



**MITSUBISHI HEAVY INDUSTRIES, LTD.**  
16-5, KONAN 2-CHOME, MINATO-KU  
TOKYO, JAPAN

April 10, 2007

Document Control Desk  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555-0001

Attention: Mr. David B. Matthews

Project No.0751  
MHI Ref: UAP-HF-07037

**Subject: Transmittal of the Topical Report entitled "Defense-in-Depth and Diversity".**

With this letter, Mitsubishi Heavy Industries, LTD. (MHI) transmits to the U.S. Nuclear Regulatory Commission (NRC) the topical report entitled "Defense-in-Depth and Diversity" for review and approval. MHI seeks NRC approval of this document for reference in the US-APWR design control document (DCD) and for reference in License Amendment Requests for operating plants.

Based on the discussion in the pre-submittal meeting between the MHI and NRC staff on November 28, 2006, MHI has developed this topical report and looks forward to the upcoming discussion of the Defense-in-Depth and Diversity (D3) System design with the NRC staff in the pre-application review meeting in early June, 2007. MHI believes that the information enclosed herewith will be of value in NRC's review for the application of the US-APWR Design Certification.

As indicated in the enclosed materials, this topical report contains information that MHI considers proprietary, and therefore the entire Topical Report should be withheld from disclosure pursuant to 10 C.F.R. § 2.390 (a)(4) and 10 C.F.R § 9.17 (a)(4) as trade secrets and commercial or financial information which is privileged or confidential. A non-proprietary version of the topical report is also being submitted in this package (Enclosure 3). In the non-proprietary version, the proprietary information, bracketed in the proprietary version, is replaced by the rationale for non-disclosure.

In accordance with the NRC submittal procedures for Topical Reports, this letter includes a copy of the proprietary version (Enclosure 2), a copy of the non-proprietary version (Enclosure 3) and the Affidavit of Masahiko Kaneda (Enclosure 1) which identifies the reasons MHI respectfully requests that all materials bracketed in Enclosure 2 be withheld from disclosure pursuant to 10 C.F.R. § 2.390 (a)(4) and 10 C.F.R.§ 9.17(a)(4).

Please contact Dr. C. Keith Paulson, Senior Technical Manager, Mitsubishi Nuclear Energy Systems, Inc. if the NRC has questions concerning any aspect of the submittals. His contact information is below.

Sincerely,



Masahiko Kaneda,  
General Manager- APWR Promoting Department  
Mitsubishi Heavy Industries, LTD.

Enclosures:

Enclosure1 - Affidavit of Masahiko Kaneda (non-proprietary)

Enclosure2 - Defense-in-Depth and Diversity (proprietary) (MUAP-07006-P, Rev.0)

Enclosure3 - Defense-in-Depth and Diversity (non-proprietary) (MUAP-07006-NP, Rev.0)

CC: S. R. Monarque

L. J. Burkhart

C. K. Paulson

Contact Information

C. Keith Paulson, Senior Technical Manager

Mitsubishi Nuclear Energy Systems, Inc.

4350 Northern Pike, Suite 301

Monroeville, PA 15146

E-mail: ckpaulson@aol.com

Telephone: (412) 374 - 4063

**MITSUBISHI HEAVY INDUSTRIES, LTD.**

**AFFIDAVIT**

I, Masahiko Kaneda, state as follows:

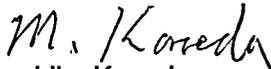
1. I am General Manager, APWR Promoting Department, of Mitsubishi Heavy Industries, LTD ("MHI"), and have been delegated the function of reviewing MHI's US-APWR documentation to determine whether it contains information that should be withheld from disclosure pursuant to 10 C.F.R. § 2.390 (a)(4) and 10C.F.R. § 9.17(a)(4) as trade secrets and commercial or financial information which is privileged or confidential.
2. In accordance with my responsibilities, I have reviewed the enclosed topical report dated April 10, 2007, entitled "Defense-in-Depth and Diversity" and have determined that portions of the report contain proprietary information that should be withheld from public disclosure. Those pages containing proprietary information are identified with the label "Proprietary" on the top of the page and proprietary information has been bracketed with an open and closed bracket as shown here "[ ]". The first page of the topical report indicates that all information identified as "Proprietary" should be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4).
3. The information identified as proprietary in the enclosed topical report has in the past been, and will continue to be, held in confidence by MHI and its disclosure outside the company is limited to regulatory bodies, customers and potential customers, and their agents, suppliers, and licensees, and others with a legitimate need for the information, and is always subject to suitable measures to protect it from unauthorized use or disclosure.
4. The basis for holding the referenced information confidential is that it describes the unique design of the Defense-in-Depth and Diversity ("D3") System, developed by MHI and not used in the exact form by any of MHI's competitors. This information was developed at significant cost to MHI, since it required the performance of Research and Development, detailed design for its software and hardware extending over several years.
5. The referenced information is being furnished to the Nuclear Regulatory Commission ("NRC") in confidence and solely for the purpose of supporting the NRC staff's review of the Topical Report.
6. The referenced information is not available in public sources and could not be gathered readily from other publicly available information. Other than through the provisions in article 3 above, MHI knows of no way the information could be lawfully acquired by organizations or individuals outside of MHI.
7. Public disclosure of the referenced information would assist competitors of MHI in their design of new nuclear power plants without incurring the costs or risks associated with the design of the subject systems. Therefore, disclosure of the information contained in

the referenced topical report would have the following negative impacts on the competitive position of MHI in the U.S. nuclear plant market:

- A. Loss of competitive advantage due to the costs associated with development of the D3 System. Providing public access to such information permits competitors to duplicate or mimic the D3 System design without incurring the associated costs.
- B. Loss of competitive advantage of the US-APWR created by benefits of enhanced plant safety, and reduced operation and maintenance costs associated with the D3 System.

I declare under penalty of perjury that the foregoing affidavit and the matters stated therein are true and correct to the best of my knowledge, information and belief.

Executed on this 10th day of April, 2007.



Masahiko Kaneda,  
General Manager- APWR Promoting Department  
Mitsubishi Heavy Industries, LTD.

Enclosure 2

MHI Topical Report: MUAP-07006-P, Rev.0

**Defense-in-Depth and Diversity**

April 2007  
(Proprietary Version)

[Important Notice]

This topical report contains proprietary information of Mitsubishi Heavy Industries, LTD (MHI). MHI requests that the NRC withhold this information from public disclosure. The first page of this topical report and those pages containing proprietary information are identified with the label "Proprietary" on the top of the page. The first page of the topical report also indicates that all information identified as "Proprietary" should be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4).

Enclosure 3

MHI Topical Report: MUAP-07006-NP, Rev.0

**Defense-in-Depth and Diversity**

April 2007  
(Non-Proprietary Version)

This is a non-proprietary version of MHI Topical Report, MUAP-07006-NP, Rev.0, with all proprietary information removed.

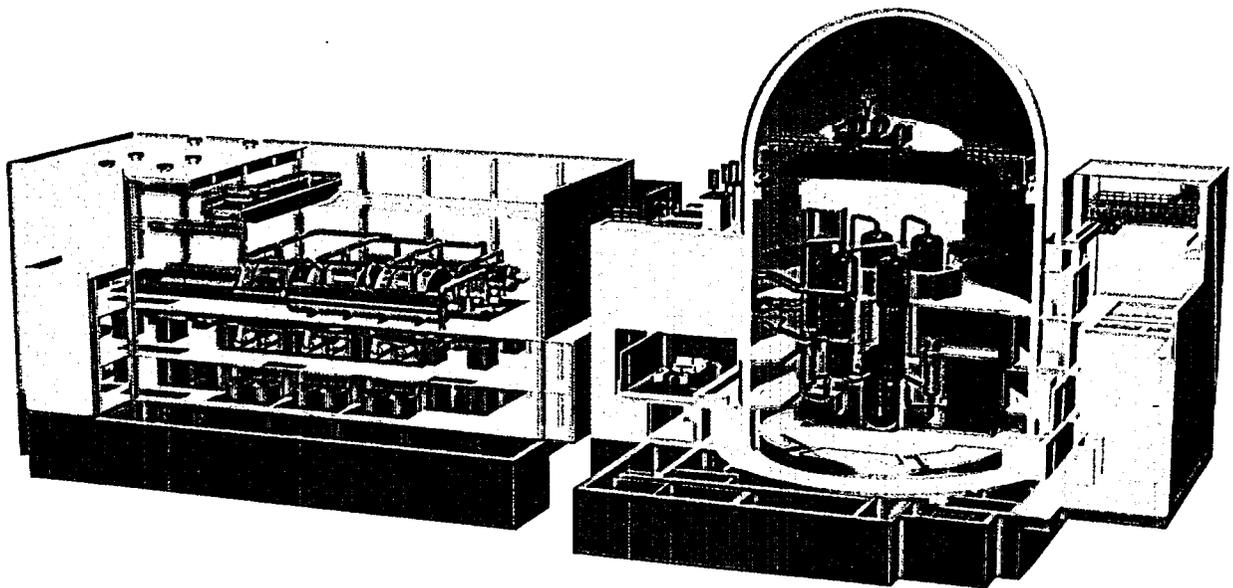
Portions of the report where proprietary information has been removed are identified by the designation “[ ]”.



Non-Proprietary

# US-APWR Topical Report

## Defense-in-Depth and Diversity



Doc. Number :  
MUAP-07006-NP R0

April 2007

 **MITSUBISHI HEAVY INDUSTRIES, LTD.**

©2007  
Mitsubishi Heavy Industries, Ltd.  
All Rights Reserved

## Defense-in-Depth and Diversity

Non Proprietary Version

April 2007

©2007 Mitsubishi Heavy Industries, Ltd.  
All Rights Reserved

**Revision History**

Revision	Page	Description
0	All	Original issued

© 2007  
**MITSUBISHI HEAVY INDUSTRIES, LTD.**  
All Rights Reserved

This document has been prepared by Mitsubishi Heavy Industries, Ltd. ("MHI") in connection with its request to the U.S. Nuclear Regulatory Commission ("NRC") for a pre-application review of the US-APWR nuclear power plant design. No right to disclose, use or copy any of the information in this document, other than by the NRC and its contractors in support of MHI's pre-application review of the US-APWR, is authorized without the express written permission of MHI.

This document contains technology 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 topical report describes Mitsubishi Heavy Industries' (MHI's) approach to Defense in Depth and Diversity (D3) for the Instrumentation and Control (I&C) systems applied to nuclear power plants. This approach includes design features and design processes that minimize the potential for Common Cause Failure (CCF) in the digital safety systems, and a diverse backup system to cope with a CCF that occurs concurrent with an Anticipated Operational Occurrence (AOO) or Postulated Accident (PA). The MHI D3 approach includes best estimate analysis methods to demonstrate this coping capability.

MHI seeks U.S. Nuclear Regulatory Commission (NRC) approval of the D3 approach for the US-APWR and for replacement of current safety systems in operating plants. The D3 approach, including the diverse backup system, was developed by MHI for nuclear power plants in Japan. For applications in the U.S., this topical report demonstrates conformance of the D3 approach to applicable U.S. Codes and Standards. These include:

- Code of Federal Regulations
- Regulatory Guides
- NUREG-Series Publications
- IEEE-Standards

MHI's fully computerized I&C system provides significant benefits to the safety of nuclear power plants, such as reduction of operations and maintenance work load, which reduces the potential for human error. Based on experience in Japan, MHI's digital I&C systems improve the reliability and availability for plant operation. The MHI Safety I&C System Description and Design Process are described in a separate topical report.

The Plant Control and Monitoring System (PCMS) and Protection and Safety Monitoring System (PSMS) utilize the MELTAC digital platform which is described in a separate topical report. Maximum utilization of a common digital platform throughout a nuclear plant reduces maintenance, training and changes due to obsolescence, thereby minimizing the potential for human error. The potential for CCF in these systems is minimized due to the simplicity of their basic design, the maturity of the MELTAC platform (based on operation in Japan), MHI's design process, including the elevated quality programs applied to both systems, and the significant functional diversity within the numerous computers that compose these systems.

Regardless of this very low potential for CCF, the Diverse Actuation System (DAS) is provided to accommodate beyond design basis CCFs that could adversely affect the PSMS and PCMS concurrent with an AOO or PA. The DAS provides diverse automatic actuation for time critical functions and diverse Human System Interface (HSI) to allow the operator to monitor critical safety functions and manually actuate safety process systems.

This topical report provides the design basis and system description of the MHI's DAS. It provides a Diversity Analysis to demonstrate the MHI's DAS has adequate diversity from the digital PSMS, which contains the Reactor Trip System (RTS) and Engineering Safety Features Actuation System (ESFAS), and is therefore not subject to any CCFs that may adversely effect those systems. This topical report also describes the D3 Coping Analysis method. The D3 Coping Analysis uses best estimate methods to demonstrate adequate coping capability,

which includes utilization of the DAS, for an AOO or PA that may occur concurrent with a CCF in the PSMS.

The information provided in this topical report describes the D3 designs and design process for the US-APWR. MHI expects to apply these same designs and design processes to upgrades in operating plants, with minor changes to accommodate plant specific configurations. Those changes would be described in specific Plant Licensing Documentation. The design basis, analysis and system description are generically applicable to all applications. The D3 Coping Analysis for specific plants, which is based on the generic methods described in this topical report, is provided in Plant Licensing Documentation.

MHI's I&C systems take advantage of capabilities within digital technology that were not available for analog systems. Therefore this document puts special emphasis on the explanation of these aspects of the design and their conformance to codes and standards. The following are key examples of these areas:

- a. Integrated RTS&ESFAS with functional diversity
- b. CCF modes for D3 analysis
- c. Credit for leak detection in D3 Analysis
- d. Common Power Interface (PIF) modules for PSMS/PCMS and DAS

MHI specifically seeks NRC approval of the design aspects for these areas.

This topical report distinguishes descriptions applicable to the US-APWR and descriptions for operating plants, where there is a clear need for this distinction. Where there are no distinctions, the description is generically applicable to the US-APWR and a broad range of operating plants, although not necessarily all operating plants. When this topical report is referenced for a plant specific Licensing Amendment Request, the Plant Licensing Documentation will identify any areas of this topical report that are not applicable.

The complete MHI digital I&C design is described in four topical reports:

- Safety I&C System Description and Design Process
- Safety System Digital Platform - MELTAC -
- HSI System Description and HFE (Human Factor Engineering) Process
- Defense-in-Depth and Diversity (this topical report)

This document identifies the additional Defense-in-Depth and Diversity related information to be submitted for NRC approval in future Plant Licensing Documentation. This Plant Licensing Documentation, in combination with the contents of this topical report and the contents of the other topical reports identified above, is expected to be sufficient to allow the NRC to make a final safety determination. Other documentation generated during the design process is available for NRC audit, as may be needed to allow the NRC to fully understand the D3 design.

## Table of Contents

List of Tables  
List of Figures  
List of Acronyms

1.0 PURPOSE.....	1
2.0 SCOPE.....	1
3.0 CODES AND STANDARDS.....	2
3.1 Code of Federal Regulations.....	2
3.2 Staff Requirements Memoranda.....	4
3.3 NRC Regulatory Guides.....	4
3.4 NRC Branch Technical Positions.....	6
3.5 NUREG-Series Publications (NRC Reports).....	6
3.6 IEEE Standards.....	7
4.0 I&C SYSTEM OVERVIEW.....	8
4.1 Comparison of Echelons to Regulatory Guidance.....	10
5.0 BASIC DEFENSE-IN-DEPTH AND DIVERSITY PRINCIPLES.....	13
5.1 Basic Principle 1- Defenses to Minimize the Potential for CCF.....	13
5.2 Basic Principle 2 - Coping with CCF for AOOs.....	14
5.3 Basic Principle 3 - Coping with Software CCF for Postulated Accidents.....	14
5.4 Basic Principle 4 - Extent of the Software CCF.....	15
5.5 Basic Principle 5 - Effects of the Software CCF.....	15
5.6 Basic Principle 6- Potential for Adverse Interaction.....	16
6.0 DAS DESCRIPTION.....	17
6.1 Functional Design Features.....	19
6.2 System Design Features.....	24
6.2.1 Overall Design.....	24
6.2.2 Diverse Automatic Actuation Cabinet (DAAC).....	26
6.2.3 Diverse HSI Panel (DHP).....	31
6.2.4 PIF Module.....	33
7.0 DIVERSITY ANALYSIS.....	35
7.1 Guideline 1: Choosing Blocks.....	35
7.2 Guideline 2: Determining Diversity.....	35
7.2.1 Design Diversity.....	35
7.2.2 Equipment Diversity.....	36
7.2.3 Functional Diversity.....	36
7.2.4 Human Diversity.....	36
7.2.5 Signal Diversity.....	36
7.2.6 Software Diversity.....	36
7.3 Guideline 3: System Failure Types.....	37
7.3.1 Type 1 Failure.....	37
7.3.2 Type 2 Failure.....	37
7.3.3 Type 3 Failure.....	37
7.4 Guideline 4: Echelons of Defense.....	37
7.5 Guideline 5: Method of Evaluation.....	38
7.6 Guideline 6: Postulated CCF of Blocks.....	38
7.7 Guideline 7: Use of Identical Hardware and Software Modules.....	38
7.8 Guideline 8: Effect of Other Blocks.....	38

---

7.9	Guideline 9: Output Signals .....	39
7.10	Guideline 10: Diversity for the AOO .....	39
7.11	Guideline 11: Diversity for the PA.....	39
7.12	Guideline 12: Diversity Among Echelons of Defense .....	39
7.12.1	Control/Reactor Trip Interaction .....	39
7.12.2	Control/ESFAS Interaction .....	39
7.12.3	Reactor Trip/ESFAS Interaction .....	39
7.13	Guideline 13: Plant Monitoring.....	40
7.14	Guideline 14: Manual Operator Action.....	40
8.0	D3 COPING ANALYSIS METHOD .....	41
8.1	Event Analysis Method .....	41
8.2	Manual Action Analysis Method.....	42
8.3	Treatment of Large Break LOCA .....	43
9.0	KEY TECHNICAL ISSUES .....	44
9.1	Integrated RPS & ESFAS with Functional Diversity .....	44
9.2	CCF Modes for Defense-in-Depth and Diversity Analysis .....	45
9.3	Credit for Leak Detection in Defense-in-Depth and Diversity Analysis .....	45
9.4	Common PIF Modules for PSMS/PCMS and DAS.....	45
10.0	FUTURE LICENSING SUBMITTALS.....	46
11.0	REFERENCES.....	47
Appendix A Conformance to BTP HICB-19.....		48
Appendix B Conformance to 10 CFR 50.62.....		50

## List of Tables

Table 4.1-1	Matrix for I&C Echelons of Defense	...11
Table 4.1-2	Assignment of I&C Equipment to Defense-in-Depth Echelons	...12
Table 6.1-1	Critical Safety Functions and Related System	...19
Table 6.1-2	Expected Time for System Action for Each Event	...20
Table 6.1-3	DAS Safety Function and Typical Components	...21
Table 6.1-4	Typical Monitoring Variables for DAS	...22
Table 9.1-1	Diverse Parameters in Two Separate Controller Groups	...44
Table 10.0-1	Future Licensing Submittals	...46

---

## List of Figures

Figure 4.0-1	The Overall Architecture of the I&C System	...9
Figure 6.0-1	The DAS System Architecture	...18
Figure 6.1-1	The DAS Functional Logic Diagram	...23
Figure 6.2-1	Configuration of the DAS Alarms	...28
Figure 6.2-2	The Signal Flow of the Status Signal	...28
Figure 6.2-3	The Prevention Diagram of Reactor Trip, Turbine Trip and MFW Isolation	...29
Figure 6.2-4	The Prevention Diagram of Emergency Feedwater	...30
Figure 6.2-5	The Signal Interface of the PIF Module	...34
Figure B-1	The Diversity between the Reactor Trip and Diverse Turbine Trip/EFW Actuation	...52
Figure B-2	The Diversity between the Reactor Trip and Diverse Reactor Trip	...52

## List of Acronyms

ALR	Automatic Load Regulator
AOO	Anticipated Operational Occurrence
ATWS	Anticipated Transient Without Scram
AVR	Auto Voltage Regulator
CCF	Common Cause Failure
CRDM	Control Rod Drive Mechanism
D3	Defense in Depth and Diversity
DAAC	Diverse Automatic Actuation Cabinet
DAS	Diverse Actuation System
DCD	Design Control Document
DHP	Diverse HSI Panel
ECCS	Emergency Core Cooling System
EFWS	Emergency Feed Water System
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Feature Actuation System
FLB	Feedwater Line Break
HFE	Human Factor Engineering
HSI	Human System Interface
HSIS	Human System Interface System
I&C	Instrumentation and Control
IPL	Interposing Logic
ITAAC	Inspection, Tests, Analysis and acceptance criteria
LBLOCA	Large Break Loss Of Coolant Accident
LOCA	Loss Of Coolant Accident
M/G	Motor-Generator
MCR	Main Control Room
MELCO	Mitsubishi Electric Corporation
MFWS	Main Feed Water System
MHI	Mitsubishi Heavy Industries
MSLB	Main Steam Line Break
PA	Postulated Accident
PCMS	Plant Control and Monitoring System
PDF	Probability of Failure on Demand
PIF	Power Interface
PRA	Probabilistic Risk Assessment
PSMS	Protection and Safety Monitoring System
QA	Quality Assurance
RCS	Reactor Coolant System
RPS	Reactor Protection System
RTS	Reactor Trip System

SBLOCA	Small Break Loss Of Coolant Accident
SGTR	Steam Generator Tube Rapture
SLS	Safety Logic System
SSE	Safe Shutdown Earthquake
TMI	Three Mile Island
UPS	Uninterrupted Power Supply
VDU	Visual Display Unit

## 1.0 PURPOSE

The purpose of this topical report is to describe the Mitsubishi Heavy Industries' (MHI's) approach to Defense in Depth and Diversity (D3) for Instrumentation and Control (I&C) systems. MHI seeks approval from the U.S. Nuclear Regulatory Commission (NRC) for the use of the MHI designs and design processes related to Defense in Depth and Diversity for new nuclear power plants and for operating nuclear power plants.

The design basis, system descriptions and analysis method are directly applicable to the MHI US-APWR. For operating plants the basic design features that ensure regulatory compliance are maintained, as described in this topical report. However, due to plant differences, specific changes in implementation detail will be described in Plant Licensing Documentation (e.g. License Amendment Request or Final Safety Analysis Report).

## 2.0 SCOPE

In this topical report the design basis of the D3 approach is described. The safety system and diverse actuation system described in this topical report are referred to as the Protection and Safety Monitoring System (PSMS) and the Diverse Actuation System (DAS), respectively. The descriptions of the PSMS and DAS functions such as automatic or manual initiating parameters, indication variables and assumptions in the D3 Coping Analysis and safety analysis should be considered typical. NRC approval of this topical report should be based on these descriptions. Any changes to the descriptions of these functions are described in Plant Licensing Documentation.

This topical report describes the diversity within the safety and non safety I&C systems. The DAS is provided as a defensive measure to cope with an Anticipated Operational Occurrence (AOO) or Postulated Accident (PA) concurrent with a Common Cause Failure (CCF) in the PSMS, which is a beyond design basis event. The DAS includes automatic and manual actuation. MHI seeks approval for the combined Defense in Depth and Diversity provided through the PSMS and DAS. The Plant Control and Monitoring System (PCMS) is described in this topical report only to the extent necessary to understand the impact a CCF may have on the PCMS and the effect of that CCF on coping with an AOO or PA.

The overall architecture of the MHI I&C system, and the PSMS description and design process are described in the Safety I&C System Topical Report. This topical report expands the system description of the DAS and describes the overall approach to Defense in Depth and Diversity.

### 3.0 CODES AND STANDARDS

This section identifies compliance to applicable codes, standards and conformance with applicable NRC guidance, as appropriate. Unless specifically noted, the latest version issued on the date of this document is applicable. The following terminology is used in this section:

**Plant Licensing Documentation** – This refers to plant level documentation that is specific to a group of plants or a single plant, such as the Design Control Document (DCD), Combined Operating Licensing Application, Final Safety Analysis Report, or License Amendment Request.

**DAS** – This refers the components that are the main subject of this topical report. This section emphasizes the applicable code, standards and regulatory guidance for the DAS and design processes related to Defense in Depth and Diversity. The applicable code, standards and regulatory guidance for the safety digital I&C system is described in the Safety I&C System Topical Report.

#### 3.1 Code of Federal Regulations

##### (1) 10 CFR 50 Appendix A: General Design Criteria for Nuclear Power Plants

- GDC 1 : Quality Standards and Records  
The Quality Assurance (QA) program meets the requirements of 10 CFR 50 Appendix B.
- GDC 2 : Design Bases for Protection against Natural Phenomena  
The safety systems described in this topical report are protected or qualified against natural phenomena. The DAS described in this topical report is non-safety system. It is located within building structures that provide protection against natural phenomena.
- GDC 4 : Environmental and Dynamic Effects Design Bases  
The DAS is located in a mild environment that is not adversely effected by plant accidents.
- GDC 5 : Sharing of Structures, Systems, and Components  
In general, there is no sharing of the DAS among nuclear power units.
- GDC 13 : Instrumentation and Control  
Typical I&C functions implemented within the DAS are described in this topical report. Specific I&C functions implemented within the DAS are described in Plant Licensing Documentation.
- GDC 17 : Electric Power Systems  
The electric power sources for the DAS and the plant components controlled by the DAS are discussed in Plant Licensing Documentation. This topical report describes the interface requirements for these power sources.

**GDC 19 : Control Room**

The DAS includes the Diverse Human System Interface Panel (DHP) in the Main Control Room (MCR). Human Factors Engineering (HFE) aspects of the DHP and the MCR are described in the Human System Interface (HSI) System Topical Report.

**GDC 24 : Separation of Protection and Control Systems**

The DAS is a non-safety system. Redundant divisions of the PSMS are physically and electrically isolated from the DAS. Where safety sensors are shared between the DAS and the PSMS, isolation modules in the PSMS prevents adverse interaction with the safety functions due to DAS failures.

**GDC 29 : Protection against Anticipated Operational Occurrences**

The PSMS provides the primary protection against AOOs. The DAS provides backup protection for AOOs through equipment that is diverse from the PSMS and therefore not subject to CCFs that may adversely affect the safety systems.

**(2) 10 CFR 50.34 (f)(2) Post-TMI (Three Mile Island) Requirements****• (iii) Control Room**

The Human Factors design aspects of the DAS HSI located within the MCR are described in the HSI System Topical Report.

**• (iv) Safety Parameter Display**

The DAS panel in the MCR provides indicators for key parameters that are indicative of the status of each critical safety function.

**(3) 10 CFR 50.36 Technical Specifications**

The DAS is not credited in the design basis for maintaining safety limits or control limits.

**(4) 10 CFR 50.49 Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants**

The DAS is a non-safety system located in a mild environment. A mild environment is an environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including AOOs. Therefore this criteria is not applicable.

**(5) 10 CFR 50.55a Codes and Standards****• (a)(1) Quality Standards for Systems Important to Safety**

The DAS was originally developed under a Japanese nuclear quality program that is equivalent to 10 CFR 50 Appendix B. Other licensing documents describe this equivalence. An approved 10 CFR 50 Appendix B quality program is now in effect for all Equipment.

**(6) 10 CFR 50.62 ATWS Rule**

The DAS is used to actuate Reactor Trip, Turbine Trip and Emergency Feedwater for Anticipated Transient Without Scram (ATWS) mitigation. The DAS also provides a diverse reactor trip function. The DAS is diverse from the reactor trip function in the PSMS, with

the exception of input sensors, which are shared by both systems. The conformance to this Code of Federal Regulations is described in Appendix B.

(7) 10 CFR 52.47

- (a)(1)(iv) Resolution of Unresolved and Generic Safety Issues
  - (a)(1)(vi) ITAAC in Design Certification Applications
  - (a)(1)(vii) Interface Requirements  
Conformance to the requirements in items iv thru vii, above, are described in Plant Licensing Documentation.
  - (a)(2) Level of Detail  
The content of this topical report, together with the additional information described in other I&C Topical Reports and Plant Licensing Documentation, is sufficient to allow the NRC staff to reach a final conclusion on all safety questions associated with the design. The information includes performance requirements and design information sufficiently detailed to permit the preparation of acceptance and inspection requirements by the NRC, and procurement specifications and construction and installation specifications by an applicant.
- (8) 10 CFR 52.79(c) ITAAC in Combined Operating License Applications  
The inspections, tests, analyses and acceptance criteria (ITAAC) that demonstrate that the DAS has been constructed and will operate in conformity with the Commission's final safety conclusion, will be described in the Plant Licensing Documentation.

### 3.2 Staff Requirements Memoranda

(1) SRM to SECY 93-087

- II.Q Defense against Common-Mode Failures in Digital Instrumentation and Control Systems  
Compliance for defense against CCF is described in this topical report.
- II.T Control Room Annunciator (Alarm) Reliability  
Alarm signals are generated directly from the DAS for input conditions that can lead to system actuation and for actuation of system outputs. These alarms are generated directly by the DAS. Therefore the alarms are not susceptible to a CCF that may affect the normal alarms which are generated from the digital safety and non-safety systems. This ensures operators are aware of abnormal plant conditions concurrent with a CCF in the digital safety systems. Alarms are also generated for DAS equipment failure, including failures that can lead to spurious DAS actuation. Summary alarms for DAS failures are also provided by the normal digital plant alarm system. These summary alarms ensure that operators are aware of failures in DAS equipment.

### 3.3 NRC Regulatory Guides

- (1) RG 1.22 Periodic Testing of Protection System Actuation Functions  
Although the DAS is a non-safety system all DAS functions can be tested.

- 
- (2) RG 1.29 Revision 3 Seismic Design Classification  
The DAS is designated Seismic Category II. Seismic Category II equipment is designed so that the Safe Shutdown Earthquake (SSE) will not cause a failure which will reduce the functioning of the safety function to an unacceptable level.
- (3) RG 1.62 Manual Initiation of Protective Actions  
All DAS functions related to reactor trip and maintaining critical safety functions can be manually initiated at the system level by conventional switches located on the DHP in the MCR. Typical functions are described in this topical report. Specific functions are described in Plant Licensing Documentation.
- (4) RG 1.75 Physical Independence of Electric Systems  
-endorses IEEE 384-1992  
Redundant safety divisions are physically and electrically independent of the DAS. Physical independence is maintained either by the required distance or by barriers which prevent propagation of fire or electrical faults. Electrical independence is maintained by conventional isolators, such as opto-couplers, relays or transformers. Conventional isolators include fault interrupting devices such as fuses or circuit breakers. Conventional isolators prevent propagation of transverse and common cause faults from the maximum credible energy source. Qualification of conventional isolators used for DAS interfaces with the safety systems are discussed in the Safety I&C System Topical Report.
- (5) RG 1.97 Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident  
-endorses IEEE Std. 497-2002  
The DAS provides diverse processing and display of signals from accident monitoring instrumentation to indicate the status of critical safety functions. Specific accident monitoring instrumentation is described in Plant Licensing Documentation.
- (6) RG 1.105 Setpoints for Safety-Related Instrumentation  
-endorses ISA-S67.04-1994 and ANS-10.4-1987  
Setpoints for DAS automatic actuation functions are determined based on nominal equipment uncertainties.
- (7) RG 1.118 Periodic Testing of Electric Power and Protection Systems  
-endorses IEEE 338-1987  
Although the DAS is a non-safety system, all DAS functions are testable. Many component failures within the DAS, such as power supply failure, are alarmed.
- (8) RG 1.151 Instrument Sensing Lines  
-endorses ISA-S67.02  
Compliance is described in Plant Licensing Documentation.
- (9) RG 1.152 Criteria for Programmable Digital Computers in Safety Systems of Nuclear Power Plants  
-endorses IEEE 7-4.3.2-2003  
The DAS is an analog system. Therefore this regulatory guide is not applicable.
- (10) RG 1.180 Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C Systems
-

---

-endorses MIL-STD-461E, IEC 61000 Parts 3, 4, and 6, IEEE Std C62.41-1991, IEEE Std C62.45-1992, IEEE Std 1050-1996

The DAS is a non-safety analog system. The design encompasses historical design practices that have proven to be adequate for immunity to EMI (Electro-Magnetic Interface) and RFI (Radio Frequency Interface).

### 3.4 NRC Branch Technical Positions

- (1) BTP HICB-8 Guidance for Application of Regulatory Guide 1.22  
All functions of the DAS are testable.
- (2) BTP HICB-11 Guidance on Application and Qualifications of Isolation Devices  
-endorses IEEE Std 472, ANSI Std C62.36, ANSI Std C62.41, ANSI Std C62.45  
See compliance to RG 1.75. Isolation devices are qualified in compliance to these standards.
- (3) BTP HICB-12 Guidance on Establishing and Maintaining Instrument Setpoints  
Setpoint calculations for DAS automatic actuation functions consider nominal equipment accuracies.
- (4) BTP HICB-16 Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52  
See compliance to 10 CFR 52.47. The level of detail needed for the NRC staff to make a final safety determination is described in Plant Licensing Documentation.
- (5) BTP HICB-17 Guidance on Self-Test and Surveillance Test Provisions  
See compliance to RG 1.22 and RG 1.118.
- (6) BTP HICB-19 Guidance on Evaluation of Defense in Depth and Diversity in Digital Computer Based I&C Systems  
The MHI safety digital I&C system, PSMS, utilize the Mitsubishi Electric Corporation (MELCO) safety digital I&C platform. The MHI non-safety digital I&C systems, PCMS, utilize the MELCO non-safety digital I&C platform. The two MELCO platforms are essentially the same, however some QA aspects of design and manufacturing are not equivalent between safety and non-safety platforms. This topical report describes the diversity within the safety and non-safety I&C systems. The report also describes the methodology for coping with an AOO or PA concurrent with a CCF that disables all of these systems. The conformance to this BTP is described in Appendix A. Coping for all AOOs and PAs is described in Plant Licensing Documentation.

### 3.5 NUREG-Series Publications (NRC Reports)

- (1) NUREG-0737, Supplement 1 Clarification of TMI Action Plan Requirements  
The DAS panel in the MCR, DHP, provides indicators for key parameters that are indicative of the status of each critical safety function.
- (2) NUREG-0800 Chapter 7 of the U.S. NRC Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Rev 4  
The DAS fulfills related requirements of this NUREG for monitoring and controlling plant

---

components. Descriptions of specific plant systems are described in Plant Licensing Documentation.

(3) NUREG/CR-6303 Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems

The design of the safety I&C system is described in the Safety I&C System Topical Report. The assessment of diversity between the safety I&C system and the DAS is described in this topical report. This topical report also describes the method of coping with CCF vulnerabilities.

### 3.6 IEEE Standards

(1) IEEE 379 2000 Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems

The DAS is a non-safety system, therefore it does not meet this standard for monitoring or actuation functions. However, the DAS is fully isolated from the safety systems so the DAS is not a source of single failure that can adversely affect the safety systems. In addition, the DAS is designed so that credible single failures, including failures resulting from fire and seismic events, will not cause spurious actuations that could adversely affect safety functions.

(2) IEEE 384 1992 Criteria for Independence of Class 1E Equipment and Circuits

The interface of the DAS to the safety systems conforms to this standard as augmented by RG 1.75. All safety functions are implemented within multiple divisions with physical separation and electrical independence between redundant safety divisions and between safety divisions and the DAS. Electrical independence between the DAS and the safety systems is accomplished primarily through the use of conventional isolators. Independence of electrical circuits is accomplished with isolators and physical separation or barriers, such as conduits.

#### 4.0 I&C SYSTEM OVERVIEW

Nuclear power plant instrumentation senses various plant parameters and transmits appropriate signals to the control systems during normal operation, and to the reactor trip and engineered safety feature (ESF) systems during abnormal and accident conditions. The 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 architecture of the Overall I&C System is shown in Fig. 4.0-1. The Overall I&C System consists of the following four echelons as illustrated in Fig. 4.0-1.

- 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 achieve high reliability as described in the Safety I&C System Topical Report. The HSI System encompasses the HSI provided by the PSMS, PCMS and DAS. The HFE aspects of the HSI system are described in the HSI System Topical Report.

For coping with an AOO or PA concurrent with a CCF in the PSMS and PCMS, the DAS provides monitoring of key safety parameters and back-up automatic/manual actuation of the safety and non-safety components required to mitigate AOOs and PAs. Where the time is insufficient for manual operator action, the DAS provides automatic actuation of the plant safety functions needed for accident mitigation.

The DAS consists of conventional analog and digital components that are diverse from the MELTAC Platform which is used in the PSMS and PCMS. A postulated CCF that adversely affects these digital systems will not also impair the DAS function.

The DAS is classified as a non-safety system. Interfaces from the process inputs of Reactor Protection System (RPS) and interfaces to the outputs of Safety Logic System (SLS) are isolated within the PSMS.

The DAS includes internal redundancy to prevent spurious actuation of automatic and manual functions due to single component failures. The DAS is also designed to prevent spurious actuations due to postulated earthquakes and postulated fires, so there is no adverse interaction with safety functions.

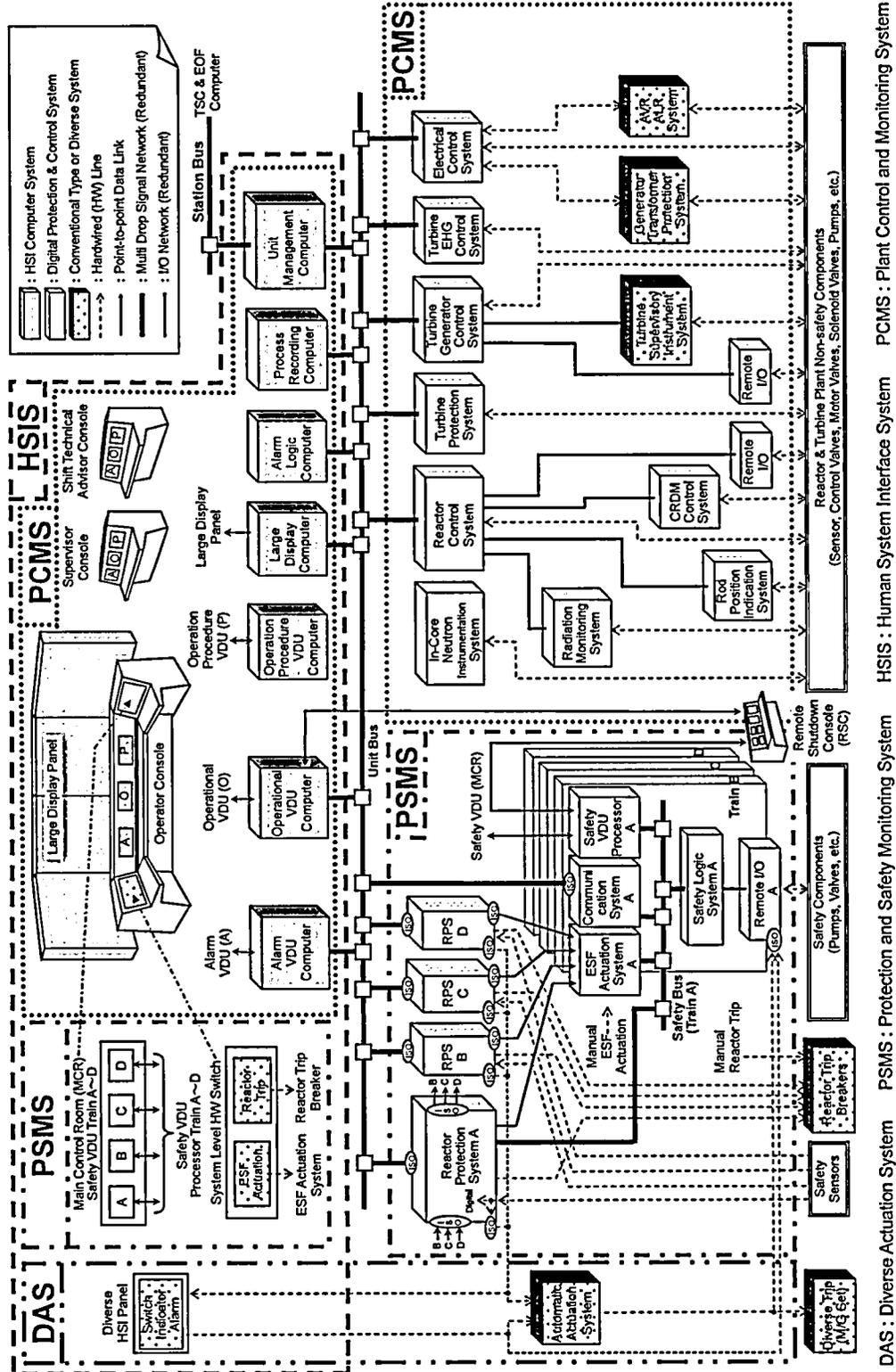


Figure 4.0-1 The Overall Architecture of the I&C System

#### 4.1 Comparison of Echelons to Regulatory Guidance

MHI's overall I&C system is categorized into four echelons, these are the HSIS, PSMS, PCMS and DAS.

BTP-19 and NUREG 6303 describe echelons of defense. These echelons corresponded to MHI's system as follows:

*Definitions as stated in BTP-19 are in Italics.*

- ***Control System - The control system echelon consists of non-safety equipment that routinely prevents reactor excursions toward unsafe regimes of operation and is used in the normal operation of the reactor.***

The reactor control functions performed by the control system echelon of defense are included in the non-safety PCMS. The PCMS includes functions to maintain the plant within operating limits to avoid the need for reactor trip or ESF actuation.

- ***Reactor Trip System - The RTS echelon consists of safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.***

The automatic reactor trip functions performed by the Reactor Trip System (RTS) echelon of defense are included in the safety PSMS. The non-safety DAS also provides diverse automatic reactor trip for accidents where there is insufficient time for manual reactor trip.

- ***Engineered Safety Features Actuation System - The ESFAS echelon consists of safety equipment that removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel, and containment).***

The automatic ESF actuation functions performed by the Engineered Safety Features Actuation System (ESFAS) echelon of defense are included in the safety PSMS. The non-safety DAS also provides diverse automatic ESF actuation for accidents where there is insufficient time for manual ESF actuations.

- ***Monitoring and Indicators - The monitoring and indicators echelon consists of sensors, displays, data communication systems, and manual controls required for operators to respond to reactor events.***

The monitoring and indication functions are provided by the HSIS which includes the HSI from the PSMS, PCMS and DAS. The safety monitoring, manual reactor trip and manual ESF actuation functions are included in the PSMS. The non-safety PCMS provides monitoring and manual controls to maintain operating limits during normal plant operation. The non-safety DAS provides monitoring, manual reactor trip and manual ESF actuation that is diverse from the PSMS and PCMS.

Table 4.1-1 maps the echelons of defense in the I&C system. The echelons are divided into the non-safety, the safety and diverse defense. Table 4.1-2 also illustrates the relationship between these subsystems and cabinets and the block structure. This table shows the assignment of equipment to the blocks for each level within the echelons of defense.

Table 4.1-1 Matrix for I&amp;C Echelons of Defense

	Defense 1 Non-Safety System	Defense 2 Safety System	Defense 3 Diverse System
Control System Echelon	PCMS <sup>Note1&amp;2</sup>		
RTS Echelon		PSMS <sup>Note2</sup>	DAS <sup>Note2</sup>
ESFAS Echelon		PSMS <sup>Note2</sup>	DAS <sup>Note2</sup>
Monitoring and Indicators Echelon	PCMS <sup>Note1&amp;2</sup>	PSMS <sup>Note2</sup>	DAS <sup>Note2</sup>
		Class 1E	

Note 1: The PCMS enables the plant to maintain conditions within operating limits and also provides automatic and manual actuations of the non-safety systems.

Note 2: Automatic and manual actions are provided in the PSMS, PCMS, and DAS.

Table 4.1-2 Assignment of I&amp;C Equipment to Defense-in-Depth Echelons

Echelon	Defense	Measured and Derived Variable Blocks	Command Block	Manual Actions
Control System Echelon	Non-safety System (PCMS)	Sensors, Signal Conditioning, (Communication Function in PSMS) <sup>Note1</sup>	Real-time Network, Output Signal Conditioning, Output Module/PIF Module	System Level Soft Control as Determined by HSI Design; Component Level Soft Control
	Safety System (PSMS)	N/A	N/A	N/A
	Diverse System (DAS)	N/A	N/A	N/A
RTS Echelon	Non-safety System	N/A	N/A	N/A
	Safety System	Sensors, Signal Conditioning, RPS Subsystem	Voting Logic, Output Module, Reactor Trip Switchgear	Hardwired Manual Reactor Trip to Reactor Trip Breakers
	Diverse System	Sensors, Signal Conditioning	Diverse Analog Processing, PIF Module, Rod Drive M/G Set Trip	Hardwired Manual Reactor Trip to Rod Drive M/G Set
ESFAS Echelon	Non-safety System	N/A	N/A	Component Level Soft Control from PCMS VDU to PSMS
	Safety System	Sensors, Signal Conditioning, RPS Subsystem	ESF Coincidence Logic, Safety Bus, ESFAS/SLS Subsystem, PIF Module	System Level to ESF Coincidence Logic in ESFAS subsystem, Component Level Soft Control from PSMS VDU
	Diverse System	Sensors, Signal Conditioning,	Diverse Analog Processing, PIF Module	Hardwired Component Level
Monitoring and Indicators Echelon	Non-safety System	Sensors, Signal Conditioning, (Communication Functions in PSMS)	Real-time Network, Large Display Panel, Non-safety VDU for monitoring and control of non-safety and safety functions	See Other Three Echelons
	Safety System	Sensors, Signal Conditioning	Conventional switches for system level actuation, Safety VDU for monitoring and control	See Other Three Echelons
	Diverse System	Sensors, Signal Conditioning	Diverse HSI Panel for monitoring and control of safety functions	See Other Three Echelons

Note 1: Used for safety sensors that provide isolated information to non-safety systems.

## 5.0 BASIC DEFENSE-IN-DEPTH AND DIVERSITY PRINCIPLES

The Defense-in-Depth and Diversity approach is based on the following basic principles.

### 5.1 Basic Principle 1- Defenses to Minimize the Potential for CCF

GDC22 and IEEE 603-1991 impose requirements to ensure digital safety and non-safety I&C systems are designed to minimize the potential for CCFs.

Multiple defense-in-depth approaches are used in the MHI safety I&C system design to meet these requirements and thereby minimize the potential for CCF. These approaches are described in detail in the Safety I&C System Topical Report. The key defense-in-depth approaches are summarized as follows:

- A safety system QA process that meets the requirements of 10 CFR 50 Appendix B is used to minimize the potential for system design errors, implementation errors and maintenance errors.
- A safety software QA process that meets the life cycle requirements of IEEE 7-4.3.2-2003 is used to minimize the potential for software design errors, implementation errors and maintenance errors.
- A safety equipment qualification process that meets the requirements of IEEE 323-2003 is used to eliminate the potential for CCF induced by external environmental conditions.
- Non-safety control systems are used to maintain critical safety functions within acceptable operating limits and independent safety systems are used to maintain critical plant safety functions within acceptable safety limits, if the operating limits are exceeded. The safety and non-safety systems provide diverse means for controlling each critical safety function. For example (1)Reactor Coolant System (RCS) inventory is controlled by the Chemical & Volume Control System (CVCS) from the PCMS and by the Safety Injection System (SIS) from the PSMS, (2)RCS heat removal is controlled by the Main Feedwater System (MFWS) from the PCMS and by the Emergency Feedwater System (EFWS) from the PSMS.
- Operators have the ability to interact through non-safety systems to monitor the plant and take manual control actions to maintain operating limits. Should operating limits be exceeded, operators have the ability to interact through non-safety systems and safety systems to monitor the plant and take manual actions to maintain plant safety limits.
- Safety systems contain multiple redundant divisions to achieve high reliability. In accordance with IEEE 384-1992 and IEEE 7-4.3.2-2003 independence is provided between safety divisions and between safety and non-safety systems to ensure random single failures do not result in CCFs that effect multiple safety divisions.
- Two functionally diverse means of controlling critical safety functions are provided within the control systems (e.g. reactivity control by control rods and boron concentration in the reactor coolant system).
- Within each redundant division of the safety systems two functionally diverse means are provided to detect AOOs and PAs, and to initiate required protective actions. Within each redundant division of the safety systems, these diverse detection functions are implemented within separate subsystems to minimize the potential for a CCF that could adversely affect both diverse functions.
- There are independent Reactor Trip Circuit Breakers for each safety division. Within each breaker, there are two diverse means of opening the breaker. One means is based on de-

energizing the under voltage coil, and the other means is by energizing the shunt trip coil. Both means are qualified as Class 1E safety related functions.

- The PSMS and PCMS utilize the MELTAC digital platform. This platform employs a very simple single task operating system and no external interrupts, which results in completely cyclical and deterministic performance. The MELTAC platform has demonstrated many years of error free performance in Japanese nuclear power plants. Therefore there is minimum potential for a CCF within the MELTAC platform hardware or operating system.

The defense-in-depth approaches, described above, reduce the probability of CCFs in the PSMS and PCMS to a sufficiently low level where they do not need to be considered as single failures and are therefore not considered in the plant safety analysis. This is consistent with the Staff Requirements Memorandum to SECY 93-087, which states "common-cause failures are beyond design basis events".

### 5.2 Basic Principle 2 - Coping with CCF for AOOs

The defensive measures described above reduce the potential for CCF to a level considered low enough to meet overall plant safety goals for low probability Postulated Accidents. However, for higher probability AOOs 10 CFR 50.62 requires equipment diversity as an additional defense in depth measure. This additional defensive measure is required by 10 CFR 50.62 to cope with the potential CCFs in the safety systems, regardless of their low probability.

In accordance with 10 CFR 50.62 the equipment diverse from the Reactor Trip system is provided to initiate Turbine Trip and Emergency Feedwater. Although not required for all reactors, MHI's D3 approach also includes a diverse reactor trip function. The DAS is used to actuate Reactor Trip for ATWS mitigation. Equipment diversity applies to all aspects of the equipment used to detect AOOs and actuate required protective actions. This includes hardware and software, however it excludes sensors. Sensors are commonly used in the safety systems for which the CCF is postulated and the system(s) used to provide diverse backup protection.

### 5.3 Basic Principle 3 - Coping with Software CCF for Postulated Accidents

The defense-in-depth approaches described in the Basic Principle 1 have shown to reduce the probability of CCFs for analog safety systems to a level that is sufficiently low to meet plant safety goals for Postulated Accidents, which are also very low probability. This is because most conditions that could lead to CCFs in analog systems have been caused by slow processes such as corrosion and equipment wearing out, which can be identified by an operator in sufficient time to prevent the ensuing CCF.

However, the NRC believes the ability to identify all software errors during the system development phase has become especially problematic due to the inherent complexity of digital systems. Hidden software errors may continue to remain undetected during system operation and therefore may result in CCFs that ultimately affect multiple systems within a relatively short time duration.

Consequently, HICB BTP-19 establishes additional guidance for identifying potential software CCFs for digital safety I&C systems and analyzing their effects. In addition, BTP-19 establishes guidance to ensure the ability to cope with an AOO or PA concurrent with these

software CCFs, through plant systems that are not subject to the CCF (i.e. diverse plant systems).

The guidance and acceptance criteria in BTP-19 recognize that, based on its low probability, a CCF is a beyond design basis event. Therefore coping methods for an AOO or PA in conjunction with a CCF include all diverse plant systems (safety, non- safety, automatic and manual) of suitable quality.

Since a software CCF is a beyond design basis event, adequate coping is judged based on best estimate analysis methods, including nominal initial plant conditions, concurrent failure assumptions and acceptance criteria that are relaxed compared to the Chapter 15 safety analysis methods for the same AOOs and PAs. The following areas exemplify key concurrent failure assumptions for MHI's best estimate D3 Coping Analysis:

- A single failure, in addition to the CCF, does not need to be postulated.
- A loss of offsite power source does not need to be postulated other than the case where this is the initiating event.
- Concurrence of an AOO or PA, and an earthquake does not need to be considered.

The final requirement in BTP-19, intended to ensure adequate coping capability for AOOs and PAs in conjunction with software CCFs in the PSMS is the provision for diverse manual monitoring of critical safety functions and diverse manual system level actuation of systems used to maintain those critical safety functions. This requirement is met regardless of the ability to demonstrate adequate coping through automated systems.

#### **5.4 Basic Principle 4 - Extent of the Software CCF**

In the MHI I&C design, the digital control and protection systems are controlled by the MELTAC digital platform. There is significant functional diversity within the control systems, within the safety systems and between the control and safety systems. This functional diversity may be credited in demonstrating that the effects of postulated software CCFs are limited. However, to be very conservative MHI conducts the D3 Coping Analysis based on the assumption that the CCF affects all digital control and protection systems in their entirety and that all the control and safety functions controlled by the MELTAC platform are disabled.

#### **5.5 Basic Principle 5 - Effects of the Software CCF**

BTP-19 requires consideration of CCFs that "disable" the protection system. Based on this, the D3 Coping Analysis considers CCFs that result in a fail-as-is condition in the PSMS and PCMS. The D3 Coping Analysis does not consider CCFs that result in output state changes (i.e., spurious actuation to the de-energized or energized state).

The basis for this is that the PSMS and PCMS employ fixed cyclical deterministic processing through a very simple single task operating system and with very simple application functions. These functions are tested through an extensive software QA program. As a result the systems will not react differently during an AOO or PA than they react every day. Based on this, it can be concluded that the designs minimize the probability of CCFs induced by changing input conditions. Therefore it is reasonable to assume that for the PSMS and PCMS, the software CCF postulated for BTP-19 is not induced by the AOO or PA, but rather by an undetected hidden defect. An undetected hidden defect that results in fail-as-is conditions may

affect multiple systems over time and may still exist when an AOO or PA occurs. Therefore this defect is considered concurrent with an AOO or PA. However a hidden defect that results in output state changes is immediately detectable by operators. Operators can correct this defect before it affects multiple systems and prior to an AOO or PA. Therefore, a CCF that results in spurious actuation concurrent with an AOO or PA is not considered in the D3 Coping Analysis.

Software defects that result in spurious actuation during normal operation are immediately detectable by operators. Therefore, the software defect can be corrected in all systems before it becomes a CCF that affects multiple systems. Software defects that result in spurious actuation of individual systems are bounded by the AOOs which are considered in the safety analysis and considered in the D3 Coping Analysis.

#### **5.6 Basic Principle 6- Potential for Adverse Interaction**

Diverse equipment provided to cope with common CCFs in digital safety systems does not prevent plant safety and does not affect plant operability. Diverse equipment is isolated and is independent from the safety systems so that the diverse equipment cannot be a source of single failure that would degrade multiple safety divisions or result in spurious actuation of multiple safety divisions. The diverse equipment design ensures spurious actuations that may result from fire, do not interfere with multiple divisions of plant safety systems. The diverse equipment design ensures spurious actuations do not result from seismic events. Diverse equipment is designed with sufficient redundancy and reliability so that the diverse equipment cannot be a source of single failure that would adversely effect plant operation.

For the prevention of unnecessary diverse action, the diverse actuation signal is automatically blocked (e.g. on-delay timer for diverse actuation and interlock signal from component status) if the digital safety and non-safety systems are normally actuated without CCF. The diverse actuation is also manually blocked (e.g. block switches) during plant start up and shutdown conditions. These interlocks and blocks are included in the diverse actuation logic.

Finally, the potential for adverse interaction for both safety and plant operability is minimized by limiting the scale of diverse equipment to the minimum required to ensure plant safety on the basis of the best estimate methods used in the D3 Coping Analysis.

## 6.0 DAS DESCRIPTION

This section provides the system description for the DAS.

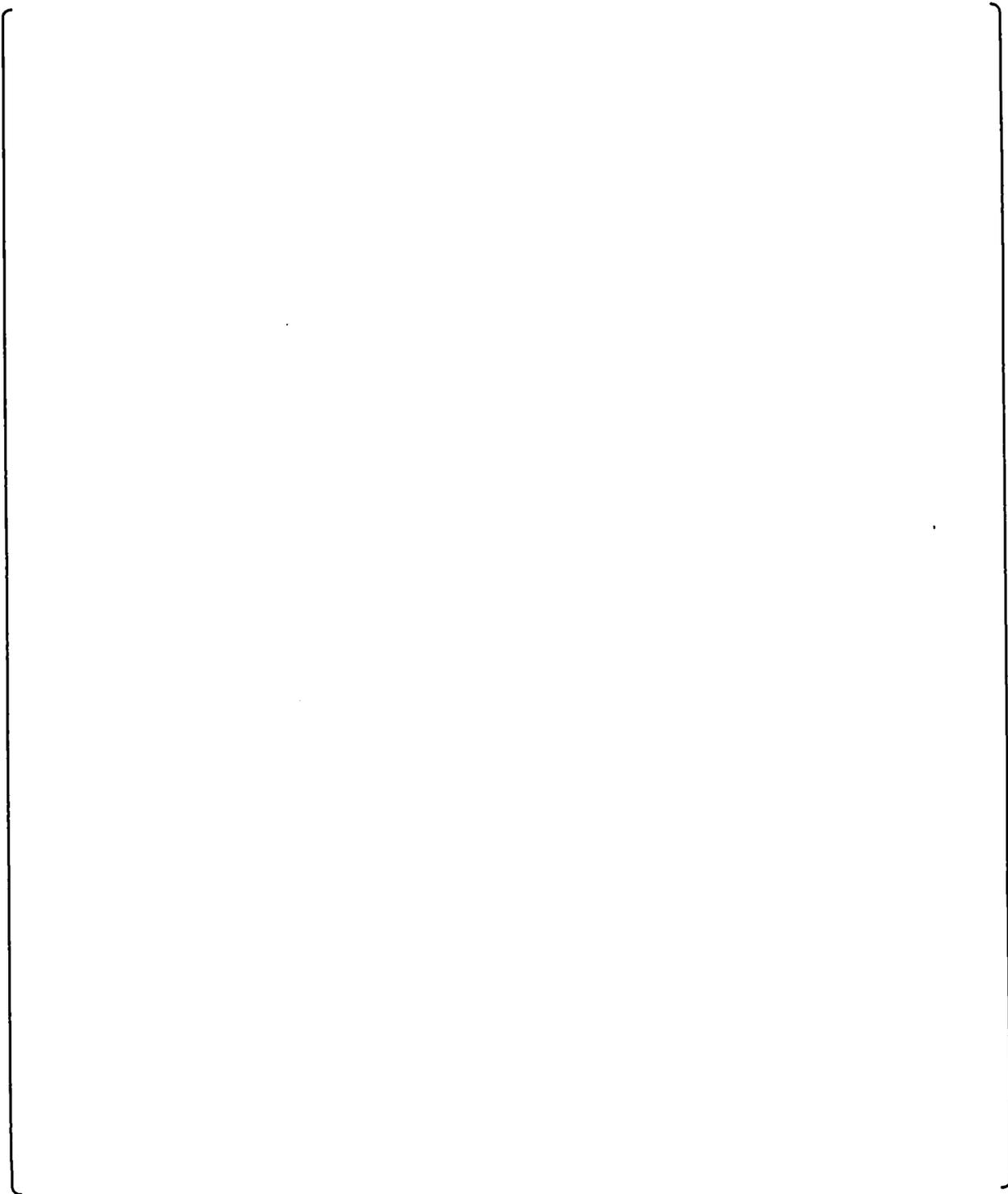
The non-safety DAS provides monitoring and control of safety related and non-safety related plant systems to cope with abnormal plant conditions concurrent with a CCF that disables all functions of the PSMS and PCMS. This section describes the interfaces of the DAS to the PSMS and PCMS and the HSI functions of the DAS that support plant safety.

Within the DAS, manual actuation is provided for all critical functions at the system level (e.g. reactivity level, core heat removal, reactor coolant inventory and containment isolation). Automatic actuation is also provided for functions where time for manual operator action is inadequate. These functional design features are described in section 6.1.

The system specifications for the DAS are described in this section. The overall DAS system architecture is shown in Fig. 6.0-1. The DAS consists of an automatic actuation function and a HSI function which includes a diverse leak detection function. These functions are in the Diverse Automatic Actuation Cabinet (DAAC), and Diverse HSI Panel (DHP), respectively.

These descriptions are provided in Section 6.2.2 for the DAAC and Section 6.2.3 for the DHP. The diverse leak detection function is also described in Section 6.2.3.

The DAS functions described in this section and shown on the figures of this section are for the US-APWR. These include automatic actuations, manual controls and indications for plant monitoring. Any changes to these DAS functions for other plants are described in Plant Licensing Documentation.



**Figure 6.0-1 The DAS System Architecture**

## 6.1 Functional Design Features

This section describes typical functional design features for DAS automation and HSI.

Critical safety functions and related individual systems assigned to the DAS are listed in Table 6.1-1. In this table, related systems are selected considering the plant design, event scenarios and design experiences for abnormal plant conditions in operating plants.

**Table 6.1-1 Critical Safety Functions and Related System**

Critical Safety Function	Related System
Reactivity Control	Reactor Trip Turbine Trip
RCS Inventory	ECCS (Emergency Core Cooling System)
Core Cooling	ECCS
Secondary Heat Sink	Emergency Feed Water System (EFWS) Isolation of Secondary System Secondary System Depressurization
RCS Integrity	Primary System Depressurization
Containment Integrity	Containment Isolation Containment Spray

The systems listed in Table 6.1-1 are required to operate at different times for different events. Table 6.1-2 shows the expected action time measured from the prompting alarms for various events.

These selected systems and expected action times establish the basis for DAS automation. The D3 Coping Analysis confirms the acceptability of DAS automation and credited manual operator action.

Table 6.1-2 Expected Time for System Action for Each Event

	AOO	SGTR	MSLB	FLB	SBLOCA	DAS Req.
Reactor Trip	A	A	A	A	A	A
(Turbine Trip)	A					A
Emergency Feed Water System	A	C	C	A	C	A
(Isolation of MFWS)	A	A	A			A
(Isolation of EFWS)		C	C	B		B
Emergency Core Cooling System		C			B	B
(Primary/Secondary Depressurize)		C				C
Isolation of Secondary System		C	C			C
Containment Spray System			C	C	C	C
Isolation of Containment Vessel					C	C

## Notes)

- A: need action within 10 minutes therefore DAS automation is provided.
- B: need action within 30 minutes therefore indications and manual controls are provided on the DHP.
- C: action after 30 minutes therefore indications and manual controls are provided outside the MCR.
- All times are from the first prompting alarm. The D3 Coping Analysis considers the additional time from the event initiation to the prompting alarm.
- AOOs are represented in a single column because most of them are terminated with reactor shutdown.
- For LBLOCA manual operator action is credited to safe shutdown of the plant based on the early indications from the diverse leak detection function described in Section 6.2.3.

Safety functions which have less than 10 minutes allowable time to actuate are automatically actuated by DAS. System level manual actuation is also provided on the DHP in the MCR for all automated functions. In addition, indications and manual controls are provided on the DHP for operating systems and components for which the allowable time for operation is less than 30 minutes. In addition, indications and manual controls are provided on the DHP to operate components which:

- should be operated frequently.  
(e.g. primary / secondary depressurization valves during SGTR)
- should be operated at the same time.  
(e.g. closure of containment isolation valves)

Manual operation that does not meet the requirements defined above is operated from outside the MCR by direct operation of local power distribution and switching devices which are not affected by the CCF in the PSMS.

All manual actions are supported by a HFE evaluation to ensure the feasibility of manual actions based on prompting alarms, monitoring information, available controls, and written procedures. Also, staffing and training will support the required action times. The HFE evaluation method is described in Section 8.2.

The associated components required for each critical safety function to be actuated by the DAS and for the type of actuation required are summarized in Table 6.1-3.

**Table 6.1-3 DAS Safety Function and Typical Components**

Safety Function / Associated Components	Number of Components	Actuation Type
Diverse Reactor Trip (M-G set trip)	2 M-G sets	Automatic
Turbine Trip	2 trip solenoids	Automatic
Turbine-Driven Emergency Feed Water Pump	2 pumps	Automatic
ECCS Pump	2 pumps	Manual (MCR)
Pressurizer Depressurization Valve	1 Valve	Manual (MCR)
Steam Generator Depressurization Valve	1 Valve / SG	Manual (MCR)
SG Blowdown Isolation Valve	1 Valve / SG	Automatic
Main Feed Water Control Valve (Close)	1 Valve / SG	Automatic
Emergency Feed Water Control Valve	1 Valve / SG	Manual (MCR)
Steam Line Isolation Valve	—	Manual (Local)
Containment Isolation Valves	1 Train	Manual (MCR)
Containment Spray Pump	—	Manual (Local)

The numbers of the required components in the above table are based on the following considerations:

- Maintain 100% of required capability of the safety function considering affected loop or SG for each accident without considering any single failure.

Automatic actuation parameters are determined from the plant design and event scenarios. These parameters are confirmed by the D3 Coping Analysis. Three actuation parameters are selected as follows:

- Pressurizer Pressure High: for pressurization events, excessive heating events, and power increasing events
- Pressurizer Pressure Low: for depressurization events, excessive cooling events, and power decreasing events.
- Steam Generator Water Level Low: for loss of secondary heat sink events.

The numbers of channels required for each Automatic actuation function are based on the following considerations.

- No single failure spuriously actuates the DAS.
- Unlimited bypass of a single channel does not cause the DAS automatic function to be inoperable, prevent decisions regarding credited manual actions or prevent monitoring critical safety functions.

Typical simplified DAS automatic actuation functional logic is shown in Fig. 6.1-1. Detailed functional logic adds considerations for plant operation, test and maintenance, and information display for operator. Specific functional logic for each plant is described in the Plant Licensing Documentation.

Automatic DAS actuation is delayed by a timer to prevent actuation before the PSMS. The time delay interval is set to approximately 10 seconds to ensure a sufficient margin for the actuation of PSMS functions. Also, proper actuation of the PSMS automatically blocks succeeded DAS actuation. The blocking function uses status signals that are directly obtained from actuated components. This ensures there is no false blocking from a point in the actuation signal path that could be subsequently affected by a PSMS CCF.

During normal cool down operation, DAS automatic actuation can be manually bypassed through predetermined plant procedures. This operational bypass of the DAS is continuously displayed in the MCR.

Selected process variables are displayed on the DHP to provide needed information to plant operators. The selected variables are based on the following considerations:

- To decide the need for manual action
- To confirm actuation of safety functions and monitor plant conditions through plant parameters for critical safety functions

**Table 6.1-4 Typical Monitoring Variables for DAS**

Variables	Number of Channel
Intermediate Range Neutron Flux	1
Pressurizer Pressure	1
RCS Pressure Wide Range	1
RCS Cold Leg Temperature (Tcold)	1 / loop
Pressurizer Level	1
Steam Generator Water Level	1 / SG
Main Steam Line Pressure	1 / SG
Containment Pressure	1

Note)

The DHP provides at least a single indicator for each parameter. The indication of parameter is switchable between two channels to accommodate a channel that may be failed on in bypass.



## 6.2 System Design Features

### 6.2.1 Overall Design

Based on the Basic Principle 1 to 6 in Section 5, the DAS includes the following design features.

#### 6.2.1.1 Operability

The DAS is a non-safety system. Therefore, there is no redundancy requirement for actuation to accommodate single failures or equipment out of service for testing or maintenance. Although the DAS function is disabled during maintenance or testing, these intervals will be administratively controlled to be consistent with the out of service times assumed in the Probabilistic Risk Assessment (PRA).

The DAS is designed to prevent spurious actuations due to single failures. Spurious DAS actuations are prevented by following DAS configuration.

- Automatic DAS functions are actuated by two subsystems and DAS actuation needs coincidence of both subsystems.
- DAS electrical circuits are designed to actuate when energized. Loss of power or removal of module does not cause spurious actuation.

In addition, the DAS is designed to prevent spurious actuation due to a seismic event. Thus the SSE will not result in a DAS failure that adversely affects the safety system.

#### 6.2.1.2 Diversity to Digital Safety and Non-Safety Systems

The DAS utilizes conventional hardware circuits (analog circuits, solid-state logic processing, relay circuits, etc.) to prevent the functions from being interrupted by the same CCFs postulated in the digital safety and non-safety systems. Furthermore, the DAS enables operation of safety system component that is independent of the safety and non-safety digital systems that are adversely affected by the CCF.

#### 6.2.1.3 Separation and Independency

The DAS is electrically and physically isolated from the PSMS as follows;

- When sharing sensors, transmitting signals, etc. between the PSMS and the DAS, isolation devices (isolation transformers, relays, optical fiber, photo couplers, etc.) are installed in the safety system. These isolators are part of the safety system and are fully qualified.
  - When DAS outputs interface to Power Interface (PIF) modules in the Safety Logic System (SLS), isolation devices (isolation transformers, relays, optical fiber, photo couplers, etc.) are installed in the safety system. These isolators are part of the safety system and are fully qualified.
-

#### 6.2.1.4 Testability

Verification of the functions, such as setpoint values, logic, etc., are conducted. Spurious actuation from one DAS subsystem during testing is prevented by 2-out-of-2 voting logic in the SLS.

#### 6.2.1.5 Maintenance bypass

If an input sensor fails in a trip state, the failed sensor signal can be bypassed by a dedicated bypass switch on the bistable module. The bypass switch bypasses only the sensor that has failed.

Other maintenance bypass functions are not necessary based on the following DAS configuration.

- Automatic DAS system consists of two subsystems and DAS actuation requires coincident outputs of both subsystems.
- DAS electrical circuit is designed to actuate when energized. Loss of power or removal of module does not cause spurious actuation.

#### 6.2.1.6 Operation Bypass

The DAS automatic functions may be manually bypassed by the actuation of a dedicated hardwired switch on the operator console. This is the Defeat Switch shown in Fig. 6.1-1 This switch bypasses both DAAC subsystems. The DAS Operation Bypass prevents unnecessary automatic DAS actuations due to expected plant conditions during plant startup and shutdown. The Operation Bypass is reset only by operator action of the above switch. Actuation of the Operation Bypass is displayed to the operators in the MCR by displaying on the non-safety operational Visual Display Unit (VDU).

#### 6.2.1.7 Quality

The DAS is designed with sufficient quality as follow:

- Designed specially for nuclear applications using a nuclear quality program that conforms to 10 CFR 50 Appendix B.
- Uses components with a long history of successful operation in Japanese nuclear power plants.
- Uses components that are common in conventional non-digital safety systems.
- A design process that includes independent review by people that were not involved in the design.

## 6.2.2 Diverse Automatic Actuation Cabinet (DAAC)

### 6.2.2.1 Automatic Actuation Logic

#### (1) Input Parameter and Actuation Logic

The following signals are isolated from the PSMS and interfaced to the separate subsystems in each DAAC. Within each DAAC these signals are compared to their setpoint values and if the setpoint values are exceeded, a partial actuation signal is generated. A diverse reactor trip and/or ESF actuation is generated from each DAAC through voting logic of sensor signals. Final actuation of Reactor Trip and/or ESF functions is based on receipt of actuation signals from both DAAC cabinets by the actuated components.

#### Input Parameter

- (a) Pressurizer pressure ...3 channels with pressure sensors
- (b) Steam generator water level...1 channel per SG

#### Actuation Logic

- (a) Pressurizer Pressure Low  
Reactor trip, turbine trip and main feedwater isolation signals are generated through 2-out-of-3 voting logic of the 3 pressurizer pressure channel signals.
- (b) Pressurizer Pressure High  
Reactor trip, turbine trip and main feedwater isolation signals are generated through 2-out-of-3 voting logic of the 3 pressurizer pressure channel signals.
- (c) Steam Generator Water Level Low  
Reactor trip, turbine trip, main feedwater isolation and emergency feedwater signals are generated through 3-out-of-4 voting logic from the 1 channel signals per SG of SG water level. The US-APWR is a 4 loop plant so that the voting logic is 3-out-of-4. The D3 Coping Analysis demonstrates this logic is adequate for all secondary events including loss of feedwater and SG rupture. In case of a 2 or 3 loop plant, 2-out-of-2 or 2-out-of-3 is adopted for the voting logic respectively.

#### (2) Maintain and Reset of DAS Actuation Signals

Once diverse automatic actuation signals (reactor trip, turbine trip, main feedwater isolation and emergency feedwater) are generated from a DAAC, these signals are latched. These signals are reset from the Defeat Switch for diverse actuation signals in the DHP in the MCR.

#### (3) Diverse Automatic Actuation

Diverse reactor trip, turbine trip, main feedwater isolation and emergency feedwater signals lead to the diverse actuation as follow.

- (a) Reactor Trip  
Reactor trip is actuated by tripping the non-safety rod drive motor-generator set. This

---

actuation leads to de-energizing the power for the Control Rod Drive Mechanism (CRDM) by a means that is diverse from the reactor trip breaker to release the control rods for gravity insertion into the reactor core. Diversity from the PSMS is maintained from sensors inputs to final actuators.

(b) Turbine Trip

Turbine trip is actuated by opening the solenoid valves for turbine trip. Diversity from the Turbine Trip function in the PSMS is maintained from sensor input up to the PIF Module.

(c) Main Feed Water Isolation

Main feed water isolation is actuated by closing the main feedwater control valve. Diversity from the feedwater isolation function in the PSMS is maintained from sensor input up to the PIF Module except for sensors.

(d) Emergency Feedwater

Emergency feedwater is actuated by opening the start up valve for the turbine driven emergency feedwater pump. Diversity from the Emergency Feedwater actuation function in the PSMS is maintained from sensor input up to the PIF Module.

**(4) Actuated Alarms**

When DAS reactor trip, turbine trip, main feed water isolation or emergency feedwater signals are automatically actuated, the DAS provides these alarms and first out alarms on the DHP to indicate the input parameter that has caused the actuation. The alarm sounds and indications are independent and diverse from the normal alarms from the PCMS. The configuration of the DAS actuation alarms is shown in Fig. 6.2-1.

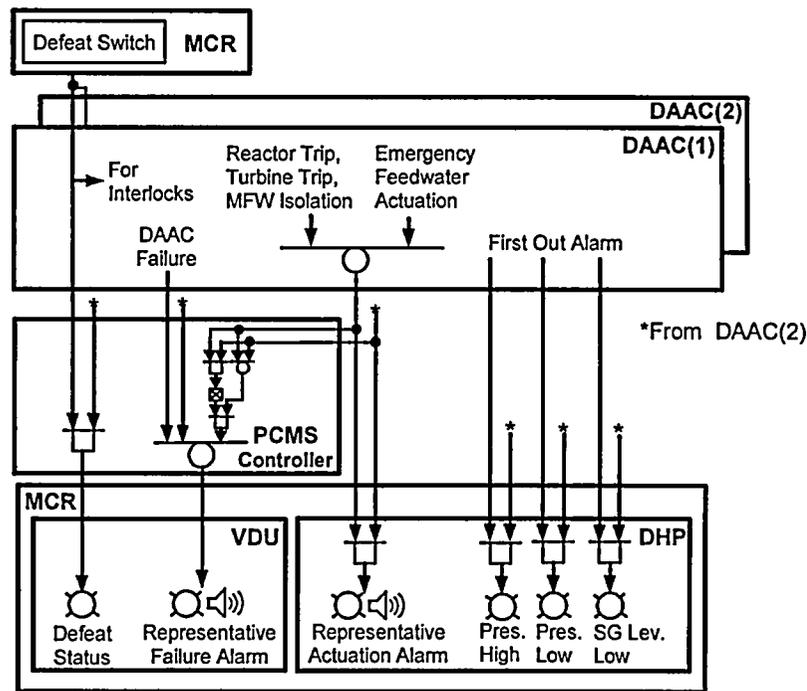


Figure 6.2-1 Configuration of the DAS Alarms

6.2.2.2 Prevention of Diverse Actuation under no CCF condition

The DAS is prevented from actuating automatically by component status signals when there are no CCF condition (i.e. the PSMS has actuated normally). Figure 6.2-2 shows the interface of the status signals from the PSMS.

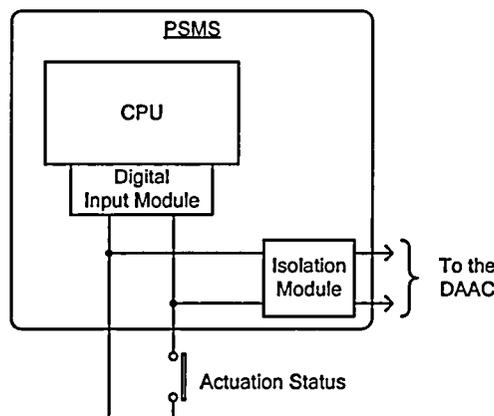
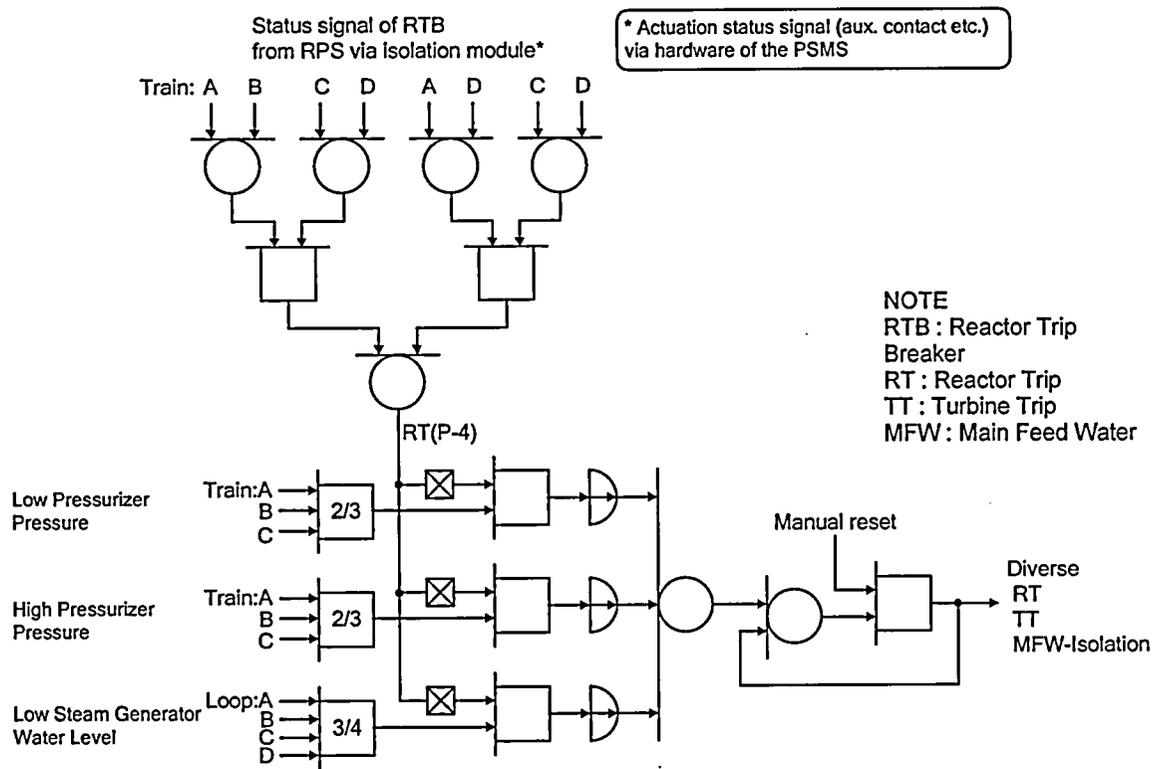


Figure 6.2-2 The Signal Flow of the Status Signal

**(1) Prevention for Diverse Actuation of Reactor Trip, Turbine Trip and MFW Isolation**

The DAS obtains status signals from the aux contacts of the reactor trip breakers via the hardware part of PSMS. When status signals are received indicating that the minimum required components for Reactor Trip have actuated, the automatic diverse reactor trip, turbine trip and main feedwater isolation signals are blocked from DAS. If any of the minimum components for Reactor Trip have not actuated, all of these DAS functions remain enabled. Figure 6.2-3 shows this prevention logic diagram. This logic ensures DAS functions are blocked when Reactor Trip functions of the PSMS function correctly.



**Figure 6.2-3 The Prevention Diagram of Reactor Trip, Turbine Trip and MFW Isolation**

**(2) Prevention for Diverse Emergency Feedwater Actuation**

When the Emergency Feedwater function is actuated correctly, the DAS automatic Emergency Feedwater actuation signal is automatically blocked. The DAS obtains the status signals from limit switch contacts on the steam inlet valves to the turbine driven EFW pump and from auxiliary contacts on the motor starters controlling the motor-driven emergency feedwater pumps. These status signals are obtained directly from the hardware part of PSMS. Figure 6.2-4 shows this prevention diagram.

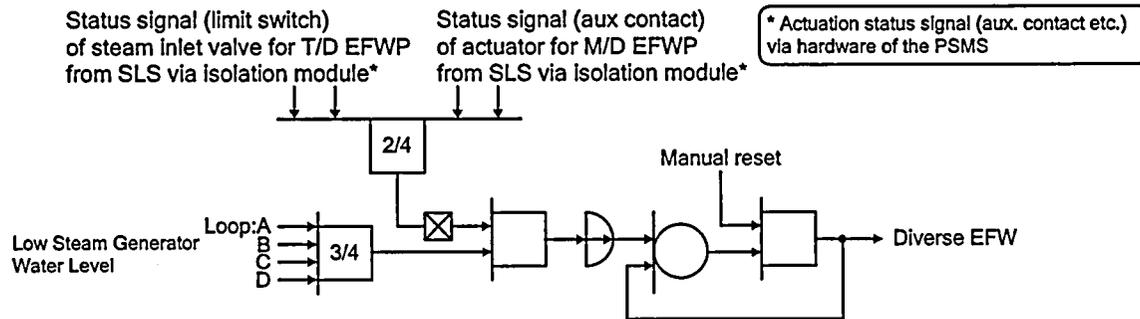


Figure 6.2-4 The Prevention Diagram of Emergency Feedwater

### 6.2.2.3 System Architectures

#### (1) Process Inputs

Safety sensors selected by the plant design for the DAS input are interfaced from within the PSMS or PCMS input modules. These input modules utilize analog distribution modules and isolation modules that connect the input signals to the DAS prior to any digital processing. Therefore, a software CCF within the PSMS or PCMS does not affect the DAS automation function or the display of plant parameters on the DHP. The MELTAC input module design is described in the Digital Platform Topical Report.

#### (2) Alarms and Indications

When diverse automatic actuation signals are actuated, the following alarms or indications are alarmed or displayed on the DHP in the MCR. The configuration of the DAS Alarms is shown in Fig. 6.2-1.

##### (a) Diverse Actuation Alarm (as a summary alarm)

- Reactor trip
- Turbine trip
- Main feed water isolation
- Emergency feedwater

##### (b) First Out Alarms

- Pressurizer pressure low
- Pressurizer pressure high
- SG water level low

With the diverse actuation alarms listed above, an audible alarm sound is also generated in the MCR to notify the operators. This DAS alarm indicators and audible sound in the MCR are independent of indicators and audible sound for the PCMS alarms.

Failure information from the DAS such as power supply failure and module failure, and spurious actuation of manual or automatic DAS functions are alarmed in the MCR as a

DAS failure summary alarm. The summarized DAS failure alarm is displayed at the alarm VDU in the MCR. Then, the detailed alarm information is displayed and can be confirmed in the DAAC in the I&C room outside the MCR. The configuration of the DAS failure alarms is shown in Fig. 6.2-1.

### (3) Testability

The following DAS components have special features to allow manual testing.

- Bistable module
- Logic module
- Output module
- Relay for permissive signal
- Relay for manual operation
- Permissive switch for DAS HSI (in Power Breaker for DHP)
- System level manual switch (on DHP)

### (4) Power Supply

The power supply for the DAAC including the relay for manual actuation circuits is supplied from the non-safety Uninterrupted Power Supply (UPS). The power supply from the non-safety UPS is described in the Safety I&C System Topical Report.

### (5) Fire Protection

Fire Protection for the DAAC is described in the Safety I&C System Topical Report.

## 6.2.3 Diverse HSI Panel (DHP)

The DHP consists of conventional switches and indicators. The DHP is used for manual actions credited in the D3 Coping Analysis. The DHP also provides monitoring and manual actuation of all critical safety functions in accordance with Position 4 of HICB BTP-19.

### (1) Switches for Manual Actuations

Manual diverse actuations are provided from conventional switches in the DHP. The DHP is activated by the permission switch in the Power Breaker for the DHP. The following diverse actuation switches are provided.

- (a) Manual Reactor Trip / Turbine Trip / Main Feedwater Isolation: 1 switch
- (b) Manual Emergency Core Cooling System (ECCS) Actuation: 1 switch
- (c) Manual Containment Vessel Isolation: 1 switch
- (d) Manual Emergency Feedwater Isolation and Flow Control
  - Emergency Feedwater Control Valve: 4 switches
- (e) Manual Control of Steam Generator Depressurization Valve: 4 switches
- (f) Manual Control of Pressurizer Depressurization Valve: 1 switch
- (g) Manual Emergency Feedwater Actuation: 1 switch
- (h) Permission switch for DAS HSI: 1 switch (installed in the Power Breaker for DAS HSI)

---

**(2) Connection of the Signals****(3) Actuation Status**

The actuation status of the systems and components actuated by DAS is confirmed through the monitoring of safety function parameters.

**(4) Parameters for Safety Function Indication**

Conventional analog indicators are provided on the DHP to monitor the process parameters for all critical safety functions. These are isolated and diverse from PCMS and PSMS so that operators can monitor the plant condition during all failures of the digital monitoring system that are caused by CCF.

The process parameters that are provided on the DHP are listed in Table 6.1-4.

**(5) Parameters for RCS Leak Detection**

The DHP provides indicators and alarms to monitor leaks in the Reactor Coolant System (RCS). According to RG 1.45 Item C.3, at least three separate methods are provided to detect leaks in the Reactor Coolant Pressure Boundary (RCPB):

- Containment vessel sump level and rate of level change monitoring
- Containment vessel airborne particulate radioactivity monitoring
- The third method is plant specific and will be identified in Plant Licensing Documentation.

These monitoring functions are implemented to DAS with diversity from the PSMS. Therefore these functions are not affected by a CCF that disables the PSMS.

If a small leak should occur in the RCS, these alarms and indicators prompt manual operator actions that allow the plant to be shutdown before the small leak can degrade. This manual operator action minimizes the potential for a LBLOCA coincident with a CCF in the PSMS.

**(6) Fire Protection**

Fire Protection for the DHP is described in the Safety I&C System Topical Report.

#### 6.2.4 PIF Module

PIF Modules in the PSMS and PCMS interface control signals to the plant components. These same PIF modules are used to interface control signals from the DAS. A common PIF Module provides one power interface conversion device for control of one plant component. This reduces the maintenance that would be required for two separate devices and it reduces the complexity of combining the PSMS/PCMS and DAS signals via relay logic. Reduced complexity results in improved reliability.

Control signals are interfaced from the PSMS or PCMS controllers to the communication interface part of the PIF Module via the controller's I/O communication network. The communication interface part converts the communication data to discrete signals. Control signals from the DAS are interfaced to the Interposing Logic (IPL) sub-board on the PIF Module via conventional hardwired connections and a conventional Isolation Module in PSMS.

The IPL is realized by discrete logic integrated circuits. The control signal from the PSMS or PCMS and the control signal from the DAS are integrated in the IPL. The logic in the IPL gives priority to the safe state, regardless of which system PSMS/PCMS or DAS is demanding this state. The safe state for each component is determined based on the plant safety analysis. For components that are repositioned at different times during an event scenario, the safe state is the state required initially for event mitigation.

The switching device part of the PIF Module is controlled by the integrated control signal from the IPL. The signal interface of the PIF Module is shown in Fig. 6.2-5. Therefore DAS output signals interface to plant components via only the hardware part of the PIF Module, so CCF within the PSMS or PCMS digital platform will not affect DAS signals.

The PIF Modules are not susceptible to a software CCF because they consist of proven, simple and fully testable hardware devices as described in the Digital Platform Topical Report.

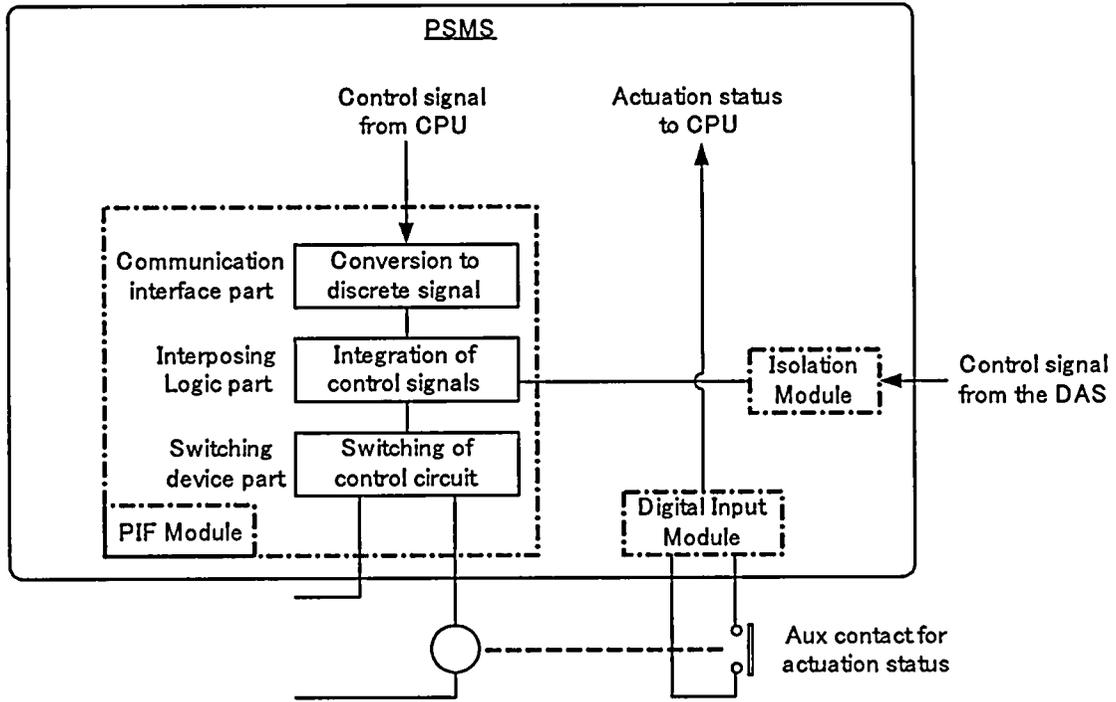


Figure 6.2-5 The Signal Interface of the PIF Module

## 7.0 DIVERSITY ANALYSIS

The defensive measures used within the PSMS and between the PSMS and PCMS to minimize the potential for CCF are described in the Safety I&C System Topical Report and are summarized in Section 5. Point 1 of BTP-19 provides guidance for assessing diversity within the protection and control systems to identify the software CCF vulnerabilities and their effects. However, MHI's defense-in-depth strategy does not rely solely on the diversity within the protection and control systems. It also relies on the diversity between the PSMS/PCMS and the DAS. The design basis for the DAS assumes that the CCF completely disables the PSMS and PCMS, regardless of where the CCF originates within these systems. The adequacy of the DAS for coping with an AOO or PA, concurrent with a PSMS/PCMS CCF, is described in Section 8.

This section analyzes the diversity between the PSMS/PCMS and the DAS. This analysis is based on NUREG/CR-6303 which describes a method for analyzing digital system vulnerability to postulated software CCFs.

NUREG/CR-6303 provides fourteen guidelines for performing a diversity and defense-in-depth analysis. The following sections describe the results of applying these guidelines to the PSMS/PCMS and DAS.

### 7.1 Guideline 1: Choosing Blocks

The DAS, PSMS and PCMS are three separate systems. The DAS is also physically and electrically independent from the PSMS. Therefore the DAS is considered a separate block from the PSMS/PCMS blocks. The CCF is assumed to cause the complete loss of function of the PSMS/PCMS blocks, but not cause loss of function of the DAS block, since they are separate and diverse blocks.

Table 4.1-1 maps the echelons of defense to the I&C architecture. The echelons are divided into the non-safety, the safety and diverse defense to reflect the means provided by the systems to implement the functions of each echelon. Table 4.1-2 also illustrates the relationship between these subsystems and cabinets and the block structure described in NUREG/CR-6303. This table shows the assignment of equipment to the blocks for each level within the echelons of defense.

The diversity between these blocks is described in the following sections.

### 7.2 Guideline 2: Determining Diversity

NUREG/CR-6303 identifies six attributes to determine the degree of diversity between two blocks.

#### 7.2.1 Design Diversity

The DAS uses different analog technology and architecture from the PSMS/PCMS.

The PSMS is a Class 1E system consisting of four separate digital trains. 2-out-of-4 voting logic is used for the reactor trip function and most ESF actuation functions. Multiple reactor trip functions and ESF actuations are provided for each AOO and PA, generally using diverse sensors, as described in the Safety I&C System Topical Report generally. The specific information will be described in the Plant Licensing Documentation. The DAS has two analog subsystems. Each analog subsystem uses a voting logic of monitored input channels for automatic actuation of each DAS function. The DAS actuation signals are configured using 2-out-of-2 voting to execute actuation of reactor trip and ESF systems. The functional logic for the automatic DAS functions is shown in Section 6.

### **7.2.2 Equipment Diversity**

The DAS equipment is based on the conventional analog technology. The PSMS and PCMS are based on digital technology. Thus the DAS, equipment used to provide automatic actions, manual actions and parameter monitoring is diverse from the equipment used for those same functions in the PSMS and PCMS. In addition, the DAS provides a reactor trip by tripping the non-safety rod drive motor-generator set. This means is diverse from the reactor trip switchgear used in the PSMS for reactor trip.

### **7.2.3 Functional Diversity**

The methods used by DAS to detect AOOs and PAs and take mitigating actions are described in section 8. In some cases the methods used by DAS are functionally diverse from the methods used by PSMS/PCMS. However functional diversity does not always exist. However, there is functional diversity within the PSMS for each AOO and PA. The functional diversity within the PSMS is described in Plant Licensing Documentation.

### **7.2.4 Human Diversity**

The design person for the DAS is different from the design person for the PSMS and PCMS.

### **7.2.5 Signal Diversity**

The DAS uses the same sensors as the PSMS. However, there is signal diversity within the PSMS as described in the Safety I&C System Topical Report. Signal diversity for each event is provided for reactor trip. In many cases this signal diversity is also applicable to ESF actuation. For some events the signals used to produce a reactor trip are diverse from the signals for ESF actuation.

### **7.2.6 Software Diversity**

The DAS uses only conventional analog technology. Thus the DAS is completely diverse from the software of the PSMS and PCMS.

### 7.3 Guideline 3: System Failure Types

NUREG/CR-6303 describes three different failure types that are applicable to US-APWR.

#### 7.3.1 Type 1 Failure

Type 1 failures are control system failures that result in plant transients that require protective actions for mitigation. As discussed in Section 5.5, a software error in the PCMS, that results in fail-as-is conditions, can go undetected. Therefore a CCF may result that leaves all PCMS functions in a fail-as-is condition. Alternately, a software failure that results in spurious actuation of a PCMS function (e.g. Reactivity Control, Pressurizer Control, Steam Generator Level Control, etc.) to the energized or de-energized state is immediately detectable and therefore very unlikely to result in a CCF that effects multiple PCMS functions. A fail-as-is condition of the entire PCMS and a spurious actuation of a single PCMS function are bounded by the AOOs analyzed in Chapter 15 of the Safety Analysis. Concurrent with each of these AOOs the PSMS is assumed to be disabled by the CCF. The ability to detect and mitigate each AOO using the DAS is described in the D3 Coping Analysis.

#### 7.3.2 Type 2 Failure

Type 2 failures do not directly cause plant transients but are undetected failures that are manifested only when a demand is received to actuate a component or system. The PSMS and PCMS are assumed to have Type 2 failures when an AOO or PA occurs. The ability to detect and mitigate each AOO or PA using the DAS is described in the D3 Coping Analysis.

#### 7.3.3 Type 3 Failure

Type 3 failures occur because, the primary sensors expected to respond to a design-basis event produce anomalous readings. The primary defense against a Type 3 failure is to provide diverse sensors for measuring the plant response to an initiating event. Sensor diversity within the PSMS for each AOO and PA is described in the Plant Licensing Documentation.

All Type 3 failures are bounded by the Type 2 failures, discussed above, since the analysis assumes that Type 2 failures completely disable the PSMS and PCMS.

### 7.4 Guideline 4: Echelons of Defense

The I&C architecture includes four echelons of defense, as defined in NUREG/CR-6303. Table 4.1-1 and Table 4.1-2 show these echelons.

The control system echelon is provided by the PCMS, with certain inputs provided from the PSMS by means of isolated data links.

The PSMS provides the RTS echelon. The functionally diverse protection subsystems within the RPS, the voting logic, dedicated data links, the reactor trip switchgear interface, and the reactor trip switchgear provide the reactor trip function in the safety PSMS.

The PSMS also provides the ESF echelon. The functionally diverse protection subsystems within the RPS, the ESFAS coincidence logic, the ESF actuation subsystems, dedicated data links, and data highways provide the ESF function in the PSMS.

The monitoring and indicators echelon is provided by both the PSMS and PCMS. The PSMS HSI provides monitoring and control for only safety related functions. The PCMS HSI provides monitoring and control for non-safety related functions and safety related functions.

The non-safety DAS provides diverse backup functions for the RTS echelon, the ESFAS echelon and the monitoring and indicators echelon.

#### **7.5 Guideline 5: Method of Evaluation**

In D3 Coping Analysis, the CCF is postulated to cause complete failure of the PSMS and PCMS concurrent with each AOO and PA. Both systems fail in the fail-as-is condition. The CCF is assumed to cause the complete loss of function of the PSMS and PCMS. Loss of function of the DAS does not occur due to the diversity of the DAS implementation. The D3 Coping Analysis also considers a software failure that results in spurious actuation of single PSMS or PCMS function during normal plant operation (i.e. without a concurrent PA). The basis for this is discussed in Section 5.5. All spurious actuation conditions are bounded by the AOOs considered in the D3 Coping Analysis.

#### **7.6 Guideline 6: Postulated CCF of Blocks**

The CCF of digital subsystems postulated for this document is a failure that occurs in all similar subsystems. This postulated failure could be caused by failure of a common hardware element, or failure of a common software element. This failure is assumed to cause the complete loss of function of the PSMS and PCMS, but not loss of function of the DAS due to the diversity of the DAS implementation. The result of this failure is that the entire system or systems fail to produce any protective actions.

#### **7.7 Guideline 7: Use of Identical Hardware and Software Modules**

In the D3 Coping Analysis, a CCF that disables the PSMS and PCMS is postulated. Therefore there is no need to assign a probability to the CCF.

#### **7.8 Guideline 8: Effect of Other Blocks**

In the D3 Coping Analysis, a CCF that disables the PSMS and PCMS outputs is postulated. Therefore there is no need to determine the CCF effect on blocks prior to the output or the propagation effect of those CCFs.

---

## 7.9 Guideline 9: Output Signals

In the D3 Coping Analysis, a CCF that disables the PSMS and PCMS outputs is postulated. The PSMS and PCMS outputs are not used by the DAS. Therefore, there is no need to evaluate propagation of CCF effects beyond the system output. However, the fail-as-is states of the PSMS and PCMS outputs are considered in the D3 Coping Analysis to ensure there is no adverse interaction with the protection functions provided by the DAS.

## 7.10 Guideline 10: Diversity for the AOO

The plant response for each AOO is evaluated, in conjunction with the postulated CCF that disables the PSMS/PCMS. Based on manual/automatic mitigation actions from the DAS, the D3 Coping Analysis demonstrates that there is no more than 10% of the 10 CFR 100 dose limit and the integrity of the primary coolant pressure boundary is not violated. The best estimate analysis methods used for the D3 Coping Analysis are described in Section 8.

## 7.11 Guideline 11: Diversity for the PA

The plant response for each PA is evaluated, in conjunction with the postulated CCF that disables the PSMS/PCMS. Based on manual/automatic mitigation actions from the DAS, the D3 Coping Analysis demonstrates that the 10 CFR 100 dose limit is not exceeded, that the integrity of the primary coolant pressure boundary is not violated, and that the integrity of the containment is not violated. The best estimate analysis methods used for the D3 Coping Analysis are described in Section 8.

## 7.12 Guideline 12: Diversity Among Echelons of Defense

### 7.12.1 Control/Reactor Trip Interaction

An AOO may result from a CCF that causes a PCMS fail-as-is condition, as discussed above. This same CCF may disable the reactor trip function in the PSMS. The DAS provides a diverse means of protection that is not effected by the CCF. The D3 Coping Analysis demonstrates compliance with the acceptance criteria defined above for each AOO.

### 7.12.2 Control/ESFAS Interaction

An AOO may result from a CCF that causes a PCMS fail-as-is condition. This same CCF may disable the ESFAS. The DAS provides a diverse means of protection that is not effected by the CCF. The D3 Coping Analysis demonstrates compliance with the acceptance criteria defined above for each AOO.

### 7.12.3 Reactor Trip/ESFAS Interaction

A CCF may disable both the RPS and ESFAS. The DAS provides all functions required by the ATWS rule (10 CFR 50.62). In addition, the D3 Coping analysis demonstrates compliance with the acceptance criteria defined above for each AOO and for each PA.

**7.13 Guideline 13: Plant Monitoring**

A CCF that affects the PSMS and/or PCMS may result in erroneous indication that may result in operator initiated transients. Operator initiated transients are bounded by the AOOs of Chapter 15. This same CCF may disable the RPS/ESFAS. For these transients the DAS provides a diverse means of protection that is not effected by the CCF. The D3 Coping Analysis demonstrates compliance with the acceptance criteria defined above for each AOO.

**7.14 Guideline 14: Manual Operator Action**

The DAS provides diverse analog data processing and HSI for at least one key variable for each critical safety function. The DAS provides diverse conventional controls for system level actuation of plant systems that can control each critical safety function.

## 8.0 D3 COPING ANALYSIS METHOD

This section describes the analysis methods used to demonstrate the plant meets the safety goals required by HICB BTP-19 for all AOOs and PAs with a concurrent CCF that disables the PSMS and PCMS.

### 8.1 Event Analysis Method

The D3 Coping Analysis shows that the plant response considering a CCF in the PSMS and PCMS, meets the following acceptance criteria.

- For each AOO in Chapter 15, plant response obtained from best estimate analysis does not result in violation of the integrity of the reactor coolant pressure boundary, or radiation release exceeding 10% of 10 CFR 100 guideline.
- For each postulated accident in Chapter 15, plant response obtained from best estimate analysis does not result in violation of the integrity of the reactor coolant pressure boundary or the integrity of the containment, or radiation release exceeding 10 CFR 100 guideline.

For all AOOs and PAs the D3 Coping Analysis demonstrates that DAS and associated operator action brings the plant to stable Hot Shut Down (HSD). Accidents such as Steam Generator Tube Rupture (SGTR), Main Steam Line Break (MSLB), Main Feed Line Break and Small Break Loss Of Coolant Accident (SBLOCA) need actuation of ESF functions in addition to reactor shutdown. Other accidents, such as Reactor Coolant Pump (RCP) Locked Rotor are terminated only with reactor shutdown.

Based on BTP-19 the D3 Coping Analysis uses best estimate methods. Plant parameters, initial conditions and related assumptions used in the D3 Coping Analysis are nominal values and realistic assumptions compared with corresponding parts of the Chapter 15 analysis. Any differences and changes from the Chapter 15 analysis are identified with an explanation of why the change is appropriate.

Major differences between the Chapter 15 Safety Analysis and the D3 Coping Analysis include:

- All the safety functions of the digital safety system are considered to be disabled by a CCF.
- Any single failure assumption in systems and components is not applied.
- Any action of the control system which mitigates the event is not considered.
- Normal control actions which may lead the event to an adverse situation are considered.
- Spurious actuations of control or safety systems which may lead the event to an adverse situation are not considered.
- Off-site power is available through the event except the Loss of Offsite Power event.
- The plant is at nominal operating conditions, not at the outside limit of any control band or operating limit.
- All systems and equipment are operable, with the exception of equipment that is licensed for unlimited bypass or out of service. Equipment licensed for unlimited bypass or out of service is assumed to be inoperable.

Response time of the DAS automatic actuation is considered in the D3 Coping Analysis. Delay of all the DAS related components from sensor to actuator is considered in the response time. Also, functional timer delay which prevents actuation of DAS before normal operation of the PSMS is considered.

Setpoints for the DAS automatic actuation is nominal equipment accuracies of the related components added as the DAS function.

The feasibility of manual operator action times is demonstrated based on the methods described in Section 8.2 below.

Using the analysis basis described above, an evaluation is performed for each event that is evaluated in the Chapter 15 accident analysis. Based on this evaluation events are categorized as follows:

- Equivalent Protection – For some events the DAS provides protection that is considered essentially equivalent to the protection provided by the RPS/ESFAS. For these events the basis of concluding equivalent protection is documented and no additional analysis is provided.
- Expertly Judged - Some events in this category are judged by the safety analysis expert to be bounded by other more severe events from the point of occurrence of the event scenario and the consequence of the event. Other events in this category are judged by the safety analysis expert to meet the acceptance criteria by detailed evaluation of the event scenario and consequences. In both cases the basis of the conclusion is clearly documented and no additional analysis is provided.
- Analyzed – Where the event cannot be dispositioned by the judgment of the safety analysis expert, the event is analyzed using computer models. The computer code used for this analysis is the same computer code used in the Chapter 15 analysis. Other computer codes may be used provided that the applicability of the code for the analyses performed is documented.

Results of the D3 Coping Analysis for each event are described in the Plant Licensing Documentation or its relevant technical report.

## 8.2 Manual Action Analysis Method

Operator action time to mitigate the event is measured from the prompting DAS alarm. The target minimum operator action time is 10 minutes. If action is needed earlier than 10 minutes the function is generally automated.

Any operator actions credited prior to 30 minutes are justified based on an HFE evaluation. Justification includes assessments of available information, the decision making process and expected steps leading to the credited action. The justification of operator actions credited prior to 30 minutes is based on the following:

- Operator training ensures operators are aware of plant conditions requiring manual reactor trip or manual actuation of ESF systems. Emergency procedures reinforce this training.
- These indications and associated alarms are provided on the LDP (Large Display Panel) and on the DHP. In addition the DHP provide alarms for actuation of automatic DAS

functions. The DHP is not affected by the CCF.

- The time zero for any operator action is assumed to be any of the prompting alarms provided on the DHP.
- The sequence of expected operator actions in response to a prompting alarm and subsequent indications is based on execution of the steps in the Emergency Operating Procedures.
- The time to execute each step in the procedure is based on HFE industry standards, such as ANS 58.8, Time Response Design Criteria for Safety Related Operator Actions
- The expected time for taking the manual action credited in the D3 Coping Analysis is based on the sequence and time for each step, including completion of the step(s) in the procedure that prompts the credited operator action.

NRC approval of manual operator actions credited in the D3 Coping Analysis is expected based on the HFE evaluation methods described above. In addition, all manual actions credited in the D3 Coping Analysis are included in the HFE Program described in the HSI System Topical Report. This program includes these actions in Human Reliability Analysis and HSI Validation using a dynamic high fidelity simulator.

### 8.3 Treatment of Large Break LOCA

The LBLOCA is 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.

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

- The PRA identifies LBLOCA as an accident with extremely low probability of occurrence.
- The SRM 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.

In establishing this coping strategy it is recognized that there are no industry accepted methods for establishing the reliability of a software based safety system. However, IEC-61226 and IEC-61508 suggest that a reasonable value to use for the probability of failure on demand (PFD) is this typical probability value for a qualified software based safety system designed to nuclear quality standards. The acceptance of this mitigation strategy is based on achieving the plant safety goals for Core Damage Frequency (CDF) and Large Early Release Frequency (LERF) using  $PFD=10^{-4}$  in the PRA.

It is also recognized that there may be uncertainty in assigning this PDF value to the PSMS. However, any uncertainty that may exist in this number is offset by the diverse leak detection function which further reduces the probability of the LBLOCA.

## 9.0 KEY TECHNICAL ISSUES

This section summarizes the Defense-in-Depth and Diversity design features that specifically address the following key technical issues.

- Integrated RPS & ESFAS with Functional Diversity
- CCF Modes for Defense-in-Depth and Diversity analysis
- Credit for Leak Detection in Defense-in-Depth and Diversity analysis
- Common PIF Module for PSMS/PCMS and DAS

### 9.1 Integrated RPS & ESFAS with Functional Diversity

Within the same subsystem of the RPS, RPS bistable and coincidence voting functions are also used for ESFAS, where both functions are actuated on the same parameters. The functions are combined because integration of RPS and ESFAS requires less hardware than if the functions were separated. Less hardware results in fewer failures and less testing. Fewer maintenance interactions with the system reduce the potential for human errors that can reduce system reliability or cause spurious actuations that threaten plant safety.

Instead of separating RPS and ESFAS, functional diversity is provided within the integrated RPS/ESFAS through two separate subsystems in each train. For each AOO and PA, each subsystem processes diverse sensor inputs that can each detect the event and initiate protective actions. PRAs done for nuclear plants in Japan show significant benefit for this functional diversity. On the other hand, PRAs done for nuclear plants in Japan show minimal benefit for additional RPS/ESFAS separation (with functional diversity). Table 9.1-1 shows typical examples of this functional diversity.

**Table 9.1-1 Diverse Parameters in Two Separate Controller Groups**

Gr.1	Gr.2	Note
Over Power Delta-T High Power Range Neutron Flux Rate High	Power Range Neutron Flux High	Over Power Protection
Reactor Coolant Pump Speed Low Over Temperature Delta-T High	Reactor Coolant Flow Low Pressurizer Pressure Low	Core Heat Removal Protection
Steam Generator Water Level Low Pressurizer Water Level High	Pressurizer Pressure High	Loss of Heat Sink Protection
Source Range Neutron Flux High Intermediate Range Neutron Flux High	Power Range Neutron Flux High (Low setpoint)	Nuclear Startup Protection
Pressurizer Water Level High	Pressurizer Pressure High	Primary Over Pressure Protection

## 9.2 CCF Modes for Defense-in-Depth and Diversity Analysis

BTP-19 requires consideration of CCFs that "disable" the protection system. Based on this, the D3 Coping Analysis considers CCFs that result in a fail-as-is condition in the PSMS and PCMS. The D3 Coping Analysis does not consider CCFs that result in output state changes (i.e., spurious actuation to de-energized or energized state).

The basis for this is that the simplicity, deterministic performance and quality of the PSMS and PCMS minimize the potential for CCFs induced by changing plant conditions. Therefore the software CCF postulated for BTP-19 is induced by an undetected hidden defect. An undetected hidden defect that results in fail-as-is conditions may occur in multiple systems over an extended time duration, and therefore may still exist when an AOO or PA occurs. However a hidden defect that results in output state changes is immediately detectable by operators. Therefore this defect can be corrected before it becomes a CCF that affects multiple systems. Software defects that result in spurious actuation of individual systems are bounded by the AOO which are considered in the D3 Coping Analysis.

## 9.3 Credit for Leak Detection in Defense-in-Depth and Diversity Analysis

The DAS includes diverse processing and display of leak measurement sensors as described in Section 6.2.3. The DAS credits this diverse leak detection which allows operators to detect and mitigate the leak even if the PSMS and PCMS are not operating correctly due to an undetected latent CCF. This is consistent with BTP-19, the System 80+ Design Control Document, and the NRC's SER of that DCD, NUREG-1462, which state "Credit for leak detection is accepted ... because (1) LBLOCAs and MSLBs ... in combination with a CCF ... is highly unlikely (2) I&C equipment possesses sufficient diversity and simplicity including manual controls ... and instrumentation ..." A mitigation strategy that considers the low probability of LBLOCA is also consistent with 10 CFR 50.62, which requires diverse mitigation only for higher frequency AOOs.

## 9.4 Common PIF Modules for PSMS/PCMS and DAS

PIF Modules in the PSMS and PCMS interface control signals to the plant components. These same PIF modules are used to interface control signals from the DAS. A common PIF Module provides one power interface conversion device for control of one plant component. This reduces the maintenance that would be required for two separate devices and it reduces the complexity of combining the PSMS/PCMS and DAS signals via relay logic. Reduced complexity results in improved reliability.

The PIF Modules are not susceptible to a software CCF because they consist of proven, simple and fully testable hardware devices as described in the Digital Platform Topical Report.

## 10.0 FUTURE LICENSING SUBMITTALS

The complete MHI digital I&C design is described in four topical reports:

- Defense in Depth and Diversity (this topical report)
- Safety I&C System Description and Design Process
- Safety System Digital Platform -MELTAC-
- HSI System Design Description and HFE Process

Table 10.0-1 summarizes the additional information related to this topical report that will be submitted for NRC approval in future Plant Licensing Documentation. Table 10.0-1 summarizes all items identified in previous sections of this topical report. This Plant Licensing Documentation, in combination with the contents of this topical report, the contents of the other topical reports identified above, and any items for Plant Licensing Documentation described in those other topical reports is expected to be sufficient to allow the NRC to make a final safety determination. Other documentation generated during the design process is available for NRC audit, as may be needed to allow the NRC to fully understand the MHI design and design process.

**Table 10.0-1 Future Licensing Submittals**

<b>Description</b>	<b>Section</b>
Changes in implementation detail, as needed	1.0, 2.0
Specific description of the PSMS and the DAS functions	2.0
Specific I&C functions implemented within the DAS	3.1 GDC 13
Electric power sources for the DAS and the plant components controlled by the DAS	3.1 GDC 17
Conformance to the requirements in items iv thru vii	3.1 10 CFR 52.47
Inspections, tests, analyses and acceptance criteria that demonstrate that the DAS has been constructed and will operate in conformity with the Commission's final safety conclusion	3.1 10 CFR 52.79
Specific DAS functions of manual Initiation of Protective Actions	3.3 RG 1.62
Specific accident monitoring instrumentation of the DAS	3.3 RG 1.97
Instrument Sensing Lines	3.3 RG 1.151
Design Acceptance Criteria	3.4 BTP-16
Coping for all AOOs and PAs	3.4 BTP-19
Descriptions of specific plant systems	3.5 NUREG-0800
Specific DAS functions for other plants	6.0
Specific functional logic for each plant	6.1
Third method for RCS leak detection	6.2.3
Specific information of multiple reactor trip functions and ESF actuations	7.2.1
Functional diversity within the PSMS	7.2.3
Sensor diversity within the PSMS for each AOO and PA	7.3.3
Results of the D3 Coping Analysis for each event	8.1
An analysis for each AOO and PA in SAR chapter 15 with a concurrent CCF that disables the PSMS and PCMS	Appendix A Point 2

## 11.0 REFERENCES

In this section, references referred in this topical report except for applicable codes, standards and regulatory guidance in Section 3 are enumerated.

1. MUAP-07004, "Safety I&C System Description and Design Process"
2. MUAP-07005, "Safety System Digital Platform -MELTAC-"
3. MUAP-07007, "HSI System Design Description and HFE Process"
4. 10 CFR 50 Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"
5. NRC Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment that is not Safety Related"
6. IEEE 323 -2003, "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations"
7. IEEE 603 -1991, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations"
8. IEEE7-4.3.2 -2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"
9. System 80+ Design Control Document

## Appendix A Conformance to BTP HICB-19

The MHI I&C system and the approach to Defense-in-Depth and Diversity is designed in accordance with the following four-point position for the US-APWR and for digital system modifications to operating plants:

Positions as stated in BTP-19 are in *Italics*.

### ***Point 1***

***The applicant/licensee should assess the defense-in-depth and diversity of the proposed I&C system to demonstrate that vulnerabilities to common-cause failures have been adequately addressed.***

The defense-in-depth and diversity within the MHI I&C system has been assessed in this topical report. The potential for CCF is minimized based on diversity between the echelons of defense and within the echelons of defense. The diversity features within and between each echelon of defense are shown in Table 4.1-1 and 4.1-2. The diversity within the RPS functions of the PSMS is shown in Table 9.1-1.

Despite the numerous defenses against CCF that are built into the digital PSMS and PCMS, the MHI approach to defense-in-depth and diversity assumes a CCF completely disables these systems. Therefore the final defense against CCF is provided by the DAS, which is completely diverse from the PSMS and PCMS. NUREG/CR-6303, Section 7.2, describes six types of diversity and describes how instances of different types of diversity might be combined into an overall case for the sufficiency of the diversity provided. The analysis of the diversity between DAS and PSMS/PCMS is described in Section 7.

### ***Point 2***

***In performing the assessment, the vendor or applicant/licensee should analyze each postulated common-cause failure 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.***

An analysis will be provided in Plant Licensing Documentation for each AOO and PA in SAR Chapter 15 with a concurrent CCF that disables the PSMS and PCMS. This analysis will use the best estimate analysis methods described in Section 8. Adequate diversity (i.e. adequate coping capability) is judged by conformance to the acceptance criteria defined in Section 8.1, which is the same as the acceptance criteria in BTP-19. The DAS, which is diverse from the PSMS and PCMS and therefore not subject to the same CCF, is credited in this analysis for accident mitigation.

### ***Point 3***

***If a postulated common-cause failure could disable a safety function, a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-cause failure, should be required to perform either the same function as the safety system function that is vulnerable to common-cause failure or a different function that provides adequate protection. The diverse or different function may be***

---

***performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.***

The analysis for Point 2 assumes the CCF completely disables the PSMS and PCMS. Adequate coping is judged solely on the capabilities of the DAS which includes both automatic and manual actuation functions. The DAS is composed only of conventional analog and binary devices, thus it provides complete diversification from the digital safety I&C system. The conclusion that DAS is not subject to the same CCF that disables the PSMS/PCMS is based on the diversity between PSMS/PCMS and DAS, which is described in Section 7. The DAS has sufficient quality to perform the necessary function under the associated event conditions and within the required time. The DAS quality is described Section 6.

***Point 4 A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions. The displays and controls should be independent and diverse from the computer-based safety systems identified in Points 1 and 3.***

The DHP in the MCR has a set of displays and controls, which provides for manual system-level actuation of critical safety functions and for monitoring of parameters that indicate the status of those critical safety functions. The DHP is composed only of conventional analog devices that are independent and diverse from the PSMS.

The displays and controls on the DHP are sufficient for the operator to monitor and control the following critical safety functions: reactivity level, core heat removal, reactor coolant inventory, containment isolation, and containment integrity. HFE principles and criteria are applied to the selection and design of the displays and controls. These HFE principles are described in the HFE Tropical Report.

The PSMS and DAS share sensors for indications. The sensor signals are interfaced to the DHP prior to any digitalization in the PSMS. Conventional analog isolators in the PSMS assure independence.

The point at which the manual controls are connected to safety equipment is downstream of any potential CCF in the computer based safety system. The PSMS and DAS actuate many of the same components. The DAS output signals are interfaced to PSMS PIF Modules through conventional isolators in the PSMS that assure independence. The portion of the PIF used by both PSMS and DAS includes only conventional binary components (i.e. no software). These components have a long history of reliable operation in nuclear plants and are fully qualified. The design of the PIF is very simple so that it can be tested completely. As a result, the shared PIF components have no credible potential for CCF.

## Appendix B Conformance to 10 CFR 50.62

This topical report demonstrates the acceptability of the DAS for coping with software CCF in accordance with HICB BTP-19. The DAS also provides the ATWS mitigation function required by 10 CFR 50.62. This appendix describes the conformance of the DAS to the requirement of 10 CFR 50.62, "Requirements for reduction of risk from ATWS events for light-water-cooled nuclear power plants". Italic sentence in this appendix indicates the original requirement of 10 CFR 50.62.

- (1) *Each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feed water system and initiate a turbine trip under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system.*

The normal reactor trip function is provided by the PSMS. The DAS provides turbine trip and EFW actuation. The DAS is diverse and independent from the reactor trip function in the PSMS from sensor output to final actuation device. The simplified architecture between the reactor trip system and diverse turbine trip/EFW actuation system is shown in Fig. B-1.

- Computer based technique is used for the normal reactor trip in PSMS. On the other hand, conventional technique (analog and solid state logic) is used for the diverse turbine trip and EFW actuation from the DAAC.
- The DAAC EFW and TT functions use a subset of the same sensors used for the normal reactor trip function in the PSMS. There is no requirement in 10 CFR 50.62 for sensor diversity.
- The type of output module used in the PSMS for normal reactor trip differs from the output module used by the DAS for diverse turbine trip/EFW actuation. The output module for normal reactor trip applies an electromechanical relay for the final switching device. On the other hand, the output module for diverse turbine trip and EFW actuation applies a semiconductor for the final switching device. The output module applied for turbine trip and EFW actuation is the PIF module, described in Section 6.
- The output module for diverse turbine trip and EFW actuation is common to normal turbine trip and EFW actuation. There is no requirement in 10 CFR 50.62 for diversity between normal EFW and TT and diverse EFW and TT.
- Interface signals between the PSMS and the DAAC are isolated by conventional isolation modules to ensure independence.

- (2) *Each pressurized water reactor manufactured by Combustion Engineering or by Babcock and Wilcox must have a diverse scram system from the sensor output to interruption of power to the control rods. This scram system must be designed to perform its function in a reliable manner and be independent from the existing reactor trip system (from sensor output to interruption of power to the control rods).*

This requirement is not directly applicable to the US-APWR because the US-APWR is manufactured by MHI. But the US-APWR conforms to this requirement.

The normal reactor trip function from the PSMS is diverse and independent from reactor trip function provided by the DAS. The simplified architecture between the normal reactor trip function from the PSMS and diverse reactor trip function from the DAS is shown in Fig. B-2.

- Computer based technique is used for the normal reactor trip in PSMS. On the other hand, conventional technique (analog and solid state logic) is used for the diverse reactor trip in DAAC.
- The DAAC reactor trip function uses a subset of the same sensors used for the normal reactor trip function in the PSMS. There is no requirement in 10 CFR 50.62 for sensor diversity.
- The normal reactor trip from PSMS breaks the power of the CRDM using the reactor trip breaker. On the other hand, the diverse reactor trip from DAS breaks the power of the CRDM by de-energizing the M-G set.
- The interface signals between PSMS and DAAC are isolated by conventional isolation modules to ensure independence.

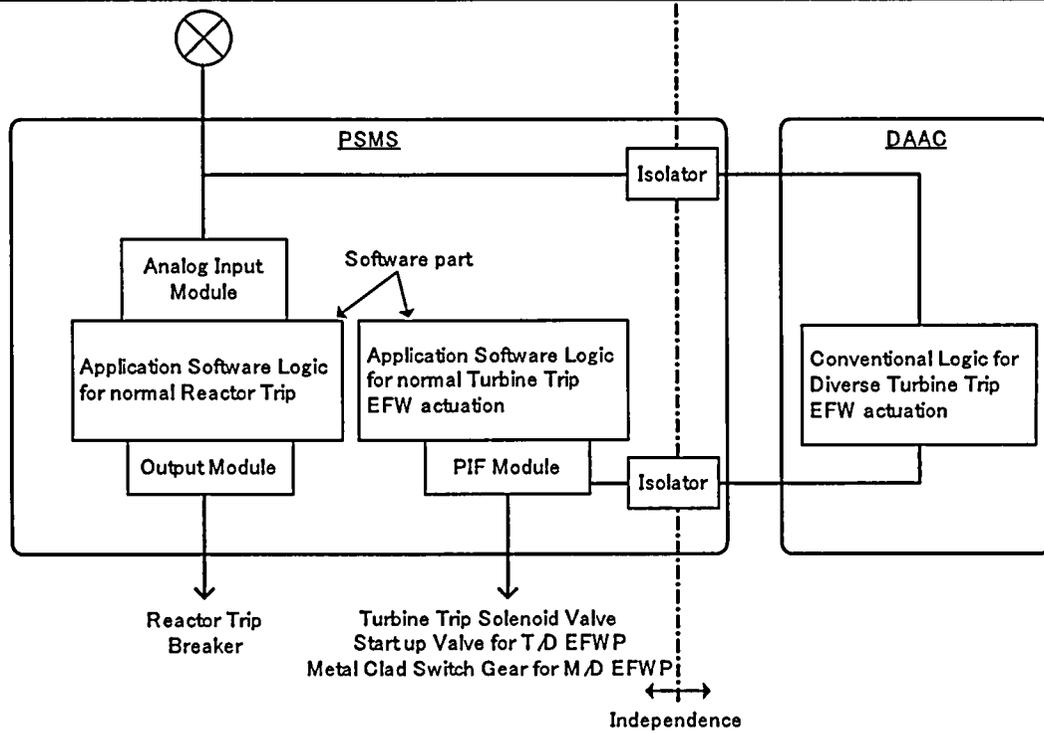


Figure B-1 The Diversity between the Reactor Trip and Turbine Trip/EFW Actuation

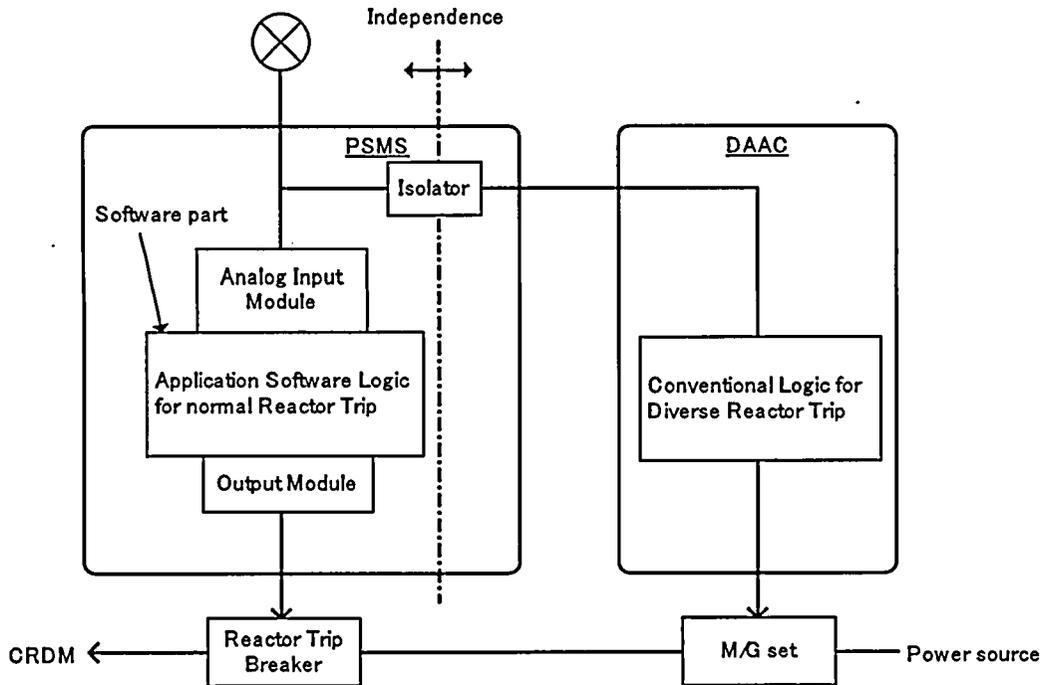


Figure B-2 The Diversity Between the Reactor Trip and Diverse Reactor Trip