1 Loss of Load

The loss of load event is modeled by assuming an instantaneous step load decrease in both steam flow and feedwater flow from their full value (100%) to zero at the beginning of the transient. This assumption bounds all credible loss of load scenarios in the event group, such as loss of external load, turbine trip, loss of condenser vacuum, closure of main steam isolation valve. This assumption is the same as the DCD chapter 15 safety analysis.

4.5.1.1 Evaluation Model

The MARVEL-M plant transient analysis code is used to calculate transient responses of reactor power, reactor coolant pressure, reactor coolant temperature, hot spot heat flux, pressurizer water volume and minimum departure from nucleate boiling ratio (DNBR) following the loss of load event. This evaluation model is the same as the DCD chapter 15 safety analysis. Additional details regarding the MARVEL-M code are provided in Reference-4.

4.5.1.2 Analysis Assumptions, Input Parameters and Initial Conditions

The following assumptions are the differences from the DCD chapter 15 safety analysis. The other assumption, input parameters and initial conditions are the same as the DCD chapter 15 safety analysis. Especially, the pressurizer pressue control system is not assumed as well as the DCD chapter 15 safety analysis.

- Any reactor trip actuation by the reactor trip system (RTS) is ignored.
- The analysis assumes the high pressurizer pressure reactor trip by the DAS and uses conservative assumptions for the analytical limit and delay time as described in Table 4.4-1.

4.5.1.3 Results

Figures 4.5.1-1 through 4.5.1-4 are plots of key system parameters versus time. The sudden reduction in steam flow results in an increase in the RCS pressure and temperature. The pressurizer safety valve opens at 8.6 seconds. The rod motion begins at 17.1 seconds by the high pressurizer pressure of the DAS. The peak reactor coolant pump (RCP) outlet pressure which is the highest pressure in the RCS is below 3200 psig as shown in Figure 4.5.1-2. Thus, the DAS and the pressurizer safety valve maintain the integrity of the reactor coolant pressure boundary.

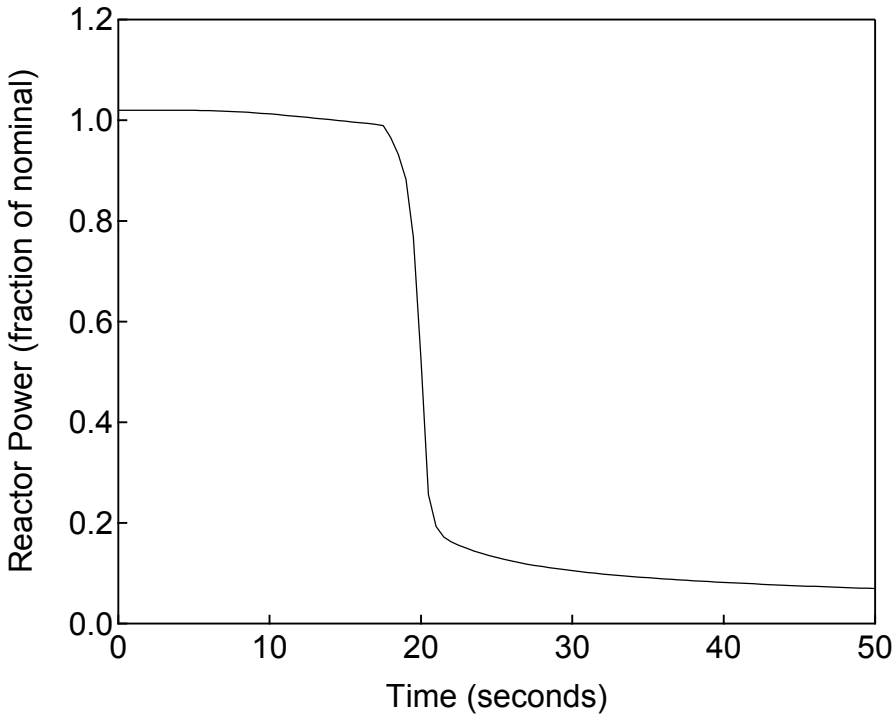

Figure 4.5.1-1 Reactor Power versus Time
Loss of Load Event

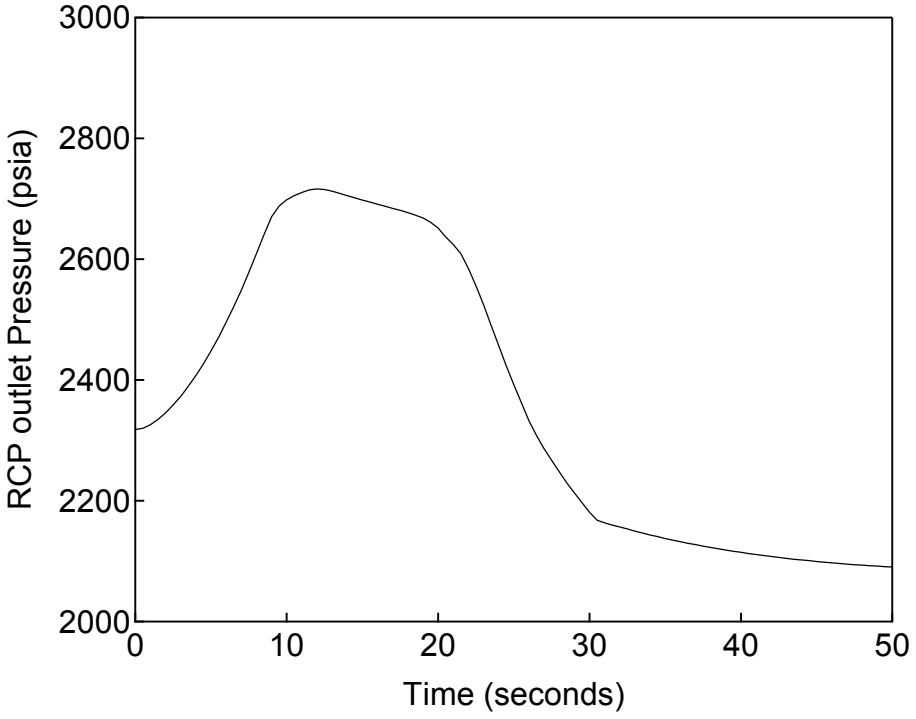

Figure 4.5.1-2 RCP Outlet Pressure versus Time
Loss of Load Event

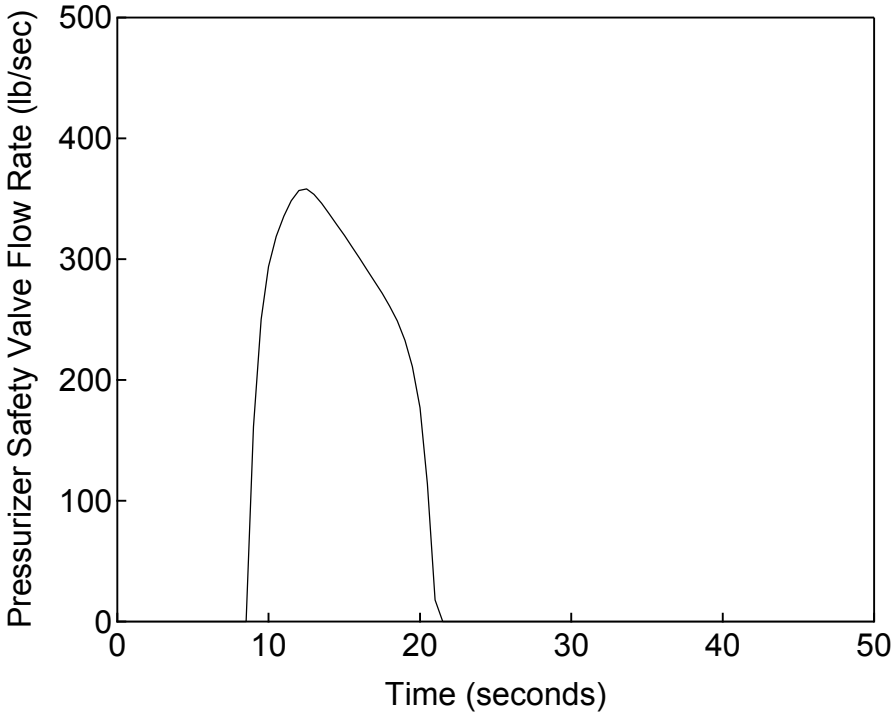

Figure 4.5.1-3 Pressurizer Safety Valve Flow Rate versus Time Loss of Load Event

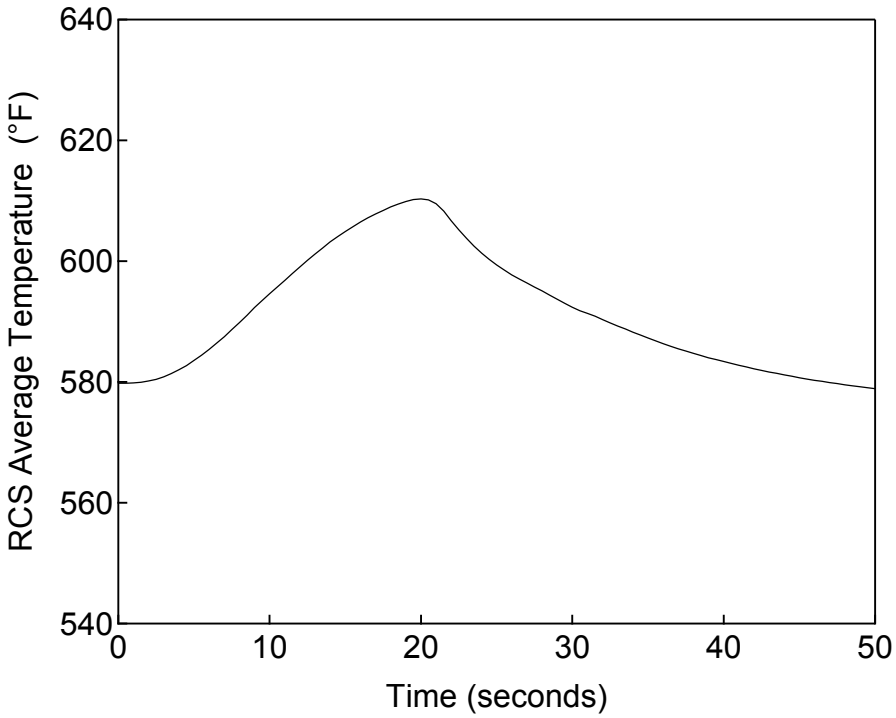

Figure 4.5.1-4 RCS Average Temperature versus Time
Loss of Load Event

4.6 Analysis for the Core Coolability

Each event in the DCD chapter 15 safety analysis assuming CCF can be assigned to the following five categories for the core coolability criteria. The categorization is based on the following conditions.

- To assume the best estimated plant parameters.
- The plant is assumed to be operated at rated power.

Category 1: Event has a very low probability of occurrence
Category 2: RTS and/or engineered safety features (ESF) not actuated and no adverse impact
Category 3: Event mitigated by DAS and no adverse impact
Category 4: Event similar to other event and no adverse impact
Category 5: Analysis required and results show acceptance criterion is met

As the result of this screening process summarized in Table 4.6-1, the following two cases are analyzed for the D3 coping analysis:

- Uncontrolled control rod assembly withdrawal at power
- Partial loss of forced reactor coolant flow

The other events do not challenge the criteria because the categories of these events are less than category 4.

Table 4.6-1
Evaluation of the Each Event for the DNBR Criterion (Sheet 1 of 3)

Section	Title	AOO/PA	Category	Evaluation
15.1.1	Decrease in Feedwater Temperature as a Result of Feedwater System Malfunctions	AOO	2	The event could result in no significant adverse consequence without RTS/ESF actuation.
15.1.2	Increase in Feedwater Flow as a Result of Feedwater System Malfunctions	AOO	2	The event could result in no significant adverse consequence without RTS/ESF actuation.
15.1.3	Increase in Steam Flow as a Result of Steam Pressure Regulator Malfunction	AOO	2	The event could result in no significant adverse consequence without RTS/ESF actuation.
15.1.4	Inadvertent Opening of a Steam Generator Relief or Safety Valve	AOO	-	N/A
15.1.5	Steam System Piping Failures Inside and Outside of Containment	PA	2	This event could result in no significant adverse consequence without RTS/ESF actuation.
15.2.1	Loss of External Load	AOO	3	The event could be mitigated by DAS and DNBR remains above the 95/95 DNBR limit.
15.2.2	Turbine Trip	AOO	3	Same as 15.2.1 with CCF
15.2.3	Loss of Condenser Vacuum	AOO	3	Same as 15.2.1 with CCF
15.2.4	Closure of Main Steam Isolation Valve	AOO	3	Same as 15.2.1 with CCF
15.2.5	Steam Pressure Regulator Failure	BWR	-	N/A
15.2.6	Loss of Non-Emergency AC Power to the Station Auxiliaries	AOO	2	The loss of the non-emergency AC power causes the loss of power supply for the motor generator (M/G) set and result in the rod cruster control assembly (RCCA) trip, which does not cause the DNBR violation.
15.2.7	Loss of Normal Feedwater Flow	AOO	3	The event could be mitigated by DAS and DNBR remains above the 95/95 DNBR limit.
15.2.8	Feedwater System Pipe Break Inside and Outside Containment	AOO PA	3	The event could be mitigated by DAS and DNBR remains above the 95/95 DNBR limit.
15.3.1.1	Partial Loss of Forced Reactor Coolant Flow	AOO	5	Event Analyzed. See section 4.6.2

Table 4.6-1
Evaluation of the Each Event for the DNBR Criterion (Sheet 2 of 3)

Section	Title	AOO/PA	Category	Evaluation
15.3.1.2	Complete Loss of Forced Reactor Coolant Flow	AOO	2	The loss of the non-emergency AC power causes the loss of power supply for the M/G set and result in the RCCA trip, which does not cause the DNBR violation.
15.3.2	Flow Controller Malfunctions	BWR	-	N/A
15.3.3	Reactor Coolant Pump Rotor Seizure	PA	4	This event could be severer than the result of the 15.3.1.1 event with CCF, but meet to the acceptance criteria for PA.
15.3.4	Reactor Coolant Pump Shaft Break	PA	4	This event could be severer than the result of the 15.3.1.1 event with CCF, but meet to the acceptance criteria for PA.
15.4.1	Uncontrolled Control Rod Assembly Withdrawal from a Subcritical or Low Power Startup Condition	AOO	-	N/A
15.4.2	Uncontrolled Control Rod Assembly Withdrawal at Power	AOO	5	Event Analyzed See section 4.6.1
15.4.3	Control Rod Misoperation (System Malfunction or Operator Error)	AOO PA	2	The event could result in no significant adverse consequence without RTS/ESF actuation.
15.4.4	Startup of an Inactive Loop or Recirculation Loop at an Incorrect Temperature	-	-	N-1 loop operation is not permitted in US-APWR.
15.4.5	Flow Controller Malfunction Causing an Increase in BWR Core Flow Rate	BWR	-	N/A
15.4.6	Inadvertent Decrease in Boron Concentration in the Reactor Coolant System	AOO	3	This event is a slow transient due to low positive reactivity insertion rate. This slow transient provides sufficient time to take corrective manual action.
15.4.7	Inadvertent Loading and Operation of a Fuel Assembly in an Improper Position	PA	-	N/A
15.4.8	Spectrum of Rod Ejection Accidents	PA	4	This event could be severer than the result of the 15.4.2 event with CCF, but meet to the acceptance criteria for PA.

Table 4.6-1
Evaluation of the Each Event for the DNBR Criterion (Sheet 3 of 3)

Section	Title	AOO/PA	Category	Evaluation
15.4.9	Spectrum of Rod Drop Accidents in a BWR	BWR	-	N/A
15.5.1	Inadvertent Operation of Emergency Core Cooling System that Increases Reactor Coolant Inventory	AOO	-	The ECCS can not inject into the RCS at nominal, at-power operating pressure.
15.5.2	Chemical and Volume Control System Malfunction that Increases Reactor Coolant Inventory	AOO	2	The event could result in no significant adverse consequence without RTS/ESF actuation.
15.6.1	Inadvertent Opening of a PWR Pressurizer Pressure Relief Valve or a BWR Pressure Relief Valve	AOO	3	The event could be mitigated by DAS and DNBR remains above the 95/95 DNBR limit.
15.6.2	Radiological Consequences of the Failure of Small Lines Carrying Primary Coolant Outside Containment	AOO	2	The event could result in no significant adverse consequence without RTS/ESF actuation.
15.6.3	Radiological Consequences of Steam Generator Tube Failure	PA	3	The DAS and manual operations can lead to no significant adverse consequence without RTS and EFS.
15.6.4	Radiological Consequences of Main Steam Line Failure Outside Containment (BWR)	BWR	-	N/A
15.6.5	Loss-of-Coolant Accidents Resulting from Spectrum of Postulated Piping Breaks within the Reactor Coolant Pressure Boundary	PA	1/3	The DAS and manual operations can lead to no significant adverse consequence without RTS and EFS at small break LOCA. This event is category 3. Large break LOCA with CCF has a very low probability of occurrence. This event is category 1.

4.6.1 Uncontrolled Control Rod Assembly Withdrawal at Power

The uncontrolled control rod assembly withdrawal at power is caused by a control system or rod control system failure that causes a bank withdrawal to occur. An uncontrolled control rod assembly withdrawal at power results in an increase in core heat flux. Since the heat extracted from the steam generator lags behind the core power until the steam generator pressure reaches the main steam safety valve setpoint, the reactor coolant temperature tends to increase. Without a manual or automatic reactor trip (typically the over temperature ΔT, high power range neutron flux, and high pressurizer pressure), the power mismatch and the rise of reactor coolant temperature could eventually result in departure from nucleate boiling (DNB).

4.6.1.1 Evaluation Model

The MARVEL-M plant transient analysis code is used to calculate transient responses of reactor power, reactor coolant pressure, reactor coolant temperature, hot spot heat flux, pressurizer water volume and minimum DNBR following uncontrolled control rod assembly withdrawal at power. The DNBR calculations use the Revised Thermal Design Procedure (RTDP) and the WRB-2 DNB correlation. This evaluation model is the same as the US-APWR DCD chapter 15 safety analysis. Additional details regarding the MARVEL-M code are provided in Reference-4.

4.6.1.2 Analysis Assumptions, Input Parameters and Initial Conditions

The following assumptions are the differences from the DCD chapter 15 safety analysis. The other assumption, input parameters and initial conditions are the same as the DCD chapter 15 safety analysis.

- Any reactor trip actuation by the RTS is ignored and no reactor trip actuation by the DAS is assumed.
- The reactivity inserted to the core is assumed to be at 200 pcm for the beginning-of cycle (BOC) case and 500 pcm for the end-of-cycle (EOC) case consistent with the available reactivity of the RCCA bank-D withdrawal from the insertion limit to the all rods fully withdrawn position.
- The withdrawal of the RCCA is assumed to be at possible maximum speed. It takes 50 seconds to withdraw RCCA bank-D from the insertion limit to the all rods fully withdrawn position.
- The moderator temperature coefficient is assumed to be -6 pcm/°F for the BOC case and -30 pcm/°F for the EOC case (These values are the realistic negative values consistent with the moderator temperature coefficient of 0 pcm/°F at the BOC hot zero power (HZP) condition).
- The doppler power coefficient is assumed considering 20% margin on the core design value. This margin is smaller than the margin used in the DCD chapter 15 safety analysis, but still conservative value.

The power distribution is assumed to be the limiting design power distribution used in the of the DCD chapter 15 safety analysis. The axial power distribution for the BOC case may be mitigated by assuming the power shape consistent with the core burn-up, but not adopted in this analysis.

4.6.1.3 Results

Figures 4.6.1-1 through 4.6.1-4 are plots of key system parameters versus time. The reactivity insertion results in increase in core heat flux, RCS temperature, and decrease in DNBR. However after the end of the reactivity insertion at 50 seconds due to fully control rod withdrawn, the reactor power is reduced by the moderator reactivity feedback and the doppler reactivity feedback. Figures 4.6.1-4 shows the minimum DNBR in both BOC and EOC cases are above the 95/95 DNBR limit. Therefore, the peak cladding temperature does not exceed 2200°F and the core coolability is maintained.

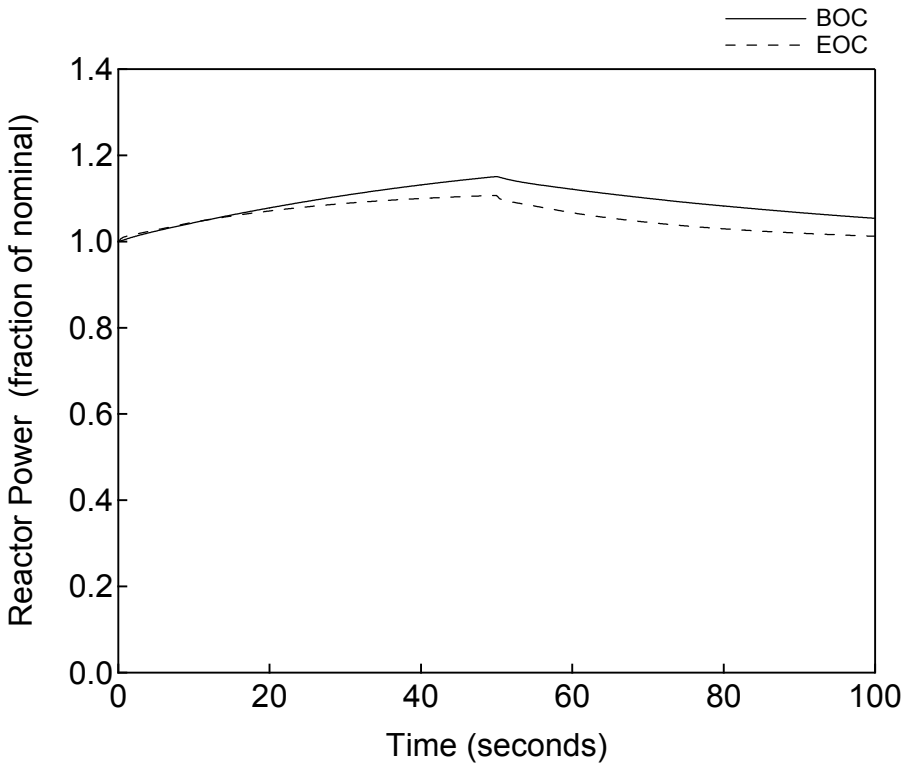

Figure 4.6.1-1 Reactor Power versus Time
Uncontrolled Control Rod Assembly Withdrawal at Power

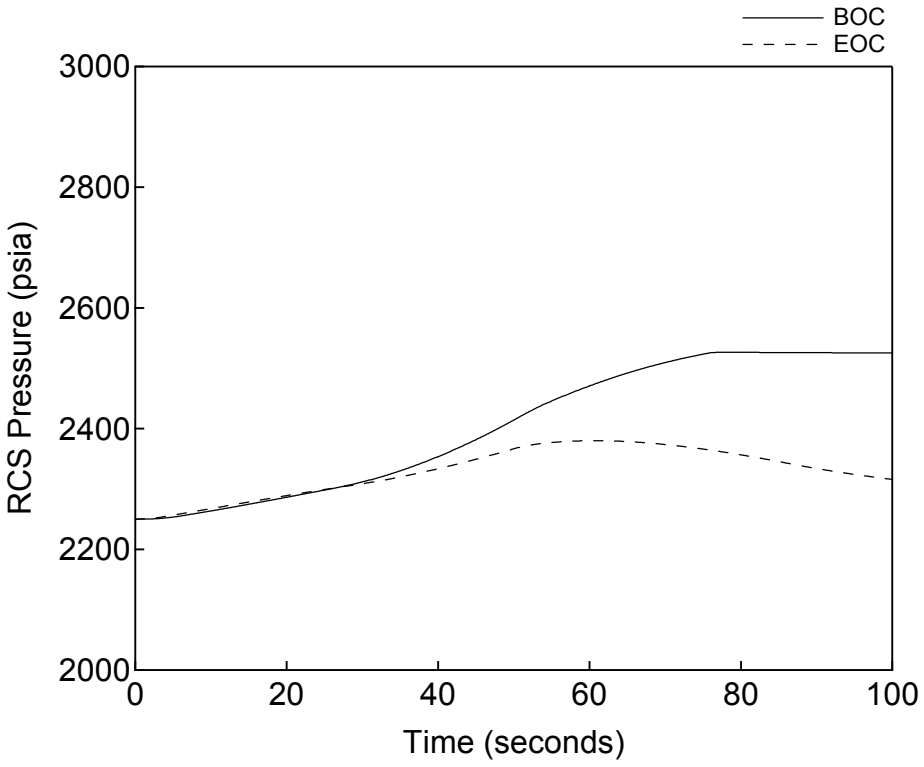

Figure 4.6.1-2 RCS Pressure versus Time
Uncontrolled Control Rod Assembly Withdrawal at Power

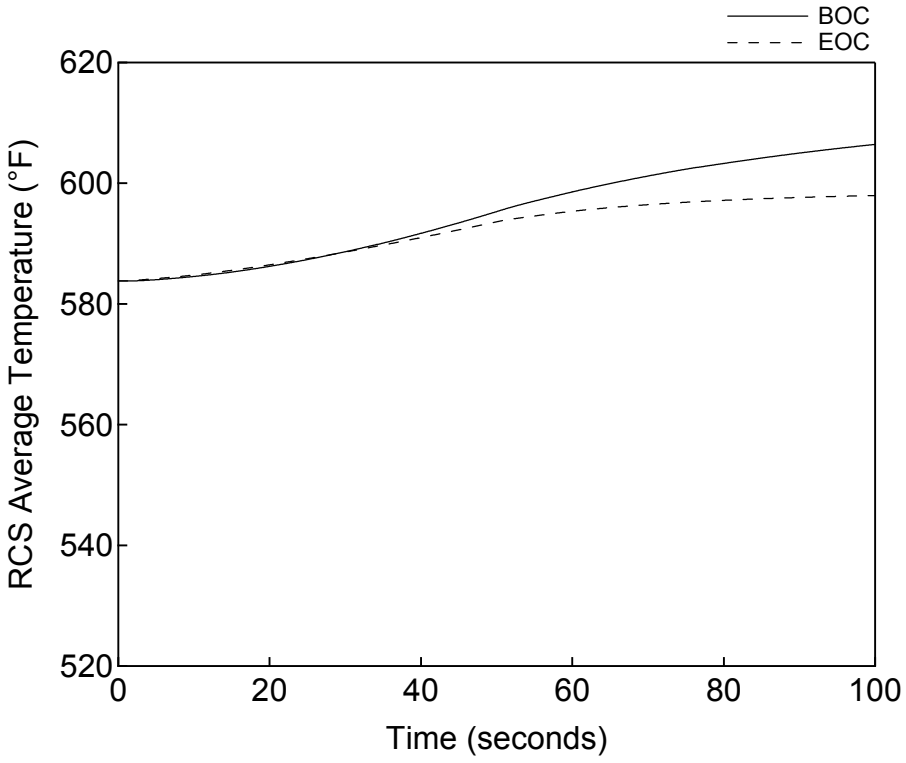

Figure 4.6.1-3 RCS Average Temperature versus Time
Uncontrolled Control Rod Assembly Withdrawal at Power

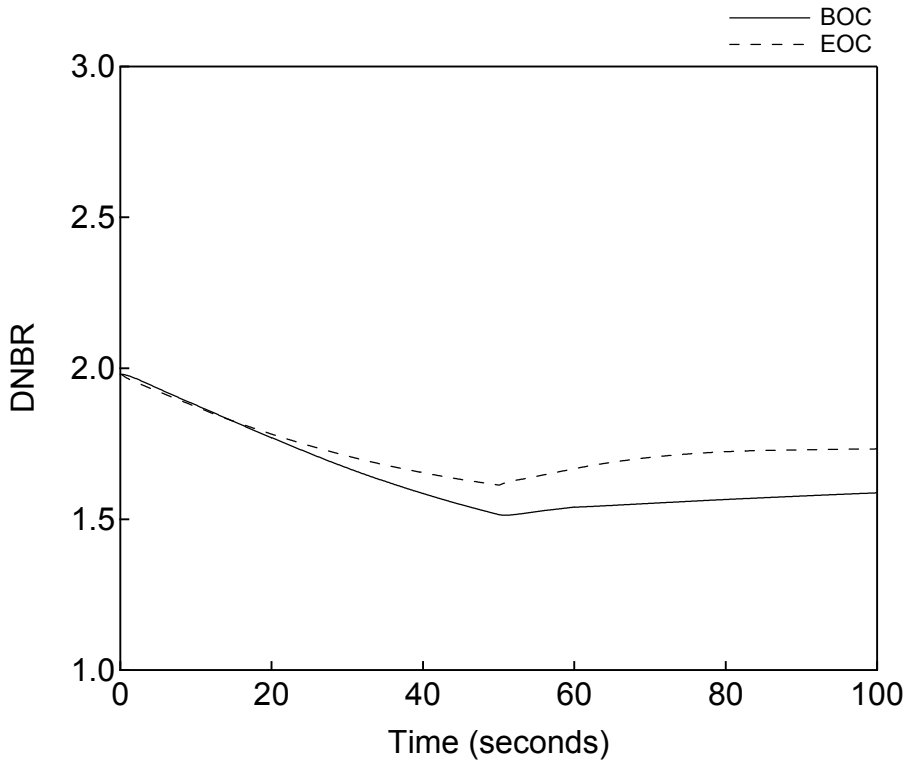

Figure 4.6.1-4 DNBR versus Time
Uncontrolled Control Rod Assembly Withdrawal at Power

4.6.2 Partial Loss of Forced Reactor Coolant Flow

Loss of forced reactor coolant flow events can result from a mechanical or electrical failure in one or more RCPs or from a fault in the power supply to the pump motor. A partial loss of forced reactor coolant flow event results from a simultaneous loss of electrical supply to one or more of the four RCP motors. If the reactor is at power at the time of the transient, the immediate effect of a loss of coolant flow is a rapid increase in the coolant temperature and a decrease in minimum DNBR. This transient is terminated by the low reactor coolant flow trip, which prevents DNB occurrence. Without a manual or automatic reactor trip (low reactor coolant flow, low reactor coolant pump speed), the rise of reactor coolant temperature could eventually result in DNB.

4.6.2.1 Evaluation Model

The MARVEL-M plant transient analysis code is used to calculate transient responses of various parameters following a loss of coolant flow. The model simulates the RCS including the RCS piping, RCPs, reactor vessel, core, pressurizer and surge line, the steam generator primary and secondary sides, control and protection systems, as well as pressurizer safety valves and steam generator relief and safety valves. The MARVEL-M code includes a dynamic RCP and flow transient model that solves the fundamental flow transient equations based on a momentum balance around each reactor coolant loop and across the reactor vessel, flow continuity, and the RCP characteristics with or without electrical power to supply the pump motors. The multi-loop capability of the MARVEL-M code allows assuming each of the loops behaves independently, allowing the analysis of the partial loss of flow event. Although the analysis of this event is terminated shortly after the reactor trip, the pump and loop flow models would establish reverse flow that bypasses the core in the loops with RCP coastdowns. The MARVEL-M code generates an interface file that includes the time-dependent histories of the reactor power, the RCS pressure, the core inlet temperature, and core inlet flow rate for use in the VIPRE-01M code.
The VIPRE-01M code calculates the minimum DNBR during the transient using this interface as a boundary condition assuming a constant design power distribution. The DNBR calculations use the RTDP and the WRB-2 DNB correlation.
These evaluation models are same as the US-APWR DCD chapter 15 safety analysis.

4.6.2.2 Analysis Assumptions, Input Parameters and Initial Conditions

In the D3 coping analysis, one RCP coastdown is assumed to be the initiating event caused by a possible single failure of a RCP breaker or pump motor. Note that the two RCP coastdown assumed in the DCD chapter 15 safety analysis is to cover future design variation in pump power supply configuration.
The following assumptions are the differences from the DCD chapter 15 safety analysis. The other assumption, input parameters and initial conditions are the same as the DCD chapter 15 safety analysis.

- Any reactor trip actuation by the RTS is ignored. And no reactor trip actuation by the DAS is assumed.

- One RCP coastdown is assumed to be the initiating event.
- The moderator temperature coefficient is assumed to be -6 pcm/°F (This values is the realistic negative value consistent with the moderator temperature coefficient of 0 pcm/°F at the BOC HZP condition).
- The doppler power coefficient is assumed considering 20% margin on the core design value. This margin is smaller than the margin used in the DCD chapter 15 safety analysis, but still conservative value.
- The DNBR analysis in VIPRE-01M uses the transient values of RCS pressure and core inlet temperature calculated by MARVEL-M, which are conservatively assumed to be constant same as in the DCD chapter 15 safety analysis.

The power distribution is assumed to be the limiting design power distribution used in the of the DCD chapter 15 safety analysis. The axial power distribution for the BOC case may be mitigated by assuming the power shape consistent with the core burn-up, but not adopted in these analyses.

4.6.2.3 Results

Figures 4.6.2-1 through 4.6.2-5 are plots of key system parameters versus time. The reduction of the core flow causes an increase of RCS average temperature. The reactor power is reduced by the moderator reactivity feedback. The minimum DNBR is above the 95/95 DNBR limit. Therefore the core coolability criterion is met. Therefore, the peak cladding temperature does not exceed 2200°F and the core coolability is maintained.

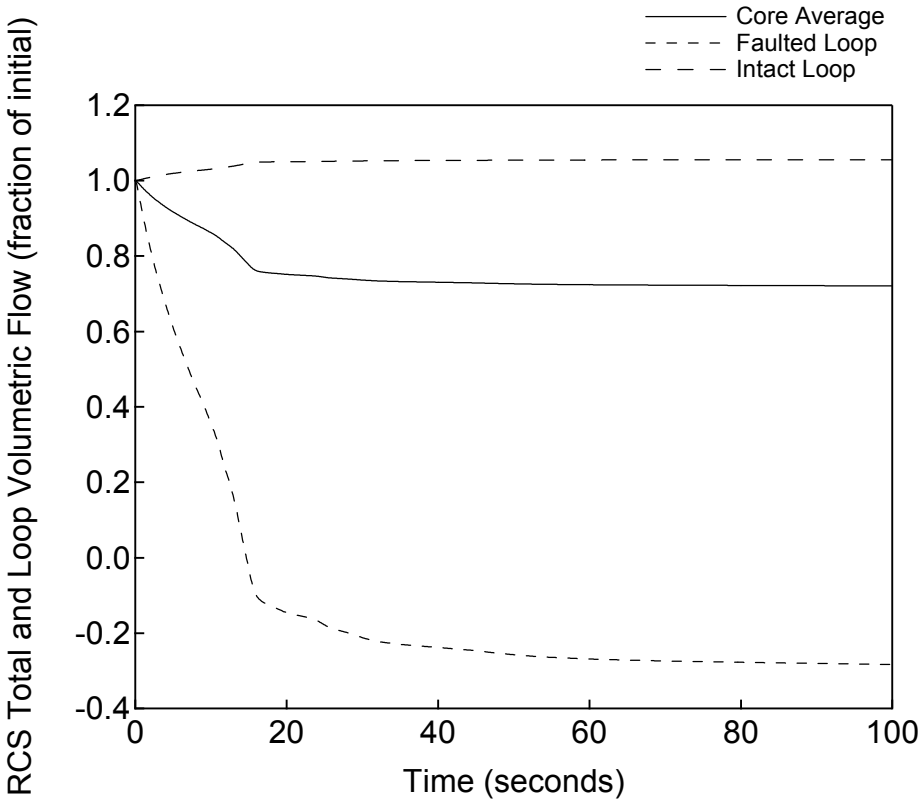

Figure 4.6.2-1 RCS Total and Loop Volumetric Flow versus Time
Partial Loss of Forced Reactor Coolant Flow

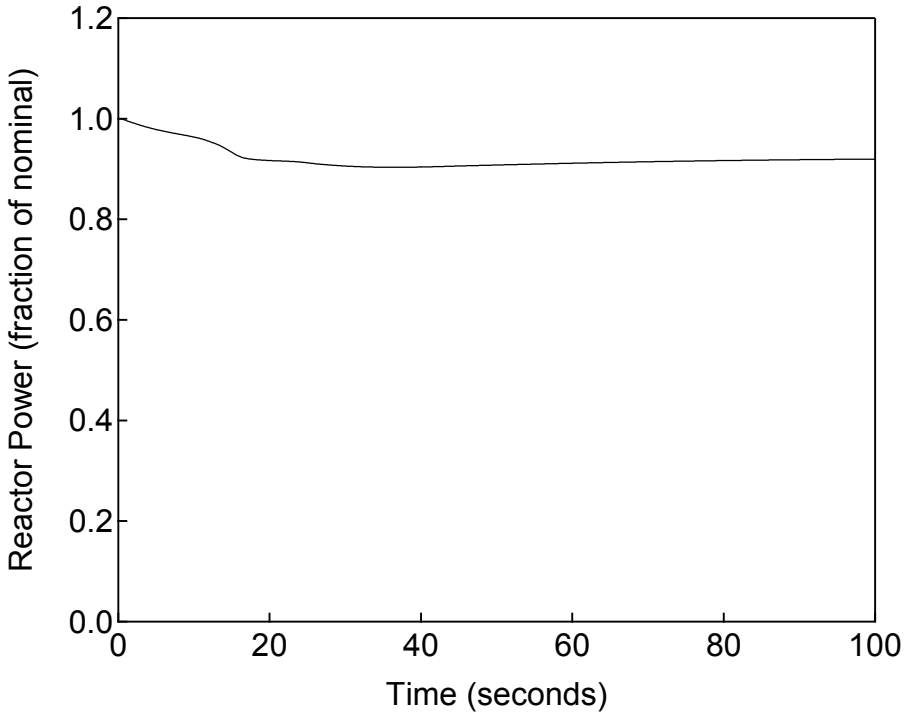

Figure 4.6.2-2 Reactor Power versus Time
Partial Loss of Forced Reactor Coolant Flow

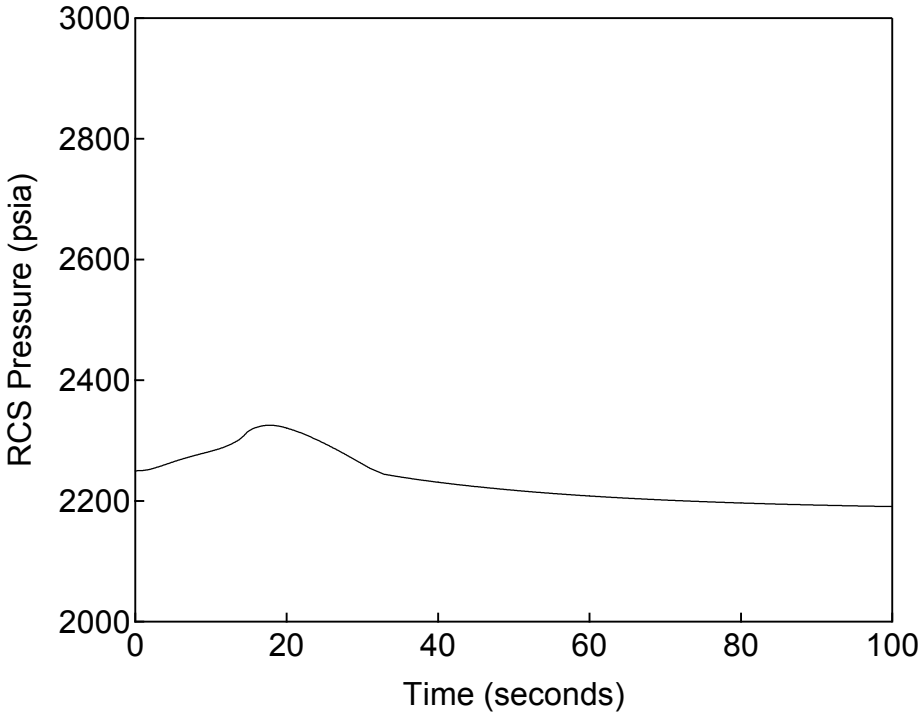

Figure 4.6.2-3 RCS Pressure versus Time
Partial Loss of Forced Reactor Coolant Flow

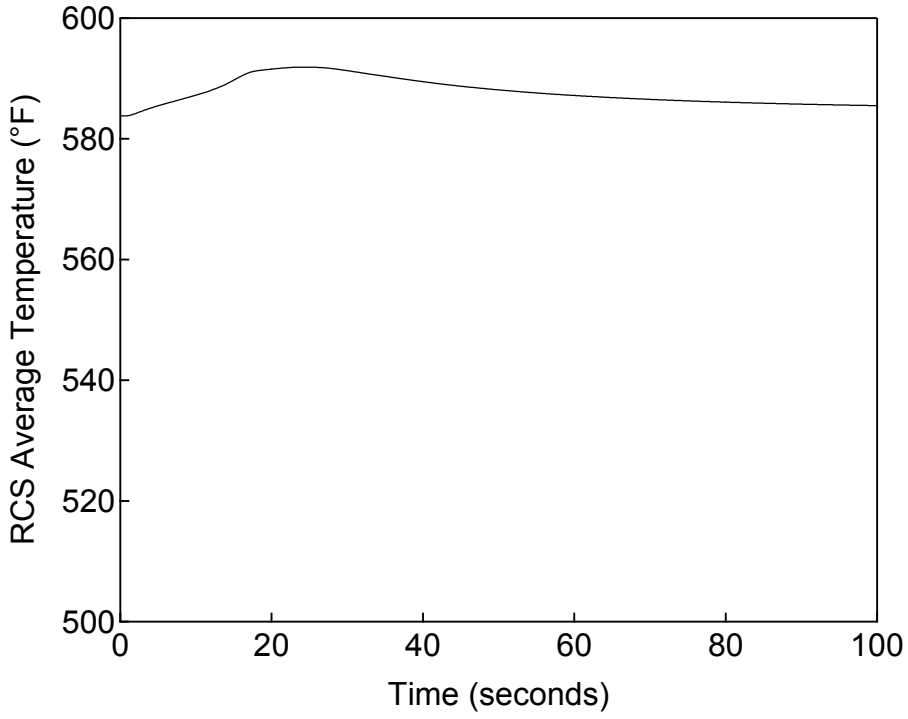

Figure 4.6.2-4 RCS Average Temperature versus Time
Partial Loss of Forced Reactor Coolant Flow

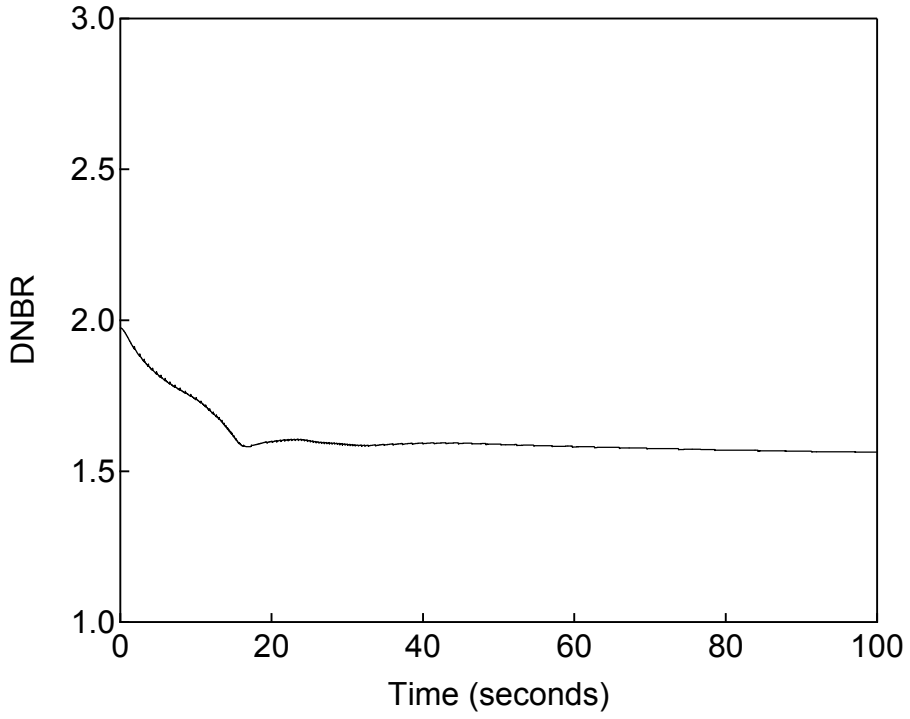

Figure 4.6.2-5 DNBR versus Time
Partial Loss of Forced Reactor Coolant Flow

4.7 Evaluation for the Radiation Release

As described in subsection 3.4, the DAS and the equipment sush as EFWS and ECCS are designed to provide adequate information to make manual actions to terminate the events and not to be exceeding the CCF radiation release criteria.

5.0 CONCLUSION

This technical report describes MHI's approach to demonstrate the D3 coping analysis for the I&C systems applied to the US-APWR.

In the D3 coping analysis, all the safety functions of the digital safety system are assumed to be disabled by a CCF. Also, mitigating functions of the control system that using the same digital platform are assumed to be disabled by the same CCF. The DAS provides diverse automatic reactor/turbine trip and diverse emergency feedwater actuation which are not impaired by the postulated CCF. The DAS also provides manual actuation functions and plant parameter monitoring functions which can be used to cope with CCFs. Available components and plant conditions assumed in the analysis are established in a best estimate manner considering beyond design basis situation.

The D3 coping analysis confirms that the DAS copes with a CCF in the digital safety system that occurs concurrent with US-APWR DCD chapter 15 safety analysis events (AOOs/PAs) in terms of the pressure boundary integrity, the coolability and the radiation release based on the CCF acceptance criteria. The analysis also shows the ATWS criteria for the DCD chapter 15 events assuming a CCF.

6.0 REFERENCES

In this section, references referred in this technical report except for applicable codes, standards and regulatory guidance in Section 2 are enumerated.

1. Safety I&C System Description and Design Process, MUAP-07004-P (Proprietary) and MUAP-07004-NP (Non-Proprietary), July 2007.

2. Safety System Digital Platform -MELTAC-, MUAP-07005-P (Proprietary) and MUAP-07005-NP (Non-Proprietary), July 2007

3. Defense-in-Depth and Diversity, MUAP-07006-P (Proprietary) and MUAP-07006-NP (Non-Proprietary), July 2007.

4. Non-LOCA Methodology, MUAP-07010-P (Proprietary) and MUAP-07010-NP (Non-Proprietary), July 2007.