



**HITACHI**

**GE Hitachi Nuclear Energy**

Richard E. Kingston  
Vice President, ESBWR Licensing

P.O. Box 780 M/C A-65  
Wilmington, NC 28402-0780  
USA

T 910.675.6192  
F 910.362.6192  
rick.kingston@ge.com

MFN 10-300, Revision 1

Docket No. 52-010

October 8, 2010

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

Subject: **Revised Transmittal of ESBWR Licensing Topical Report, NEDO-33251, "ESBWR I&C Diversity and Defense-In-Depth Report," Revision 3**

The purpose of this letter is to transmit a corrected NEDO-33251, "ESBWR I&C Diversity and Defense-In-Depth Report," Revision 3. This revised letter and associated LTR are provided to correct the page headers to reflect the correct revision. The corrected LTR is contained in Enclosure 1.

If you have any questions or require additional information, please contact me.

Sincerely,

*Richard E. Kingston*

Richard E. Kingston  
Vice President, ESBWR Licensing

*DOLO  
KRO*

Reference:

1. MFN 10-044 Supplement 3, Letter from Richard E. Kingston to US Nuclear Regulatory Commission, "*Revised Response (Revision 3) to NRC Request for Additional Information Letter No. 411 Related to ESBWR Design Certification Application – Engineered Safety Features – RAI 6.2-202 Supplement 1,*" dated September 28, 2010
2. MFN 10-300, Letter from Richard E. Kingston to US Nuclear Regulatory Commission, "*Transmittal of ESBWR Licensing Topical Report, NEDO-33251, "ESBWR I&C Diversity and Defense-In-Depth Report,"* Revision 3, dated October 2, 2010.

Enclosure:

1. NEDO-33251, "ESBWR I&C Diversity and Defense-In-Depth Report," Revision 3

cc: AE Cubbage      USNRC (with enclosure)  
JG Head            GEH/Wilmington (with enclosure)  
DH Hinds          GEH/Wilmington (with enclosure)  
PM Yandow        GEH/Wilmington (with enclosure)  
eDRF Section      0000-0090-5856

**Enclosure 1**

**MFN 10-300, Revision 1**

**NEDO-33251, "ESBWR I&C Diversity and Defense-In-Depth  
Report," Revision 3**

**September 2010**



**HITACHI**

GE Hitachi Nuclear Energy

NEDO-33251

Revision 3

Class I

DRF 0000-0073-2894

September 2010

LICENSING TOPICAL REPORT  
ESBWR I&C  
DIVERSITY AND DEFENSE-IN-DEPTH REPORT

*Copyright 2008, 2010 GE-Hitachi Nuclear Energy Americas LLC*

*All Rights Reserved*

## **INFORMATION NOTICE**

This document NEDO-33251 contains no proprietary information.

### **IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT**

#### **PLEASE READ CAREFULLY**

The information contained in this document is furnished as a reference to the NRC Staff for the purpose of obtaining NRC approval of the ESBWR Certification and implementation. The only undertakings of GE Hitachi Nuclear Energy (GEH) with respect to information in this document are contained in contracts between GEH and participating utilities, and nothing contained in this document shall be construed as changing those contracts. The use of this information by anyone other than that for which it is intended is not authorized; and with respect to any unauthorized use, GEH makes no representation or warranty, and assumes no liability as to the completeness, accuracy, or usefulness of the information contained in this document.

## Table Of Contents

List of Tables .....	iv
List of Figures.....	iv
GLOSSARY OF TERMS.....	xi
1.1 PREFACE.....	1
1.2 ARCHITECTURE OVERVIEW .....	1
1.3 SCOPE .....	2
1.4 SUMMARY AND CONCLUSIONS .....	3
1.4.1 Compliance with NUREG-0493 .....	3
1.4.2 Compliance with NUREG/CR-6303.....	3
1.4.3 Compliance with DI&C-ISG-02 .....	3
1.4.4 Meeting Probabilistic Safety-Related Goals.....	3
2.1 ARCHITECTURE DESCRIPTION .....	4
2.2 SAFETY-RELATED DISTRIBUTED CONTROL AND INFORMATION SYSTEM OVERVIEW .....	15
2.3 NONSAFETY-RELATED DISTRIBUTED CONTROL AND INFORMATION SYSTEM OVERVIEW .....	19
2.4 DIVERSE PROTECTION SYSTEM OVERVIEW.....	20
2.5 PCF (PLANT COMPUTER FUNCTIONS) OVERVIEW .....	24
2.6 CONFORMANCE TO THE NUREG/CR-6303 ECHELON OF DEFENSE STRUCTURE AND TO THE NUREG/CR-6303 BLOCK STRUCTURE .....	24
3.1 INTRODUCTION.....	27
3.2 DEFINITION OF COMMON-MODE FAILURES .....	27
3.3 OVERALL INSTRUMENTATION AND CONTROL FAULT TOLERANT DESIGN FEATURES.....	27
4.1 IDENTIFYING SYSTEM BLOCKS - GUIDELINES 1 AND 5.....	32
4.2 DETERMINING DIVERSITY- GUIDELINE 2 .....	32
4.3 SYSTEM FAILURE TYPES - GUIDELINE 3.....	35
4.3.1 Type 1 Failure .....	35
4.3.2 Type 2 Failure .....	35
4.3.3 Type 3 Failure.....	35
4.4 ECHELONS OF DEFENSE - GUIDELINE 4.....	36
4.5 POSTULATED COMMON-MODE FAILURE OF BLOCKS – GUIDELINE 6.....	36
4.6 USE OF IDENTICAL HARDWARE AND SOFTWARE MODULES – GUIDELINE 7.....	36

<b>4.7</b>	<b>EFFECT OF OTHER BLOCKS - GUIDELINE 8</b> .....	<b>37</b>
<b>4.8</b>	<b>OUTPUT SIGNALS - GUIDELINE 9</b> .....	<b>37</b>
<b>4.9</b>	<b>DIVERSITY FOR ANTICIPATED OPERATIONAL OCCURRENCES AND ACCIDENTS - GUIDELINES 10 AND 11</b> .....	<b>37</b>
<b>4.10</b>	<b>DIVERSITY AMONG ECHELONS OF DEFENSE - GUIDELINE 12</b> .....	<b>37</b>
	4.10.1 Control/Reactor Trip.....	37
	4.10.2 Control/Engineered Safety-Related Features (SSLC/ESF) .....	38
	4.10.3 Reactor Trip/ESFAS.....	38
<b>4.11</b>	<b>PLANT MONITORING - GUIDELINE 13</b> .....	<b>38</b>
<b>4.12</b>	<b>MANUAL OPERATOR ACTION – GUIDELINE 14</b> .....	<b>39</b>
<b>5.1</b>	<b>INTRODUCTION</b> .....	<b>40</b>
<b>5.2</b>	<b>DIVERSITY OVERVIEW OF THE ESBWR INSTRUMENTATION AND CONTROL ARCHITECTURE</b> .....	<b>40</b>
	5.2.1 ESBWR DCIS Hierarchy.....	40
<b>5.3</b>	<b>REACTOR SHUTDOWN</b> .....	<b>42</b>
<b>5.4</b>	<b>REACTOR COOLANT SYSTEM INVENTORY CONTROL</b> .....	<b>44</b>
<b>5.5</b>	<b>CORE DECAY HEAT REMOVAL</b> .....	<b>45</b>
<b>5.6</b>	<b>CONTAINMENT COOLING</b> .....	<b>46</b>
<b>5.7</b>	<b>CONTAINMENT ISOLATION</b> .....	<b>47</b>
<b>5.8</b>	<b>EVENT SCENARIOS</b> .....	<b>47</b>
	5.8.1 MSIV closure.....	48
	5.8.2 Loss of Condenser Vacuum.....	48
	5.8.3 Loss of Feedwater Heating .....	48
	5.8.4 Loss of Normal AC Power to Station Auxiliaries .....	48
	5.8.5 Loss of Feedwater Flow.....	48
	5.8.6 Generator Load Rejection with a Single Failure in the Turbine Bypass System..	49
	5.8.7 Inadvertent Isolation Condenser Initiation.....	49
	5.8.8 Turbine Trip with Full Bypass.....	49
	5.8.9 Opening of One Control or Turbine Bypass Valve .....	50
<b>APPENDIX A: ESBWR Instrumentation &amp; Control Defense-in-Depth and Diversity (D3) Evaluation of Reference 6-3, Chapter 15 Events Assuming Common Mode Failure of a Digital Protection System</b> .....		<b>1</b>

### List of Tables

<b>Table 1</b>	<b>ESBWR Instrumentation and Control Echelons of Defense .....</b>	<b>25</b>
<b>Table 2</b>	<b>Assignment of I&amp;C Equipment to Defense-in-Depth Echelons.....</b>	<b>26</b>

### List of Figures

<b>Figure 1</b>	<b>ESBWR DCIS Architecture.....</b>	<b>7</b>
<b>Figure 2</b>	<b>Hardware/Software (Platform) Diversity .....</b>	<b>11</b>
<b>Figure 3</b>	<b>ESBWR Logic Platform and Power Diversity .....</b>	<b>12</b>
<b>Figure 4</b>	<b>Main Control Room Layout - Typical .....</b>	<b>13</b>
<b>Figure 5</b>	<b>ESBWR DCIS and POWER Separation .....</b>	<b>14</b>
<b>Figure 6</b>	<b>RTIF-NMS, ICP, SSLC/ESF and DPS .....</b>	<b>18</b>
<b>Figure 7</b>	<b>N-DCIS Control Systems.....</b>	<b>41</b>
<b>Figure 8</b>	<b>Reactor Trip and Isolation Function of Q-DCIS .....</b>	<b>43</b>

## ACRONYMS AND ABBREVIATIONS

ABWR	Advanced Boiling Water Reactor
AC	Alternating Current
ADS	Automatic Depressurization System
AFIP	Automatic Fixed In-Core Probe
ALWR	Advanced Light Water Reactor
AMS	Alarm Management System
AOO	Anticipated Operational Occurrence
APRM	Average Power Range Monitor
ARI	Alternate Rod Insertion
ASME	American Society of Mechanical Engineers
ATLM	Automated Thermal Limit Monitor
ATWS	Anticipated Transient(s) Without Scram
BiMAC	Basemat Internal Melt Arrest Coolability
BOP	Balance of Plant
BTP	Branch Technical Position
BWR	Boiling Water Reactor
CB	Control Building
CCF	Common Cause Failure
CIRC	Circulating Water System
CMF	Common Mode Failure
CMS	Containment Monitoring System
COL	Combined License
CRD	Control Rod Drive/Control Rod Drive System
CRHA	Control Room Habitability Area
CRHS	Control Room Habitability System

## ACRONYMS AND ABBREVIATIONS

CWS	Chilled Water System
DAS	Data Acquisition System
DATALINK	A communication path between two systems – almost always by fiber-optic cable.
DC	Direct Current
DCD	Design Control Document
DCIS	Distributed Control and Information System
DPS	Diverse Protection System
DPV	Depressurization Valve
EB	Electrical Building
ECCS	Emergency Core Cooling System
EHC	Electrohydraulic Control
EQV	Equalizing Valve
EMI	Electromagnetic Interference
EOF	Emergency Operations Facility
ESD	Electrostatic Discharge
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Features (ESF) Actuation System
FAPCS	Fuel and Auxiliary Pools Cooling System
FB	Fuel Building
FMCRD	Fine Motion Control Rod Drive
FOAKE	First-of-a-Kind Engineering
FW	Feedwater
FWCS	Feedwater Control System
GATEWAY	A device representing a “translator” between two datalinked systems
GDC	General Design Criteria (or Criterion)

## ACRONYMS AND ABBREVIATIONS

GDCS	Gravity-Driven Cooling System
GDS	Gated Diode Switch
HCU	Hydraulic Control Unit
HFE	Human Factors Engineering
HMI	Human-Machine Interface
HP CRD	High Pressure Control Rod Drive (or Control Rod Drive high pressure makeup water injection)
HSI	Human-System Interface
HVAC	Heating, Ventilation and Air Conditioning
I&C	Instrumentation & Control
IAS	Instrument Air System
IC	Isolation Condenser
ICP	Independent Control Platform
ICS	Isolation Condenser System
IDIF	ICS DPV Isolation Function
IEEE	Institute of Electrical and Electronics Engineers
INOP	Inoperable
kV	Kilovolt (1000 volts)
LD&IS	Leak Detection and Isolation System
LFCV	Low Flow Control Valve
LOCA	Loss-of-Coolant-Accident
LPRM	Local Power Range Monitor
LTR	Licensing Topical Report
Deleted	Deleted
MCR	Main Control Room
MRBM	Multi-Channel Rod Block Monitor
MSIV	Main Steam Isolation Valve

## ACRONYMS AND ABBREVIATIONS

N-DCIS	Nonsafety-related Distributed Control and Information System
NDL	Nuclear Data Link
NI	Nuclear Island
NIC	Network Interface Card
NMS	Neutron Monitoring System
NRC	Nuclear Regulatory Commission
PAS	Plant Automation System
PCCS	Passive Containment Cooling System
PCD	Plant Configuration Database
PCF	Plant Computer Function(s)
PIP	Plant Investment Protection
PLC	Programmable Logic Controller
PMC	Performance Monitoring and Control
PRA	Probabilistic Risk Assessment
PSWS	Plant Service Water System
Q-DCIS	Safety-related Distributed Control and Information System
RAT	Reserve Auxiliary Transformer
RB	Reactor Building
RBM	Rod Block Monitor
RC&IS	Rod Control and Information System
RCCWS	Reactor Component Cooling Water System
RCS	Reactor Coolant System
RFI	Radio Frequency Interference
RG	Regulatory Guide
RMU	Remote Multiplexer Unit

## ACRONYMS AND ABBREVIATIONS

RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RSS	Remote Shutdown System
RTIF	Reactor Trip and Isolation Function(s)
RTOS	Real-Time Operating System
RW	Radwaste Building
RWCU/SDC	Reactor Water Cleanup and Shutdown Cooling System
RWM	Rod Worth Minimizer
SB	Service Building
SB&PC	Steam Bypass and Pressure Control
SBWR	Simplified Boiling Water Reactor
SCRR	Selected Control Rod Run-In
SDG	Standby Diesel Generator
SIU	Signal Interface Unit
SLC	Standby Liquid Control
SOE	Sequence of Events
SPDS	Safety Parameter Display System
SPTM	Suppression Pool Temperature Monitoring
SRI	Select Rod Insert
SRNM	Startup Range Neutron Monitor
SRV	Safety Relief Valve
SSLC	Safety System Logic and Control
TBV	Turbine Bypass Valve
TCV	Turbine Control Valve
TCCWS	Turbine Component Cooling Water System
TGCS	Turbine Generator Control System

## ACRONYMS AND ABBREVIATIONS

TMI	Three Mile Island
TMR	Triple Modular Redundant
TRA	Transient Recording and Analysis
TSC	Technical Support Center
TSV	Turbine Stop Valve
UAT	Unit Auxiliary Transformer
VBIF	Vacuum Breaker Isolation Function
VDU	Video Display Unit
WDP	Wide Display Panel

## GLOSSARY OF TERMS

This section contains clarifications of terms used in this report that are defined in NUREG/CR-6303 (Reference 6-1). These definitions are provided to aid in the understanding of the report text, instrumentation and control architecture, and conformance to guidelines. The definitions and clarifications may vary from corresponding definitions in Reference 6-1 because of development and evolution of the ESBWR I&C architecture. *Definitions verbatim from Reference 6-1 are italicized.*

### Anticipated Operational Occurrences

*“Those conditions of normal operation which are expected to occur one or more times during the life of the nuclear power unit and include, but are not limited to loss of the turbine generator set, isolation of the main condenser and loss of offsite power.”* (10 CFR 50, Appendix A, Definition and Explanations).

Subsection 15.0.1 of the ESBWR Design Control Document (DCD) (Reference 6-3), ‘Classification and Selection of Events,’ provides the definition and discussion of Anticipated Operational Occurrences.

### Accidents

*“Accidents are defined as those conditions of abnormal operation that result in limiting faults. These are occurrences that are not expected to occur but are postulated because their consequences would include the potential for the release of a significant amount of radioactive material.”* (Standard Format, Section 15, ‘Accident Analysis,’ NRC Reg. Guide 1.70).

Subsection 15.0.1 of Reference 6-3 provides the definition and discussion of Accidents.

### Block

*“Generally, a system is described as an arrangement of components or black boxes interconnected by communication, electrical connections, pipes, or physical effects. This kind of description, often called a ‘system architecture,’ may be too complex or may not be partitioned conveniently for diversity and defense-in-depth analysis. A more convenient description may be obtained by restricting the portion of the system under consideration to instrumentation and control equipment and partitioning the restricted portion into ‘blocks.’ A ‘block’ is the smallest portion of the system under analysis for which it can be credibly assumed that internal failures, including the effects of software errors, will not propagate to other equipment. The objective of choosing blocks is to eliminate the need for detailed examination of internal failure mechanisms while examining system behavior under reasonable assumptions of failure containment.*

*“Examples of typical software-containing blocks are computers, local area networks or multiplexers, or programmable logic controllers (PLCs). A block can be solely hardware, but there are no solely software blocks; software-containing blocks suffer the distinction that both hardware or software faults (and sometimes both acting together) can cause block failure. Consequently, it is difficult to separate the effects of software from the machine that executes that software. For example, a software defect in one small routine can cause an entire computer to fail by corruption of other data or software.”*

### Channel

*"A channel is defined as a set of interconnected hardware and software components that processes an identifiable sensor signal to produce a single protective action signal in a single division when required by a generating station condition. A channel includes the sensor, data acquisition, signal conditioning, data transmission, bypasses, and logic up to voters or actuating device inputs. The objective of the channel definition is to define subsets of a reactor protection system that can be unambiguously tested or analyzed from input to output."*

#### Common-Mode (or -Cause) Failure

*"Common-mode failures (CMFs) are causally related failures of redundant or separate equipment. For example, (1) a CMF of identical subsystems across redundant divisions defeats the purpose of redundancy, or (2) a CMF of different subsystems or echelons of defense defeats the use of defense-in-depth. CMF embraces all causal relations, including severe environments, design errors, calibration and maintenance errors, and consequential failures..."*

For this report, a distinction is made between CMFs and multiple failures. CMFs are further discussed in subsection 3.2. Multiple failures are addressed in the ESBWR Probabilistic Risk Assessment (PRA).

#### Defense-in-Depth

*"Defense-in-depth is a principle of long standing for the design, construction and operation of nuclear reactors, and may be thought of as requiring a concentric arrangement of protective barriers or means, all of which must be breached before a hazardous material or dangerous energy can adversely affect human beings or the environment. The classic three physical barriers to radiation release in a reactor - cladding, reactor pressure vessel, and containment - are an example of defense-in-depth."*

#### Diversity

*"Diversity is a principle in instrumentation systems of sensing different parameters, using different technologies, using different logic or algorithms, or using different actuation means to provide several ways of detecting and responding to a significant event. Diversity is complementary to the principle of defense-in-depth and increases the chances that defenses at a particular level or depth will be actuated when needed. Defenses at different levels of depth may also be diverse from each other. There are six important types of diversity to consider:*

- *Human diversity,*
- *Design diversity,*
- *Software diversity,*
- *Functional diversity,*
- *Signal diversity, and*
- *Equipment diversity.*

On the ESBWR, Diversity in instrumentation or sensors used to perform the same function is achieved by one of the following two (2) methods:

- Use of different principles of operation from the same or different manufacturer(s)

- Use of similar principles of operation from different manufacturer(s)

Devices using the same principles of operation or transducer technologies from the same manufacturer(s), but procured separately as safety-related and nonsafety-related, are not considered to meet diversity requirements.

The requirement of diverse instrumentation or sensors as implemented on the ESBWR is clarified as follows:

- All safety-related digital hardware/software control platforms (Q-DCIS) (i.e.; RTIF-NMS, SSLC/ESF, ICP) must use signals from physically independent sensors but they do not have to come from diverse sensors.
- Diverse Protection System (DPS), a nonsafety-related digital hardware/software control platform, must use signals from sensors that are diverse from those used on the safety-related digital hardware/software (Q-DCIS) platforms.

Other nonsafety-related digital hardware/software control platforms can use signals from any available non safety-related sensors independent of their diversity and can share signals from the same sensors as long as the control platform using these signals has three or more measurement inputs of the controlled parameter concerned.

#### Echelons of Defense

Reference 6-1 provides definitions of four echelons of defense. The definition of each level is reproduced in the following along with a brief description of the ESBWR I&C systems that accomplish the task.

- (1) Control System [Nonsafety-Related Distributed Control and Information System (N-DCIS)].

*"The control echelon is that nonsafety-related manual or automatic equipment which routinely prevents reactor excursions toward unsafe regimes of operation and is generally used to operate the reactor in the safe power production operating region. Indicators, annunciators, and alarms may be included in the control echelon. Reactor control systems typically contain some nonsafety-related equipment to satisfy the ATWS rule (10 CFR 50.62) or the requirement for a safety-related remote shutdown panel. Examples of such equipment include high-quality nonsafety-related equipment for which credit may be taken solely for compensating rare common-mode failures of safety-related reactor protection equipment... "*

The functions performed by the control system echelon of defense are included in the N-DCIS. These systems normally function to maintain the plant within operating limits to avoid the need for a reactor trip or Engineered Safety Feature (ESF) actuation. All of the ESBWR control systems involved in normal power generation are at least dual redundant.

- (2) Reactor Trip or Scram System [Reactor Protection System (RPS)]

*"The reactor trip echelon is that safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion. It consists of instrumentation for detecting potential or actual excursions, means for rapidly and completely inserting the reactor*

*control rods, and may also include certain chemical neutron moderation systems (e.g., boron injection)."*

The automatic reactor trip functions performed by the reactor trip echelon of defense are included in the Safety-related Distributed Control and Information System (Q-DCIS), specifically by the RPS that is part of the Reactor Trip and Isolation Function (RTIF)-Neutron Monitoring System (NMS) platform. As will be later described, the nonsafety-related Diverse Protection System (DPS) also provides automatic and manual reactor trip capabilities. Reactor trip and scram are used as interchangeable terms in this document.

(3) ESF Actuation System [Safety System Logic and Control (SSLC)/Engineered Safety Feature (ESF) RTIF-NMS and Independent Control Platform (ICP)]:

*"The ESFAS echelon is that safety equipment that removes heat or otherwise assists in maintaining the integrity of the physical barriers to radioactive release (cladding, vessel, and containment). This echelon detects the need for and performs such functions as emergency cooling, pressure relief or depressurization, isolation, and control of various support systems (e.g. emergency generators) or devices (valves, motors, pumps) required for ESF equipment to operate."*

The functions associated with the automatic ESF actuation echelon are primarily performed by the Safety System Logic and Control (SSLC)/ESF logic platform. Some isolation logic is implemented in the RTIF-NMS logic platform and Independent Control Platform (ICP). The aforementioned logic platforms are part of the Q-DCIS. The nonsafety-related DPS also provides automatic actuation capability for a subset of Emergency Core Cooling System (ECCS) components and containment isolation components. The ESBWR is a passive plant and does not require emergency generators, motors, or pumps to perform its ECCS functions.

(4) Monitoring and Indicator System [N-DCIS, Q-DCIS]:

*"The monitoring and indication echelon is the slowest and also the most flexible echelon of defense. Like the other three echelons, operators are dependent upon accurate sensor information to perform their tasks, but, given information, time and means, can perform previously unspecified logical computations to react to unexpected events. The monitoring and indication echelon includes both safety-related and nonsafety-related manual controls, monitors, and indicators required to operate components nominally assigned to the other three echelons."*

Monitoring and indication functions are provided by both the N-DCIS and Q-DCIS. The safety-related manual reactor trip and manual ESF actuation functions performed by the monitoring and indication echelon of defense are included in the Q-DCIS. The nonsafety-related DPS also provides manual reactor trip and a subset of manual ESF actuation capabilities. The Q-DCIS design provides the flexibility to display process parameters monitored by safety-related sensors. The N-DCIS design provides the flexibility to display process parameters monitored by safety-related and nonsafety-related sensors. The Human Factors Engineering design process described in Tier 2 Chapter 18 of Reference 6-3 finalizes the development of the indication required to support manual component operation.

### Instrumentation System

*“A reactor instrumentation system is that set of equipment that senses various reactor parameters and transmits appropriate signals to control systems, to the reactor trip system, to the engineered safety features actuation system, and to the monitoring and indicator system for use in determining the actions these systems or reactor operators will take. Independence is required between control systems, safety monitoring and display systems, the two safety systems, and between redundant divisions of the safety systems.”*

In this report, the instrumentation system includes the following systems in the I&C architecture (refer to Subsections 7.1.3.2 and 7.1.4.8 of DCD Tier 2 [Reference 6-3] for a listing of [Q-DCIS and N-DCIS] I&C systems/functions):

- N-DCIS or cabinets including:
  - GENE Systems
  - DPS (part of the GENE Systems),
  - Plant Investment Protection A,
  - Plant Investment Protection B,
  - Balance of Plant Control, and
  - Plant Computer Functions,
  - Severe Accident Deluge Lines Flooder System ([also called the GDCS Deluge Subsystem] part of the PCF Network).
- Q-DCIS or cabinets including:
  - Reactor Trip and Isolation Function (RTIF), (the RTIF includes the RPS and the Main Steam Isolation Valve [MSIV] logic of the Leak Detection and Isolation System [LD&IS]).
  - Neutron Monitoring System (NMS)
  - Anticipated Transients Without Scram/Standby Liquid Control System - (ATWS/SLC) logic (consisting of independent controllers that are physically located in the RTIF cabinets).
  - Containment System Vacuum Breaker Isolation Function (VBIF) (consisting of independent controllers that are physically located in the RTIF cabinets).
  - Control Rod Drive high pressure makeup water injection (HP CRD) Isolation Bypass function (consisting of independent controllers that are physically located in the RTIF cabinets).
  - SSLC/ESF (includes logic for the ECCS [Isolation Condensers, Automatic Depressurization System, Gravity-Driven Cooling System and Standby Liquid Control System], Control Room Habitability System [CRHS], Non-MSIV LD&IS, certain safety-related functions of the Containment Monitoring System [CMS], and safety-related information systems).

## 1. INTRODUCTION

### 1.1 PREFACE

Since the Simplified Boiling Water Reactor (SBWR) was originally designed, there have been dramatic changes and improvements in power plant Distributed Control and Information Systems (DCIS) and there has been a slow but continuous introduction of retrofit safety-related and nonsafety-related digital control systems into operating nuclear power plants. The control systems concepts were further improved as part of the U.S. certification and First-of-a-Kind Engineering program (FOAKE) of the Advanced Boiling Water Reactor (ABWR) which incorporated industry guidance and requirements from the Advanced Light Water Reactor (ALWR) Utility Requirements Document; a good starting point for DCIS reliability and safety-related system challenges, is represented by recent ABWR contractual requirements that the DCIS be single failure proof/one failure per 50 years for power generation. Experience gained from the delivery of an ABWR DCIS in Japan and, most recently Taiwan (where U.S. standards were closely followed) has been incorporated into the ESBWR DCIS systems.

Changes beyond the ABWR design have been incorporated because of the ESBWR passive safety-related systems and new regulatory requirements that must also be considered in the diversity assessment:

Probabilistic Risk Assessment (PRA) methods are used to consider the role of both safety-related and nonsafety-related equipment in the prevention and mitigation of transients and faults. This consideration has been reflected in the overall design of the ESBWR plant DCIS and mechanical systems.

The nonsafety-related Diverse Protection System (DPS) provides reactor trip and Engineered Safety Features (ESF) actuations diverse from the Safety-related Distributed Control and Information System (Q-DCIS). The DPS is included to support the ESBWR risk goals by reducing the probability of a severe accident that potentially results from the unlikely coincidence of postulated transients and postulated Common-Mode Failures (CMFs).

In December 1994, the Nuclear Regulatory Commission (NRC) published Reference 6-1, which describes a deterministic method of analyzing computer-based nuclear reactor protection systems that identifies and evaluates design vulnerabilities to CMF. The ESBWR I&C system functions follow the SBWR instrumentation and control systems and the ABWR hardware and software applications, which were designed and analyzed before Reference 6-1 was published. As with the SBWR design, PRA methods are used for the analysis of systems used to provide ESBWR diversity and defense-in-depth. These PRA methods are consistent with Reference 6-1 and allow the designers to concentrate on situations that are the largest potential contributors to the predicted core melt frequency. A deterministic assessment of the Reference 6-3 Tier 2 Chapter 15 events is also performed and documented in Appendix A to demonstrate ESBWR digital protection system common mode failure coping.

### 1.2 ARCHITECTURE OVERVIEW

The Q-DCIS is a safety-related I&C system that is included in the ESBWR distributed control and information systems architecture to address the anticipated operational occurrences and

accidents outlined and described in Chapter 15 of the ESBWR Design Control Document (DCD) Tier 2 (Reference 6-3). The Q-DCIS design complies with NEDO-33245P – Software Quality Assurance Program Manual (Reference 6-4) and specifically meets plant licensing requirements by including design features such as:

- Redundancy,
- Functional diversity,
- Fail safe design,
- Continuous self-diagnostics,
- Periodic surveillance test capability,
- Isolation (division to division and division to nonsafety-related), and
- A design verification and validation process.

Subsection 3.3 describes the fault tolerant features of the Q-DCIS.

The DPS is a nonsafety-related I&C system whose functions augment those of the Anticipated Transients without Scram/Standby Liquid Control system (ATWS/SLC) logic included in the ESBWR and the ABWR. The DPS enables the ESBWR DCIS to meet reliability goals, when the Q-DCIS is assumed to fail as a result of a postulated beyond design basis software CMF. The DPS design complies with the applicable requirements outlined in NEDO-33245P – Software Quality Assurance Program Manual (Reference 6-4).

### 1.3 SCOPE

Diversity is a principle in instrumentation systems of sensing different variables, using different technology, using different logic or algorithms, or using different actuation means to provide multiple ways of responding to postulated plant conditions. Reference 6-1 describes six types of diversity:

- Human,
- Design,
- Software,
- Functional,
- Signal, and
- Equipment.

Reference 6-1 defines echelons of defense as:

*“...specific applications of the principle of defense-in-depth to the arrangement of I&C systems attached to a nuclear reactor for the purpose of operating the reactor or shutting it down and cooling it. Specifically, the echelons are the control system, the reactor trip or scram system, the engineered safety features actuation system (ESFAS), and the monitoring and indicator system.”*

The following sections describe the types of diversity that exist among the four echelons of defense and identify dependencies between the echelons. Redundancy and segregation are also discussed.

## **1.4 SUMMARY AND CONCLUSIONS**

### **1.4.1 Compliance with NUREG-0493**

The I&C architecture meets the expectations of NUREG-0493 (Reference 6-8); in particular, Section 2, "Technical Discussion:" and Section 3.3 "Guidelines," which contain guidelines, requirements, and recommendations.

### **1.4.2 Compliance with NUREG/CR-6303**

The I&C architecture complies with Reference 6-1, in particular, Section 3 "Guidelines," which contains guidelines, requirements, and recommendations.

### **1.4.3 Compliance with DI&C-ISG-02**

The manual and automatic features of the DPS comply with Reference 6.14, which contains guidance, clarifications and recommendations.

### **1.4.4 Meeting Probabilistic Safety-Related Goals**

The analysis of protection against CMF has been conducted in parallel with the development of the PRA. In the PRA, failures of the I&C architecture, including common cause failures, are analyzed. The PRA report NEDO-33201 (Reference 6-7) describes these analyses. The conclusion is that the I&C architecture is, as calculated by PRA analysis, sufficient to meet probabilistic safety-related goals.

## 2. ESBWR INSTRUMENTATION AND CONTROL ARCHITECTURE / SYSTEMS DESCRIPTION

### 2.1 ARCHITECTURE DESCRIPTION

The architecture of the I&C associated function is shown in Figure 1. This figure is a simplified representation of the ESBWR I&C architecture that illustrates the interactions between the various safety-related and nonsafety-related components. Divisional Q-DCIS cabinets are located in one of the four dedicated DCIS rooms appropriate to their division. The nonsafety-related Distributed Control and Information System (N-DCIS) cabinets and components are located in one of two nonsafety-related DCIS rooms; although also nonsafety-related, the DPS control cabinet is located separately from the other nonsafety-related control system cabinets. Specifically the four (redundant) divisional safety-related control systems of the Q-DCIS are physically separated from each other and from the nonsafety-related control systems of the N-DCIS and from the DPS. The two trains of the nonsafety-related plant investment protection (PIP) system controllers are physically separated from each other and from the Q-DCIS and the DPS.

Communication between the safety-related and nonsafety-related DCIS is through fiber optic cable (fiber) and from Q-DCIS to N-DCIS [the only exceptions are time of day (used for time tagging safety-related data for later analysis but not for synchronization of the Q-DCIS) and Average Power Range Monitor/Local Power Range Monitor (APRM/LPRM) calibration which can only be done by making the affected instrument inoperable (INOP)]. All communication between divisions (to perform two-out-of-four logic) is also fiber isolated and one-way in the sense that no division is dependent on any other division for information, timing, data or the communication itself. No safety-related function depends on the accuracy or existence of any nonsafety-related communication, or any nonsafety-related component.

Almost all communication to/from the field Remote Multiplexing Units (RMUs) is by fiber and all communication from the DCIS rooms to the main control room (MCR) safety-related and nonsafety-related Video Display Units (VDUs) are via fiber. The few hard-wired exceptions are for signals like main turbine trip or reactor scram signals. These MCR considerations are important because the communications protocol is such that a failure of a fiber will not cause erroneous operation nor affect the continued operation of all automatic safety-related or nonsafety-related systems. Likewise, operation of the VDUs<sup>1</sup> requires several operator actions whose resulting communication is unlikely to be replicated by communications loss or damage; similarly the DCIS represents a distributed network whose nodal addresses are equally unlikely to be replicated by fiber loss.

The major functional groupings of the DCIS include:

- Safety-related Reactor Trip and Isolation Function (RTIF) cabinets. These cabinets include the fail-safe logic for the following systems and functions (in four redundant divisions):
  - Reactor Protection System (RPS),

<sup>1</sup> In this document the VDUs are assumed to be touch screen but further Human Factors Engineering analysis (as part of the HFE development process described in Chapter 18 of Reference 6-3) may dictate other operator pointing devices.

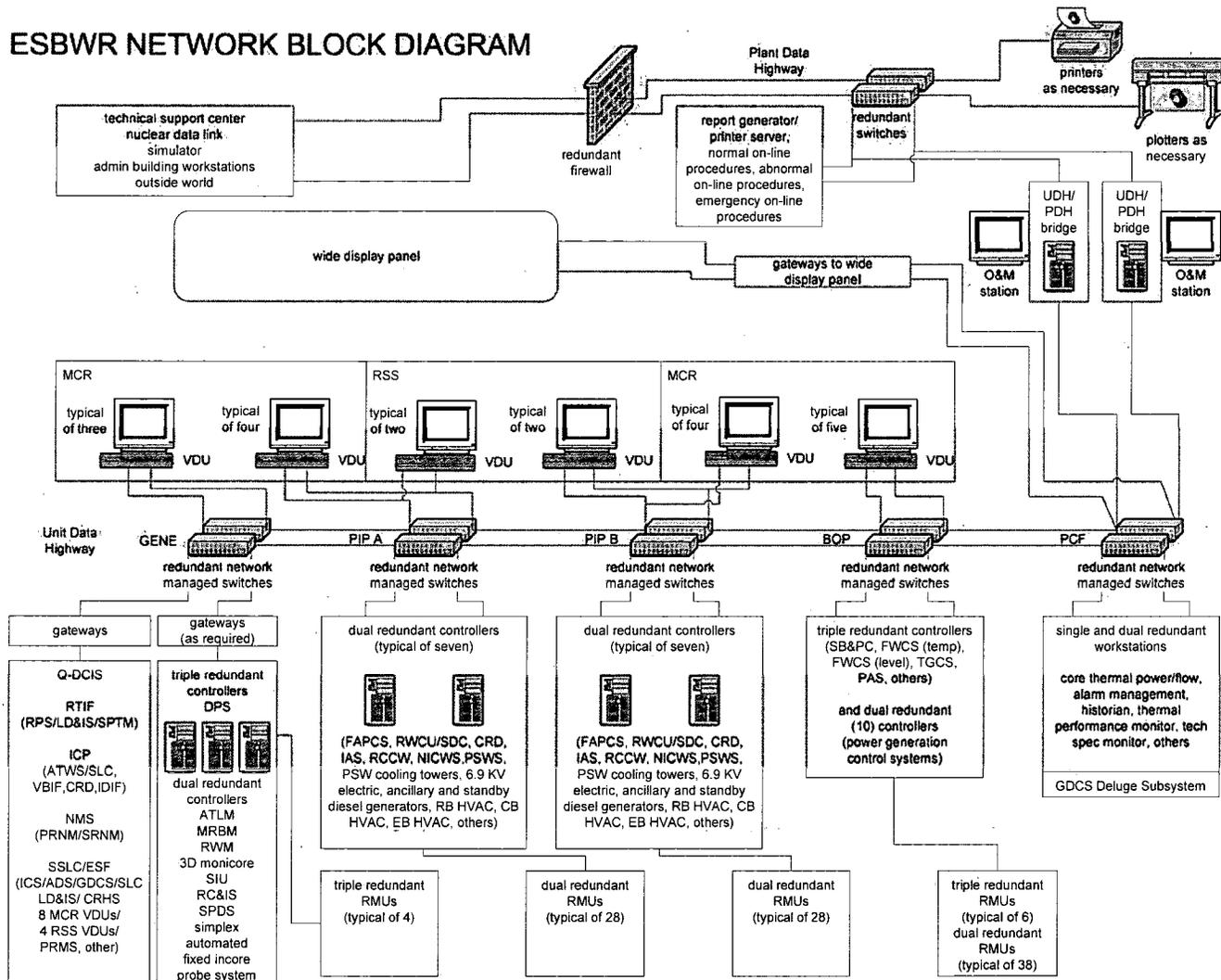
- (Nuclear Boiler System (NBS)) Main steam isolation valve (MSIV) and drain valve logic and MSIV and drain valve isolation functions of the Leak Detection and Isolation System (LD&IS)
- Suppression Pool Temperature Monitoring (SPTM) function of the Containment Monitoring System (CMS) – a process sensing function supporting RPS.
- Safety-related Neutron Monitoring System (NMS), including APRM, LPRM and Startup Range Neutron Monitor (SRNM) functions (four redundant divisions)
- Safety-related Independent Control Platform (ICP) - this functional group of fail-as-is logic consists of chassis that are physically located in the RTIF cabinets (four redundant divisions):
  - Anticipated Transient Without Scram/Standby Liquid Control System (ATWS/SLC) functions (includes ATWS mitigation logic processors and SLC system control logic processors),
  - Vacuum Breaker Isolation Function (VBIF) of the Containment System,
  - HP CRD Isolation Bypass function, and
  - ICS DPV isolation function

Space consideration may dictate locating the ICP hardware in separate cabinets.

- Safety System Logic and Control (SSLC)/ESF which provides safety-related fail-as-is ESF logic. Emergency Core Cooling System (ECCS) functions (four redundant divisions) which includes:
  - Isolation Condenser System (ICS) functions,
  - Automatic Depressurization System (ADS) functions of the NBS,
  - Gravity-Driven Cooling System (GDCCS) functions, and
  - Standby Liquid Control (SLC) System functions, and
  - LD&IS functions (non-MSIV),
  - Control Room Habitability System (CRHS) functions,
  - Containment Monitoring System (CMS) functions, and
  - Safety-related information systems.
  - The Process Radiation Monitoring System provides process-sensing inputs to the LD&IS and CRHS to support the isolation functions.
- Nonsafety-related nuclear systems of the N-DCIS that are divided into the following network segments
  - GENE systems (including DPS)
  - PIP A functions
  - PIP B functions
  - BOP Control, and

- Plant Computer Functions (PCF) [Performance monitoring and control (PMC), Historian, Alarm Management System (AMS), etc], and
- Severe Accident Mitigation Deluge Lines Flooder System, which is associated with the PCF network.
- The N-DCIS also provides the control logic for the:
  - 3D-Monicores,
  - Rod Control and Information System (RC&IS),
  - Automated Thermal Limit Monitor (ATLM),
  - Multi-Channel Rod Block Monitor (MRBM),
  - Rod Worth Minimizer (RWM),
  - Signal Interface Unit (SIU),
  - Logic for the Safety Parameter Display System (SPDS),
  - DPS,
  - Datalinks and gateways to translate and distribute data between Q-DCIS and N-DCIS
  - MCR VDUs, and
  - AFIP, and
  - Tech spec monitor.

Figure 1 ESBWR DCIS Architecture



The DCIS hardware and software architecture is compliant with NEDO-33226P – Software Management Plan (Reference 6-5). The configuration supports:

- Controlling and monitoring of the safety-related systems on the safety-related displays that are unaffected by the status of the N-DCIS,
- The alarm management of safety-related systems on the N-DCIS (through isolated data links from the four divisions (control of Q-DCIS from N-DCIS is not possible through the data links),
- Dual and triple redundancy for all important PCF and for control of power generation systems,
- Segmented PIP systems, and
- A high quality nonsafety-related DPS that can perform a subset of reactor scrams, isolations, and ESF actuations without affecting or interfering with its safety-related counterparts.

The ESBWR DCIS uses methodologies mandated by the various regulations to maximize control system reliability and safety as delineated in Table 7.1-1, “I&C Systems Regulatory Requirements Applicability Matrix,” and described in Subsection 7.1.1, “Distributed Control and Information System,” of the ESBWR DCD (Reference 6-3). Design principles such as physical and electrical independence, redundancy, segmentation and diversity are employed. Diversity is employed for the various control systems.

As indicated in Figure 2, within the Q-DCIS, RTIF-NMS, SSLC/ESF and ICP each use diverse hardware and software. In turn the RTIF-NMS logic platform, ICP, and SSLC/ESF logic platform of the Q-DCIS use hardware and software that is diverse from the N-DCIS systems, specifically including the DPS, which provides a completely diverse backup design to most protection functions in the Q-DCIS. The severe accident Deluge Lines Flooder System is also diverse from both Q-DCIS and N-DCIS. Figure 3 indicates the logic platform and power relationships between the various diverse I&C systems.

On the N-DCIS side, the important nuclear instrumentation and control systems, such as DPS, use triple modular redundant (TMR) controllers to improve their reliability for power generation and, in the case of DPS, to provide reliability for both the backup scram and ESF/ECCS functions and to prevent inadvertent actuations.

The control schemes assigned to the specific DCIS cabinets are appropriately segregated; for example, the RMUs, control processors and displays that operate PIP A systems are separate from those operating PIP B systems; similarly reactor pressure control and reactor level control are in different cabinets (this is discussed below). These cabinets/systems are connected by means of hardwired conductors, data links/gateways, and data highways (real time networks).

The I&C architecture is hierarchical. “Above” the real time data network are the PCF whose purpose is to provide and facilitate the interaction between the plant operators and the DCIS. These specifically include, the plant Alarm Management System (AMS), the operator displays and the Safety Parameter Display System (SPDS). Also included in these functions is the secure communication (plant firewall) that protects the N-DCIS networks from and interfaces with external systems requiring data from the plant [Nuclear Data Link (NDL), Technical Support

Center (TSC), Emergency Offsite Facility (EOF), etc.]. “Below” the real time data network are those systems that perform the protective, control and monitoring functions.

The Human System Interface (HSI) functions of the DCIS define the arrangement of the MCR, the layout of the DCIS equipment in the Control Room and Remote Shutdown System (RSS) panels, and dictate the design process for the layout and content of operating and safety-related displays, alarms, controls, and procedures for the HSI. The HSI functions, developed under the formal Human Factors Engineering (HFE) plans, are defined in the appropriate I&C sections of the ESBWR Design Control Document (Reference 6-3).

Figure 4 is a functional representation of the MCR panels. The design is contingent upon final HFE analyses. There are five principle control room panels.

The Wide Display Panel (WDP), which is nonsafety-related, displays the plant mimic, variable display sections, and group viewable alarm notification communicators.

The Main Control Console is the primary operator interface, and also houses compartmentalized (one per division) sections housing VDUs and manual switches. The remainder of the Main Control Console houses the nonsafety-related VDUs and hard controls [for example, main turbine trip, control rod insert/withdraw (in manual mode)] that are used for normal plant operation. The plant can be manually scrammed and the MSIVs isolated from Main Control Console switches that are independent of software; similarly the main turbine can be tripped without software. Although the nonsafety-related displays are segmented in that they are driven by the PIP A, PIP B and BOP portions of the N-DCIS, in normal operation they appear “seamless” to the operator and all displays can control and monitor all nonsafety-related equipment that the operator selects. The segmentation of the nonsafety-related DCIS allows operation of each segment independently should another segment be lost (the “uplinks” between the segmented network switches are by fiber).

The Main Control Console has four divisional VDUs from which safety-related systems can be both monitored and controlled. The safety-related VDUs use touch screen technology diverse from that of the nonsafety-related VDUs, and are completely isolated from the N-DCIS and from each other.

The Shift Supervisor Console contains nonsafety-related VDUs from which the supervisor can monitor safety-related and nonsafety-related systems. All nonsafety-related displays are part of the PCF (a sub-system of the N-DCIS) and are implemented using a distributed architecture. The distributed PCF subsystem obtains input from the real-time data network and delivers output over the network to other users and to the nonsafety-related displays.

A Left Side Panel contains four divisional VDUs from which safety-related systems can be monitored and controlled. This panel also contains four nonsafety-related VDUs for surveillance. Separation/isolation is maintained between the safety-related and nonsafety-related equipment, and between each division of safety-related equipment. The Left Side Panel contains the hard control and bypass switches that contribute to ESBWR diversity.

A Right Side Panel contains nonsafety-related VDUs, standby and ancillary diesel generator synchronizing panels, and a fire protection panel and display.

In addition to diversity, the ESBWR power and DCIS are also functionally separated to minimize the potential failures due to common mode physical events. Figure 5 is a simplified illustration of the ESBWR raceway system; the ESBWR raceways, conduits and duct banks fully

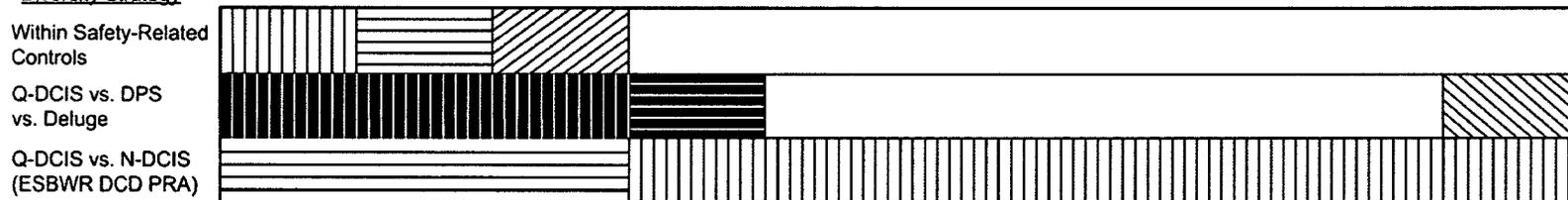
support the divisional and non-divisional separation criteria. The four divisions of RPS and NMS cabling are always in four separated raceways/conduits and the very low level signals on LPRM and SRNM cables are further segregated from all other wiring. The signals representing the Hydraulic Control Unit (HCU) scram solenoid currents in division 1 and 2 are also further subdivided into four scram groups (per division) and segregated from each other and all other plant wiring.

Figure 5 also indicates other safety-related and nonsafety-related signal, fiber and power separation. An example is the SSLC/ESF separation into four divisions whose fibers and wires are in four separated raceways/conduits. An example of nonsafety-related separation is the PIP "A" and "B" dual redundant fibers in separate raceways/conduits.

Figure 2 Hardware/Software (Platform) Diversity

Safety Category	Safety-Related			Nonsafety-Related						
	Q-DCIS			N-DCIS						
Platform/Network Segment	RTIF NMS	SSLC/ESF	Independent Control Platform	GENE		PIP A/B	BOP		PCF	
Architecture	Divisional	Divisional	Divisional	Triple Redundant (DPS)	Dual Redundant	Dual Redundant	Triple Redundant	Dual Redundant	Workstations	PLC (Deluge)

Diversity Strategy



NOTE: Crosshatching denotes different platforms or networks.

Figure 3 ESBWR Logic Platform and Power Diversity

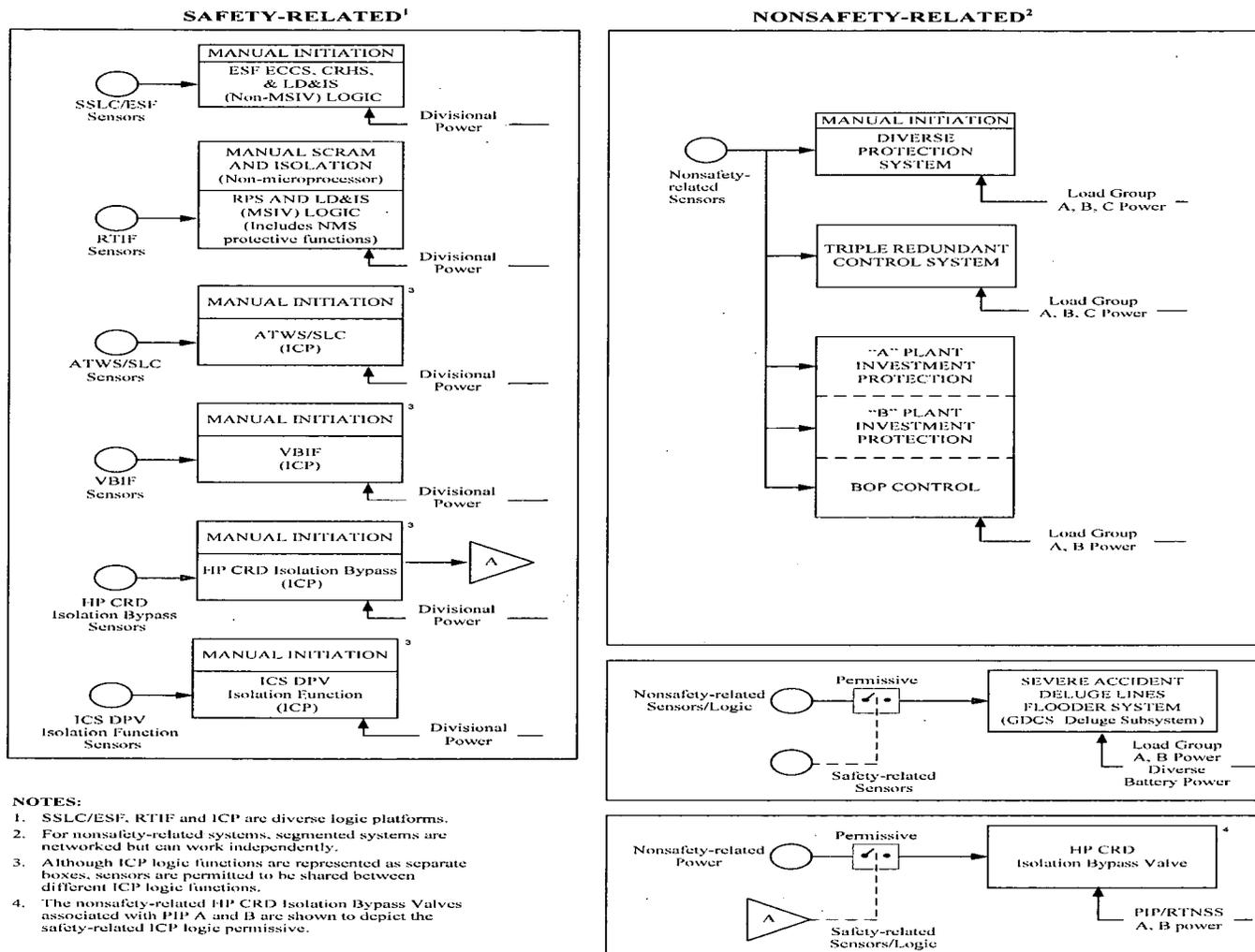


Figure 4 Main Control Room Layout - Typical

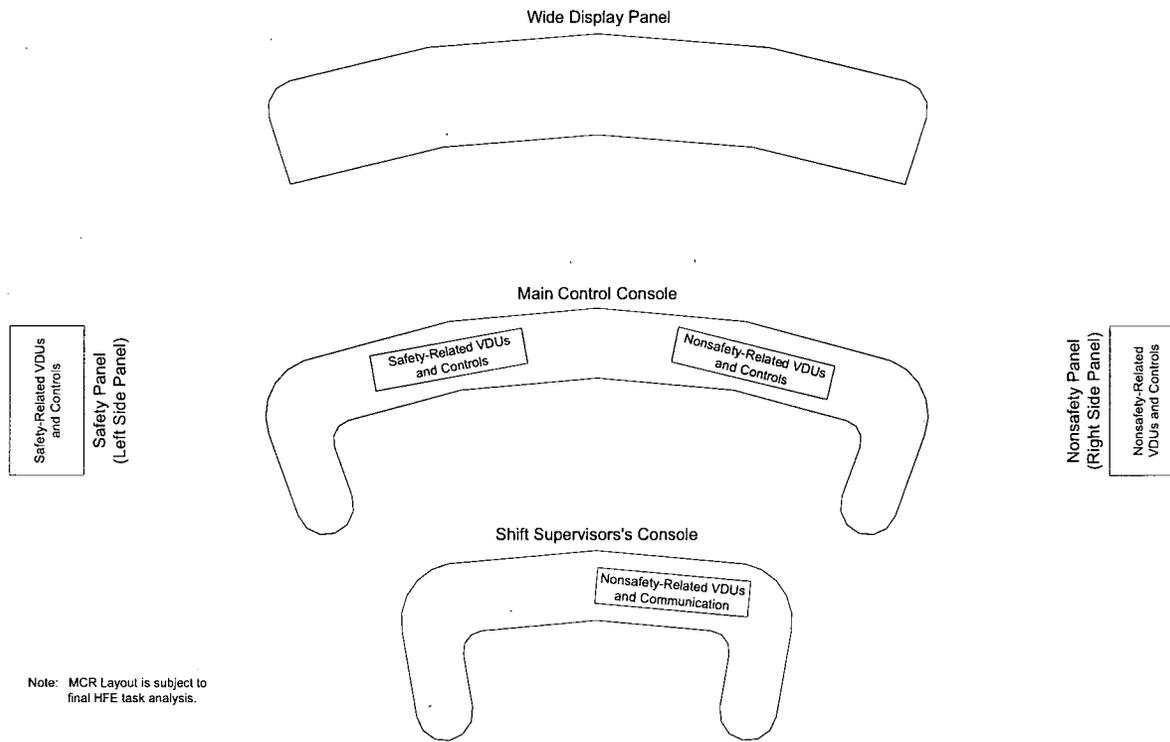
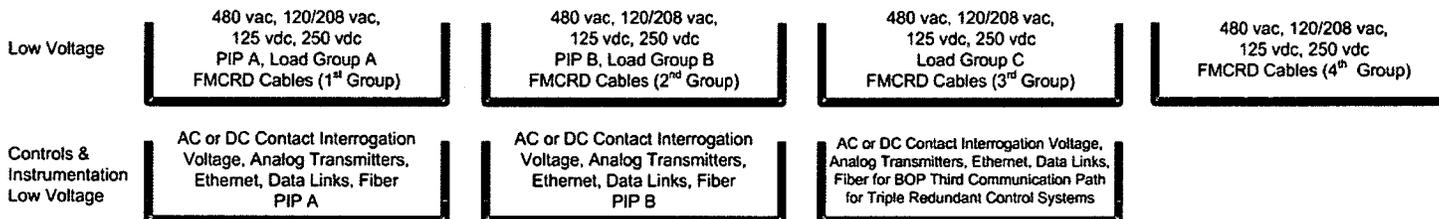
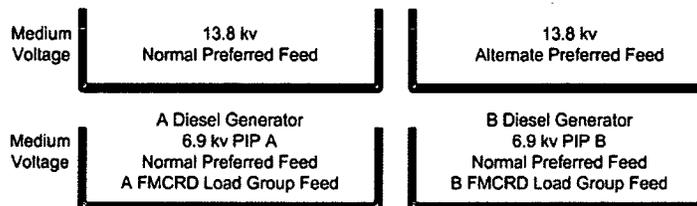


Figure 5 ESBWR DCIS and POWER Separation

The raceway, duct bank and conduit systems of the ESBWR are designed to provide physical separation of divisional cables from both other divisions and from nonsafety-related cables.

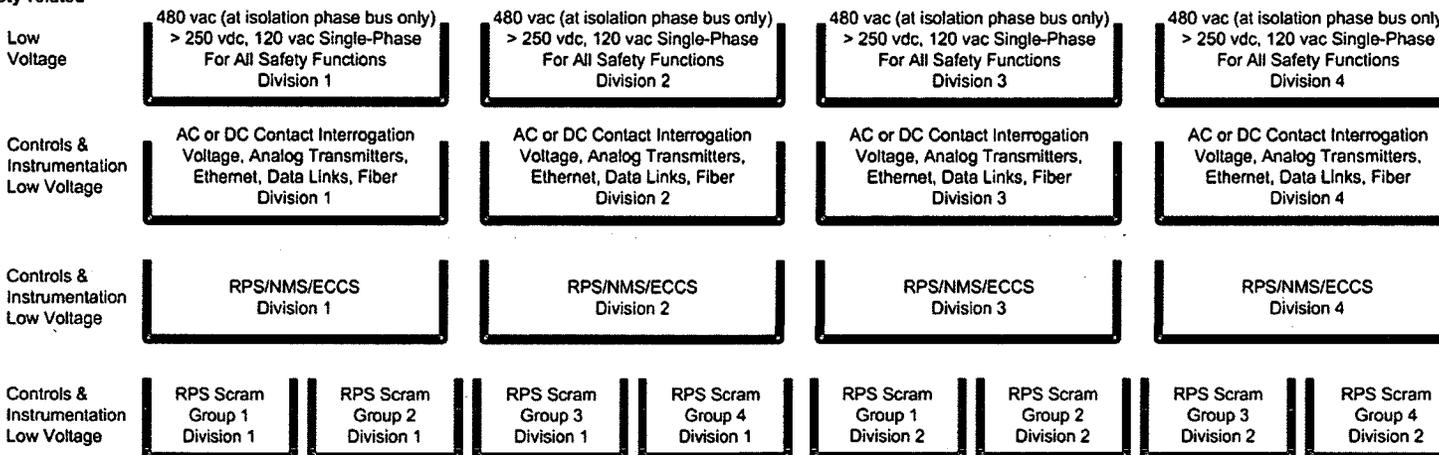
The raceway system also minimizes the potential for EMI/RFI interference (already very low because of the extensive use of fiber optics) by separating instrumentation cabling from large power cables.

Finally RPS and NMS copper cables are conduit separated even with a division to prevent hot shorts and generally prevent any interference with a required reactor scram.



Nonsafety-related

Safety-related



## 2.2 SAFETY-RELATED DISTRIBUTED CONTROL AND INFORMATION SYSTEM OVERVIEW

The Q-DCIS consists of the RTIF-NMS logic platform, the ICP and the SSLC/ESF logic platform. These systems and their associated sensors are organized into four divisions; the VDUs associated with each division provide for the control of the safety-related ESF equipment and additionally provide the necessary monitoring of the plant safety-related functions during and following an accident as required by Regulatory Guide (RG) 1.97 (Reference 6-13). The two-out-of-four logic associated with the RTIF-NMS logic platform, ICP and SSLC/ESF logic platform and the unique nature of the ESBWR solenoid and squib actuators allow the plant to be designed as "N-2"; specifically, any two divisions can accomplish the safety-related trip and ESF functions. N-2 is a significant element of the defense-in-depth design of the ESBWR DCIS.

The general relationship of the Q-DCIS is shown in Figure 6. (There are also nonsafety-related functions of NMS that are part of the N-DCIS.) The RTIF logic processors are located in the RTIF cabinet (one per division in separate Q-DCIS rooms) that combines the RPS, LD&IS (for MSIVs and drains only), SPTM, VBIF, HP CRD Isolation Bypass Function, ATWS/SLC functions, and ICS DPV isolation function. Although all equipment located in the RTIF cabinet is appropriate to the division and everything in the cabinet is powered by the appropriate divisional uninterruptible and battery power, the VBIF, HP CRD Isolation Bypass, ATWS/SLC functions, and ICS DPV isolation function (which are part of the ICP) are segregated to separate chassis from the remaining RTIF logic processors and from one another. The ICP (i.e., VBIF, HP CRD Isolation Bypass, ATWS/SLC, and ICS DPV isolation) is diverse from the RTIF-NMS and SSLC/ESF logic platforms. All of the safety-related functions are implemented in hardware/software platforms diverse from the DPS.

The ESBWR RPS design has several important differences from other Boiling Water Reactor (BWR) scram logic and hardware (although many of these features were included in the ABWR design); these include:

- Per parameter trip (specifically there must be (for example) two un-bypassed level trips to scram, a pressure trip and a level trip will not cause a scram).
- No operator manipulation of the division of sensors and/or division of logic bypass, nor any operation of the RPS back panel inoperable switches can reduce scram logic redundancy to less than "any two un-bypassed same parameters in trip will cause a scram". Only one division at a time can be physically bypassed. The RPS (and MSIV LD&IS) is N-2 to scram/isolate.
- Communication with the nonsafety-related DCIS is one-way (Q-DCIS to N-DCIS) through fiber; the loss of this communication does not affect RPS functionality.
- Communication with other RPS divisions is one-way, fiber isolated, and does not mix divisional data.
- All signals are actively transported such that "fail safe" is not a "1" or a "0" but rather "trip on loss of communication". As a result, loss of communication from another division is interpreted as a trip signal (unless that division is bypassed) and loss of communication with a bypass joystick switch is interpreted as "no bypass".

- RPS (and Q-DCIS) logic is powered by divisional redundant (uninterruptible 120V AC) power supplies that are backed by redundant batteries; additionally, the systems are backed up by offsite power and either of the two diesel generators.
- The CRD Hydraulic Control Unit (HCU) scram solenoid power is local to the Reactor Building (RB) and switched by fiber driven two-out-of-four logic from the RPS logic processors (located in the RTIF cabinet in the Control Building (CB)). This avoids the long distance voltage drops to the solenoids in the older BWR designs and eliminates (along with using monitored, safety-related inverters for solenoid power) the need for Electric Protection Assemblies. Loss of communication from the CB RTIF cabinets is interpreted as a trip.
- The hardware, software and solenoid switching for the RPS are diverse from the DPS.

The ICP provides a safety-related platform that is diverse from the RTIF-NMS and SSLC/ESF platforms. The ICP implements the following ESF, diverse reactor shutdown, ATWS mitigation, and beyond design basis event mitigation functions (Reference 6-3 provides additional details on the ICP).

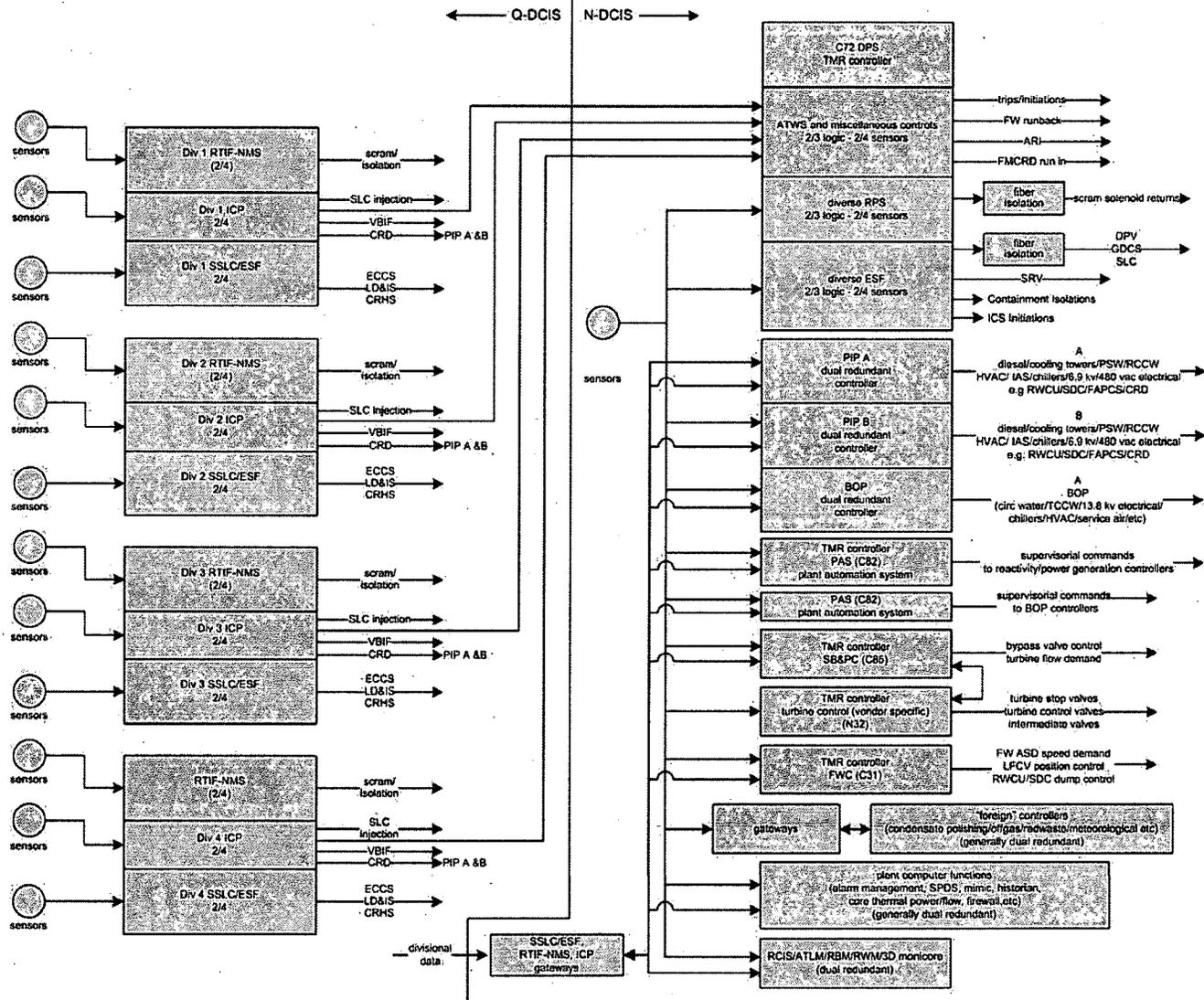
- ATWS/SLC – Certain ATWS mitigation functions are implemented as safety-related logic. The ATWS mitigation logic processors provide SLC initiation and feedwater runback signals, as well as ADS Inhibit logic that inhibits the sustained RPV Level 1, sustained drywell pressure high, and drywell pressure high-high initiation logic within the SSLC/ESF platform. SLC logic processors provide SLC system actuation and accumulator isolation functions in support of ATWS mitigation, diverse reactor shutdown, and ECCS operation. Isolation of the respective SLC accumulators on low accumulator level prevents nitrogen intrusion into containment to preclude a containment integrity or safety-related cooling system challenge.
- VBIF – To isolate a leak from (or failure of) any of the three Wetwell to Drywell vacuum breakers, the vacuum breaker isolation valve logic provides the backup means of isolating the Wetwell from the Drywell. The Vacuum Breaker Isolation valves provide a diverse means of system isolation to the mechanical vacuum breakers and are not required to mitigate a CCF of the RTIF-NMS or SSLC/ESF platforms.
- Control Rod Drive high pressure makeup water injection (HP CRD) Isolation Bypass function – HP CRD flow to the RPV is isolated by SSLC/ESF logic during accidents that could challenge peak containment pressure. As part of beyond design basis scenarios where injection of the GDCS pool inventory is not successful, HP CRD isolation is bypassed automatically by ICP logic to provide additional coolant inventory.
- ICS DPV isolation function – To automatically close the ICS steam admission valves upon opening of any two DPVs. Closing the ICS steam admission valves when the RPV is depressurized mitigates the accumulation of radiolytic hydrogen and oxygen.

The SSLC/ESF DCIS is implemented on a hardware/software platform that is a sub system of the Q-DCIS. The SSLC/ESF hardware/software platform is diverse from RTIF-NMS, ICP and the DPS. SSLC/ESF has a separate set of sensors from RTIF-NMS and ICP, and a diverse set of sensors from DPS. Since it is highly desirable to avoid the consequences of inadvertent actuation of ECCS (specifically automatic depressurization) and also important to reliably actuate ECCS when required, the SSLC/ESF ECCS logic is implemented on a triple redundant

hardware/software platform per division. The SSLC/ESF ECCS functions are described in more detail in Reference 6-3, but include the following systems/functions controlled by the SSLC/ESF DCIS:

- ADS (Safety Relief Valves (SRVs) and Depressurization Valves (DPVs)) - The (NBS) Reactor Pressure Vessel (RPV) SRVs are actuated by solenoids and the DPVs are actuated by explosive squibs. These valves are used to bring the reactor pressure to a low enough value for the GDCS to work.
- GDCS Injection (also Squib-Actuated Valves) - These valves allow the water stored in the gravity pools within the containment to drain into the depressurized RPV.
- GDCS Suppression Pool Equalizing (also Squib-Actuated Valves) - These equalizing valves allow the water stored in the suppression pool to drain into the depressurized RPV well after a postulated accident event to compensate for long-term reactor coolant boil-off.
- SLC (also Squib Actuated Valves) - These valves allow soluble boron (i.e., sodium pentaborate) to be injected into the RPV from two accumulator tanks to provide additional coolant inventory. (The sodium pentaborate also provides buffering to ensure the iodine chemical distribution assumed in the LOCA analysis remains valid.)
- ICS - The four isolation condensers are passive heat exchangers with Isolation Condenser/Passive Containment Cooling System (IC/PCCS) pool water on one side and reactor steam on the other. Each IC, once initiated by either of two valves that open a condensate return path to the reactor, condenses reactor steam and returns it to the RPV. The system operates at high RPV pressures and provides cooling and depressurization without reactor coolant inventory loss. The ICS also provides RPV pressure control and safe shutdown cooling functions.
- LD&IS - The SSLC/ESF processors perform the inboard and outboard isolation function for all isolation valves other than the MSIVs and selected steam line drain valves.
- CRHS - The SSLC/ESF processors perform the isolation of the Control Room Habitability Area (CRHA) inlet ventilation air and implement logic to isolate and filter the CRHA on detection of high radiation conditions.

Figure 6 RTIF-NMS, ICP, SSLC/ESF and DPS



The general arrangement of the ESBWR SSLC/ESF DCIS is also shown in Figure 6. There are four divisions of redundant logic; each division has a main chassis located in the MCR area dedicated safety-related DCIS rooms and remote chassis (in the reactor and control buildings). All remote chassis connections are through redundant fiber as are the connections to the MCR displays and (one way) connections to the N-DCIS. All chassis are redundantly powered by uninterruptible power and all four divisions can be powered by either diesel generator or offsite power through the isolation load centers.

Per parameter, two of four divisions of sensors must agree before each of three processors within a division provides a command signal to operate the final actuators. Per division, logic that requires the agreement of two-out-of-three processors is used to determine whether an ESF actuation condition is completed. The squib and solenoid actuators are designed such that any one of the four divisions can operate the actuator (after the two-out-of-four sensor agreement and two-out-of-three processor agreement logic); however the actuator cannot be operated by a single failure within the division.

### **2.3 NONSAFETY-RELATED DISTRIBUTED CONTROL AND INFORMATION SYSTEM OVERVIEW**

The N-DCIS contains the DPS and provides for control and monitoring of the PIP systems, the BOP (power generation) control systems, the PCF and the severe accident (Deluge Lines Flooder System) functions. The N-DCIS PCF also provides the main operator Human-Machine Interface (HMI). (The DPS is further discussed in the following subsection.)

The N-DCIS provides the functions necessary for normal operation of the plant from cold shutdown through full power. The N-DCIS controls nonsafety-related components and systems in the plant that are operated from the MCR or Remote Shutdown System (RSS) panels.

The PIP systems are those important for nonsafety-related reactor control and shutdown and their supporting systems; they include:

- Diesel Generators,
- 6.9 KV PIP Buses,
- Plant Service Water System (PSWS),
- Reactor Component Cooling Water System (RCCWS),
- Reactor Building (RB) Chillers,
- Instrument Air,
- Reactor Water Cleanup/Shutdown Cooling System (RWCU/SDC),
- Fuel and Auxiliary Pools Cooling System (FAPCS),
- CRD,
- PIP A and PIP B DCIS,
- Nonsafety-related Battery and Uninterruptible Power,
- PCCS Ventilation Fans

- Drywell Cooling, and
- RB, Fuel Building (FB), Control Building (CB), Switchgear Building Heating Ventilation and Air Conditioning (HVAC).

The PIP systems are organized mechanically into two trains (i.e., pump "A" and pump "B") with each train powered by a different diesel generator and 6.9 KV bus. The two trains are controlled by a deliberately segmented N-DCIS, so that the RMUs, control processors and displays that operate PIP A systems are separate from those operating PIP B systems. The segmentation is implemented using managed network switches; approximately one third of the nonsafety-related control room displays are assigned to the PIP A and the PIP B switches. Normally any control room nonsafety-related display can control/monitor any PIP or BOP system but the loss of either PIP system DCIS or the BOP DCIS will not affect the operation of the remaining PIP system or its displays.

The BOP control systems are those used principally for power generation and are not normally used for shutting down the plant, nor monitoring the more important plant parameters. They specifically include the triple redundant systems used to control the turbine, reactor pressure, RPV water level and plant automation and dual redundant systems, such as, the RC&IS, hotwell level control and condensate polishing systems.

The above systems provide margins to plant safety-related limits and improve the plant's transient performance. The systems also maintain the plant conditions within operating limits. The BOP functions can also be used to shut down the plant and are also part of the ESBWR defense-in-depth automatic and manual functions.

The PCF of N-DCIS redundantly provides for the plant AMS, some of the rod blocks for the Rod Control and Information System (RC&IS), the monitoring of thermal limits including core thermal power and flow calculation and calculation of calibration information for NMS and the isolated safety-related parameter display functions. The PCF of N-DCIS provides information to and receives demands from the nonsafety-related VDUs. The N-DCIS also provides for the acquisition and display of sensor outputs for nonsafety-related plant monitoring functions.

The N-DCIS supports the Severe Accident Deluge Lines Flooder System using diverse hardware and software and separate sensors from both the safety-related and nonsafety-related DCIS systems. The Deluge Lines Flooder System uses squib valves to drain GDCS pool water underneath the RPV should all other core cooling and shutdown systems fail. The valves are actuated by sensed containment floor high temperatures attributable to the postulated core and vessel melt.

## **2.4 DIVERSE PROTECTION SYSTEM OVERVIEW**

The DPS is a triple redundant, nonsafety-related system that provides an alternate means of initiating a reactor trip, actuating selected Engineered Safety Features and providing plant information to the operator. The relationship is shown in Figure 6. For functions credited with mitigating a digital protection system CCF, the DPS receives signals directly from a diverse set of sensors that are electrically independent from the sensors used by the Q-DCIS platforms. Specifically, the DPS uses hardware, software and power that are diverse from those used by the safety-related systems. The DPS is described further in Tier 2 Chapter 7 of Reference 6-3.

The DPS system performs several major/minor functions:

- It scrams the plant using a subset of the safety-related RPS parameters.
- It scrams the plant on a SCRRI/SRI command with power remaining elevated, or on receipt of an RPS scram demand from two of four RPS divisions.
- It closes the MSIVs on receipt of a high steam flow signal, low RPV water level, or low reactor pressure (i.e., low turbine inlet pressure).
- It initiates Selected Control Rod Run-in (SCRRI) and Select Rod Insert (SRI) to rapidly reduce power.
- It initiates selected ECCS.
- It transmits ATWS/SLC logic signals to cause the Feedwater Control System (FWCS) to run back feedwater flow.
- It initiates a delayed feedwater runback if elevated power levels persist following either a SCRRI/SRI command or an RPS scram command from two of four RPS divisions.
- It trips the feedwater pumps on RPV water level 9 (after they have been run back to zero flow on RPV water level 8 by the FWCS).
- It opens the ICS lower header vent valves after six hours of ICS initiation.

The DPS initiates a plant scram on a per parameter two-out-of-four coincidence of:

- Detected high or low RPV water level,
- Detected high RPV pressure,
- Detected high drywell pressure,
- Detection of high suppression pool temperature, and
- Inboard or outboard MSIV closure on two or more main steam lines.

The DPS causes a scram by interrupting the current in the 120 VAC return power from the HCU scram solenoids using the same switches used to perform individual control rod scram timing. The two-out-of-three scram decision of the triple redundant processors is sent to the scram timing test panel where they are two-out-of-three voted to open all the solenoid return power switches. The operator also has the ability to initiate a manual DPS scram from either hard switches or the N-DCIS VDUs.

The DPS processes a SCRRI/SRI signal to hydraulically scram selected control rods and to command the RC&IS to perform the SCRRI function based on any of the following initiators:

- Generator load rejection signal from the Turbine Generator Control System (TGCS),
- Turbine trip signal from the TGCS,
- Loss of feedwater heating, and
- Oscillation Power Range Monitor (OPRM) thermal neutron flux oscillation signal from the NMS (two-out-of-four logic).

The DPS also processes a SCRRI/SRI signal anytime the ATLM determines a loss of feedwater heating has occurred, or any time RC&IS indicates a SCRRI is being performed.

The DPS is also able to initiate the following diverse protective functions automatically:

- The isolation condensers on high RPV dome pressure, low RPV water level, or MSIV closure,
- The ADS (SRVs and DPVs) on low RPV water level,
- The GDCS injection squib valves on low RPV water level,
- The SLC System squib valves on low RPV water level,
- The opening of the IC/PCCS expansion pool to equipment storage pool cross-connect valves on low ICS/PCCS expansion pool level.

Only manual GDCS suppression pool equalizing function is provided in lieu of ECCS sequenced automatic actuation because the earliest the equalizing function is required is 30 minutes following a LOCA and only in the unlikely event that RPV level reaches level 0.5.

In lieu of delayed automatic initiation, DPS has the capability to initiate ADS and GDCS injection sequencing manually in response to high drywell pressure. The ADS initiation and GDCS sequence is not required for approximately 60 minutes during small and medium break LOCA scenarios that do not result in ECCS initiation from low RPV water level. This capability is automatically inhibited under ATWS conditions.

For automatic actuation, the two-out-of-four sensor logic and the two-out-of-three processing logic are similar to the scram logic and the operator also has the ability to initiate the above actions from the N-DCIS VDUs. The ECCS actuated components that use divisional solenoids to initiate flow (SRVs, ICs, and IC/PCCS to equipment storage pool cross-connect), also have a nonsafety-related solenoid to cause initiation from the DPS (after a two-out-of-three vote). The ECCS squib valves also use a DPS actuated squib initiator that is electrically isolated from the safety-related initiators on the same valve.

The DPS also provides the following major isolations:

- Closure of the MSIVs on detection of high steam flow, low reactor pressure or low RPV water level,
- Closure of the RWCU/SDC isolation valves on high differential flow using two-out-of-four sensor logic and 2/3 processing logic, and
- Closure of the feedwater isolation valves and trip of the ASD controller circuit breaker for the feedwater pumps on either of the following signals:
  - High drywell pressure coincident with high feedwater line differential pressure; or
  - High-high drywell pressure. This logic is automatically bypassed under ATWS conditions, and has manual inhibit capability; or
  - High drywell pressure coincident with high drywell water level.
- Isolation of HPCRD (i.e., high pressure makeup water injection to the RPV) on either of the following signals:

- High drywell pressure coincident with high drywell water level; or
- Low level in two out of three GDCS pools.

The DPS does not actuate the CRHS since no adverse consequences occur at the control room boundary if realistic assumptions are applied with the functioning of the diverse engineered safety features described above. Manual CRHS isolation is also available from the safety-related monitoring and indication segment of SSLC/ESF that is not assumed to fail coincident with a failure of the SSLC/ESF automatic actuation logic.

The DPS does not violate the general rule of avoiding communication between nonsafety-related systems and safety-related systems. The DPS has its own “actuators” (SRV and IC solenoids or 120 VAC HCU scram solenoid return switches). The DPS does not interface with the RPS or ESF logic or processors, except to initiate a diverse scram any time RPS transmits a scram signal to DPS via one-way fiber communication. For both RPS and ESF functions, the failure of the DPS cannot prevent the Q-DCIS from performing its safety-related functions and the communication path from Q-DCIS to N-DCIS is always by fiber.

The DPS controls can be accessed from VDUs not on the PIP A, PIP B or BOP N-DCIS segments (meaning that the DPS displays and soft controls can operate even if other segments fail) to provide the operator with manual control of the actuators within DPS scope. The same VDUs allow the operator to monitor those signals used for DPS automatic operation (and, normally, every other N-DCIS – including isolated Q-DCIS – signal); this provides the operator with the information needed to operate the DPS manually. The N-DCIS VDUs rely on a technology diverse from that of the Q-DCIS VDUs.

The DPS is implemented as a triple redundant control system and is expected to be reliable, because it is a backup system. Because of the undesirability of inadvertent actuation of the various ADS valves, its logic is a “fail as is” design. Failure of its self-diagnostics prevents it from actuating any connected ADS valves. The DPS controller is located in a different fire area from the Q-DCIS and other N-DCIS controllers so it can be expected to operate even if PIP A, PIP B or the Q-DCIS controllers are inoperable. Additionally the DPS RMU cabinets in the RB are in two pairs of two cabinets each with each pair in a separate fire zone. The DPS input signals are divided evenly between each pair of cabinets. To further prevent inadvertent actuation of the ADS valves, the solenoids/squibs connected to DPS each require a series connected set of two or three switches to close before the final device is energized; each of the series connected switches is individually two-out-of-three voted and located in a different cabinet to eliminate the possibility of hot short circuits.

The interfacing systems (i.e. NBS, Condensate and Feedwater System sensors, CMS (including SPTM), FAPCS sensors, TGCS, GDCS, SLC, ICS, RWCU/SDC, RC&IS, CRD, and FWCS) provide nonsafety-related sense and actuate features required to perform the diverse functions. The portions of these systems used to support the diverse functions are developed using a quality assurance program that meets or exceeds the guidance contained in NRC Generic Letter 85-06, “Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related.”

## **2.5 PCF (PLANT COMPUTER FUNCTIONS) OVERVIEW**

The PCF which are a subsystem of the N-DCIS provide the equipment used for processing data that result in nonsafety-related alarms and displays for both normal and emergency plant operations, generating these displays and alarms, providing analysis of plant data, providing plant data logs and historical storage and retrieval, and providing operational support for plant personnel. The AMS conditions (i.e., filters) alarms based on both plant operating modes and events to prevent the operator from being presented with unnecessary alarms and information during transient and accident scenarios. Additionally, alarm response procedures and operating/emergency procedures are available on line. Although a traditional set of SPDS displays is available on the nonsafety-related VDUs, the important SPDS parameters are also permanently available on the mimic on the WDP.

The N-DCIS also contains the real-time data network, which is a redundant data network that links the elements of the ESBWR I&C architecture.

## **2.6 CONFORMANCE TO THE NUREG/CR-6303 ECHELON OF DEFENSE STRUCTURE AND TO THE NUREG/CR-6303 BLOCK STRUCTURE**

The I&C conforms to the echelon of defense structure defined in Section 2.2 and the block structure described in Section 2.5 of Reference 6-1. The four echelons are divided into three levels containing the nonsafety-related systems, safety-related systems, and nonsafety-related diverse systems that provide automatically and manually actuated functions to support them.

The functions assigned to the I&C systems are implemented by processor-based subsystems, which are placed within a structure of separate cabinets and DCIS rooms. Table 1 maps the echelons of defense to the I&C architecture. The echelons are divided into a nonsafety-related layer, a safety-related layer, and a nonsafety-related diverse layer to reflect the means provided by the systems to implement the echelon functions. Table 2 illustrates the relationships between these subsystems and cabinets and the block structure described in Reference 6-1 and shows the assignment of equipment to the blocks for each level within the echelons of defense.

Because of the processor implementation, the demarcation between measured variable blocks and derived variable blocks lies within the software structure of a channel or function. These blocks are combined into a single column for purposes of defining hardware assignments.

Indications to support manual actions to maintain the plant within operating limits, trip the reactor, and actuate ESF functions are provided within the three layers of the I&C architecture. The N-DCIS provides nonsafety-related operator displays and alarms. Plant data for the nonsafety-related displays and alarms is obtained from across the I&C architecture by means of the real-time data network. The Q-DCIS provides safety-related operator displays. In addition, for functions credited with mitigating a digital protection CCF, the DPS provides nonsafety-related operator indications that are derived from a diverse set of sensors that are electrically independent from those of the Q-DCIS sensors.

The N-DCIS provides for normal plant control and power generation. The redundancy in these systems normally prevents them from causing transients because of their own failure and they are normally responsive enough to prevent externally caused transients from initiating safety-related functions. All of the above systems have both manual and automatic initiation modes.

**Table 1 ESBWR Instrumentation and Control Echelons of Defense**

	<b>LAYER 1</b> NONSAFETY-RELATED SYSTEMS	<b>LAYER 2</b> SAFETY-RELATED SYSTEMS	<b>LAYER 3</b> DIVERSE NONSAFETY-RELATED SYSTEMS
<b>CONTROL</b> ECHELON	N-DCIS (PIP A, PIP B, BOP)		
<b>REACTOR TRIP</b> ECHELON		Q-DCIS RTIF-NMS (RPS, NMS) and ICP (ATWS/SLC)	Diverse Protection System (DPS - some RPS)
<b>ESF ACTUATION</b> ECHELON		Q-DCIS SSLC/ESF (ECCS - ICS, ADS, GDCS, SLC, Misc. Isolation), RTIF-NMS (LD&IS-MSIV), and ICP (ATWS/SLC)	Diverse Protection System (DPS - ICS, ADS, GDCS, SLC, some LD&IS)
<b>MONITORING AND INDICATION</b> ECHELON	N-DCIS Plant Computer Functions	Q-DCIS SSLC/ESF	DPS

For monitoring/indication applications, DPS is able to indicate the appropriate critical safety-related (through isolated gateways) and nonsafety-related parameters needed to operate DPS manually; this information is on segmented DPS displays that work even if PIP or BOP displays do not.

In addition to the four echelons described above, the Deluge Lines Flooder System and the Basemat-Internal Melt Arrest Coolability (BiMAC) device are included in the ESBWR design to reduce the consequences of severe accidents. They provide an engineered method to assure heat transfer between a core debris bed and cooling water in the lower drywell and provide for scrubbing of fission products released from the debris during severe accident scenarios.

**Table 2 Assignment of I&C Equipment to Defense-in-Depth Echelons**

<b>Echelon</b>	<b>ESBWR Function</b>	<b>Measured and Derived Variable Blocks</b>	<b>Command Block</b>	<b>Manual Actions</b>
Plant Control	Nonsafety-related	Sensors, Signal Conditioning, Network, Isolated NMS Inputs	Network, Output Signal Conditioning, Analog/Discrete Output	Network, VDU, Soft Control, Some Hard Control
	Safety-related	Level 8 feedwater isolation and Level 9 pump trip	2/4 voting logic, Load Drivers, ASD control power circuit breakers.	N/A
	Diverse	Level 9 trip	Level 9 trip	N/A
Reactor Trip				
	Safety-related	Sensors, Signal Conditioning, RTIF-NMS, ATWS/SLC (diverse)	2/4 voting logic, Load Drivers, HCU Scram Solenoids, SLC squib valves,	Hardwired Manual Reactor Trip, HCU Scram Solenoids ATWS/SLC - Manual
	Diverse (Nonsafety-related)	Sensors, Signal Conditioning, Diverse Processor Platform	2/4 and 2/3 Voting Logic, Load Drivers, HCU Scram Solenoids (120 VAC return), Backup Scram Valve Solenoids, FMCRD Run-In, Feedwater Runback, ARI	Hardwired DPS Reactor Scram Switches, Soft DPS VDU Controls
ESF Actuation				
	Safety-related	Sensors, Signal Conditioning, SSLC/ESF (all Diverse from Reactor Trip Functions)	2/3 Logic per Division, 2/4 Divisional Voting Logic, Load Drivers, Solenoids, Squib Valves	Manual Switches through SSLC/ESF Logic, some Hardwired Switches
	Diverse (Nonsafety-related)	Sensors, Signal Conditioning, Diverse Processor Platform	2/4 and 2/3 Voting Logic, Load Drivers, IC, SRV and Isolation Valve Solenoids, Squib Valves for ADS, GDSC and SLC System, and Misc. Isolations	Soft DPS VDU Controls
Monitoring and Indication	Nonsafety-Related	Sensors, Signal Conditioning, Network	Network, Mimic, AMS, VDU	VDUs, some Hardwired Indications
	Safety-related	Sensors, Signal Conditioning, SSLC/ESF	VDU	Safety-related VDUs, some Hardwired Indications
	Diverse	Sensors, Signal Conditioning, Diverse Processor Platform	Network, VDU	VDU

### **3. DEFENSE-IN-DEPTH FEATURES OF THE ESBWR INSTRUMENTATION AND CONTROL ARCHITECTURE**

#### **3.1 INTRODUCTION**

This section describes features of the I&C architecture that provide redundant design, fail-safe design, and self-diagnostics/failure detection and repair. Section 5 discusses design diversity.

#### **3.2 DEFINITION OF COMMON-MODE FAILURES**

For the purpose of this report, Common-Mode Failures (CMFs) are considered to be sets of causally related failures that occur within a limited time, and fall outside of system design capabilities for detection or mitigation of those failures; the limited time is because simultaneous failures of diverse platforms are considered less credible than simultaneous failures of isolated, redundant systems. The failures that meet this definition exhibit the following characteristics:

- The failures occur in a sufficient number of places in the I&C architecture that redundant design is ineffective in enabling the system to tolerate them.
- The failures are such that fail-safe design is ineffective in enabling the system to tolerate them.
- The failures are undetectable, or they occur within a sufficiently short time that neither automatic nor manual responses are possible to enable the system to tolerate them.
- The failures occur simultaneously in only related hardware/software platforms.

An I&C system, or a portion of a system, can be capable of tolerating some combinations of CMFs because:

- Diverse design exists (for example RPS and ATWS/SLC).
- Redundant design exists (most nonsafety-related control logic, most safety-related logic divisions).
- Fail-safe design exists (for example RPS and MSIV isolation).
- The failure is detectable and sufficient time exists between instances of failure that there is an automatic or manual response to the failure (most safety-related and nonsafety-related DCIS).

In this evaluation, CMFs are postulated to cause complete failure of similar or identical equipment (hardware/software platforms). This failure mode is assumed to cause complete loss of function of either the RPS or SSLC/ESF logic but not loss of function of the DPS. A simultaneous digital protection system CMF of both the RPS and SSLC/ESF logic is not assumed due to the diversity between the platforms.

#### **3.3 OVERALL INSTRUMENTATION AND CONTROL FAULT TOLERANT DESIGN FEATURES**

The I&C architecture contains design features which enhance plant reliability and availability. However, these features also provide a degree of protection against CMFs/CCFs, and, as a result, decrease the probability that a CMF/CCF causes any portion of the ESBWR I&C architecture to

be unable to respond to a transient, accident or plant fault. Among the design features that protect against failures, including CMFs and CCFs, are:

The Design, Verification, and Validation Process - The design of the I&C system hardware and software components is controlled by a design, verification, and validation process that is described in Reference 6-3 and Reference 6-4. These processes are formal, rigorous methods to detect and correct design errors before they can result in plant CMFS/CCFs.

Automated software tools aid in verification and validation. Commercial development tools and languages with a known history of successful applications in similar designs are used for software development.

- Fail Safe/Fault Tolerant Design – In addition to the use of high quality components and deference to microprocessors with simple operating systems, fail safe design features are employed in the I&C architecture. RPS features such as de-energizing to trip or actuate or, most important in distributed systems, tripping or actuating on loss of communications, provide the capability to automatically or manually restore the plant to a safe condition following a failure. Some multiple failures can also be accommodated; for example, two divisions of RPS can be lost without losing the ability to scram. In the case of SSLC/ESF, de-energization or loss of communication results in no actuation as the desired state, since loss of two SSLC/ESF divisions can be tolerated without losing the ability to actuate ESF systems. Fault-tolerant design features such as functional diversity and redundancy also provide the capability to automatically or manually restore the plant to a safe condition.

Software design uses recognized defensive programming techniques, backed up by self-diagnostic software and hardware watchdog timers.

Fixed message formats are used for plant sensor data, equipment activation data, and diagnostic data. Corrupted messages are readily detected by error detecting software in each digital instrument.

- Redundancy – Redundant design alone does not prevent CMFs, but the use of redundant subsystems can enable the plant to detect and respond to failures, including CMFs when sufficient time exists between occurrences of the individual failures. For example the four divisions of SSLC/ESF are neither time synchronized nor dependent on other divisions for correct operation, which indicates that non-simultaneous (non time-related) CMFs/CCFs can be detected by surveillance testing.
- Modular Design - Modular design enhances the rapid isolation and repair of failures. When failures, including CMFs, occur, but sufficient time between them exists for detection and repair, modular design enables the redundant or diverse subsystems to be made available in response. The redundant components of the N-DCIS can be changed on line without affecting plant control, and divisional systems can be made inoperable and their chassis replaced on line without affecting plant operation. The total amount of hardware is minimized.

Software for control programs is permanently embedded as firmware in controller Read Only Memory (ROM). The man-machine interface (MMI) is implemented so that the equipment is structured into small units with sufficient diagnostics that a user can repair

equipment by replacing modules and can operate equipment by following straightforward instructions.

The software design process specifies modular code. Code is segmented by system and function. Software modules have one entry and one exit point and are written using a limited number of program constructs.

- Use of Distributed Processing Architecture - I&C functions are divided among multiple subsystems so that diverse functions are separated into different subsystems. Program code for each safety-related system resides in independent modules that perform setpoint comparison, voting, and control logic. This, in conjunction with other design features such as divisional isolation and independence, has the effect of localizing certain CMFs to a single subsystem. When functional diversity exists in the I&C architecture, complete system failure may not occur as a result of CMF. For example, RPV water level and reactor pressure control are implemented in different cabinets with each cabinet using triple redundant processors. It is very unlikely that both functions would be lost simultaneously. The reactor pressure control function is implemented on the Q-DCIS by the SRVs and the isolation condensers (SSLC/ESF) and on the N-DCIS by the triple redundant Steam Bypass and Pressure Control (SB&PC) System; given the diversity of these systems it is highly unlikely that both reactor pressure control functions could be completely or simultaneously lost.
- Alarm Management System - The ESBWR AMS is capable of alerting the operator, via audible annunciation or visual display, to not only process failures, but also DCIS failures including multiple failures, in other parts of the I&C system. The main ESBWR AMS is part of the PCF of N-DCIS, which uses hardware and software diverse from the Q-DCIS.
- Continuous Self-Diagnostics - In the ESBWR I&C architecture, the subsystems continuously execute self-diagnostic software routines. Other self-diagnostic features, such as read-backs and watchdog timers continuously monitor the operation of critical subsystems. These self-diagnostic features are designed to detect and report hardware failures, enabling the operator to respond appropriately. For example, the Q-DCIS and most of the N-DCIS use redundant power supplies; a detected power supply failure allows diagnosis and replacement before the second power supply fails. An additional example is the adjustable speed drives in the feedwater system that continuously report back the received speed demand to the FWCS. When the FWCS senses a difference between transmitted and received demand, the adjustable speed drive is "locked up" (held at constant speed) until another drive can be brought on line.

Code for calibration, signal input/output, online diagnostics, and graphical displays are common to all systems.

- Test Subsystem - The test subsystem rapidly and consistently verifies system operation. The use of the test subsystem enhances the timely detection of all failures, including CMFs. The test subsystem also enhances the ability of plant personnel to quickly diagnose and repair detected failures.
- Circuit Isolation - Circuit isolation is used to electrically isolate segments of the I&C architecture and to prevent propagation of electrical faults caused by failures, including CMFs. For example all interdivisional communication (for two-out-of-four trip

decisions) is via isolated fiber, similarly all safety-related to nonsafety-related communication is also via fiber; the fiber communication is monitored to implement both fail-safe and self- diagnostic schemes. Both the safety-related and nonsafety-related DCIS communicate with their remote multiplexing (data acquisition) units using redundant fibers to prevent circulating ground currents that could adversely (and commonly) affect all DCIS in an area.

- Control of Setpoint and Tuning Adjustments – The I&C architecture has physical and administrative controls and multiple levels of security for access to setpoint and tuning adjustments. This helps to prevent CMF due to incorrect constants entered as a result of a maintenance error. For example access to nonsafety-related setpoints requires a higher level of security than simply operating the system. A safety-related example is the requirement to make NMS, RPS, or SSLC/ESF divisions inoperable before setpoints can be changed; the rendering of a division inoperable generates a plant alarm as required by RG 1.47 (Reference 6-11).
- Use of Engineering Units for Setpoints and Tuning Constants - Setpoints and tuning constants in the I&C architecture are entered in engineering units rather than as scaled values. This prevents a potential common-mode error by eliminating scaling calculations.
- Signal Selection Algorithms in the DCIS - All of the signals used for nonsafety-related plant control and power generation (for example hotwell level, feedwater heater level and reactor pressure) are used only after a validation process that combines the signals from multiple sensors. No single sensor (or its power supply) failure causes a transient or loss of power generation; the failures are alarmed to allow timely repair. On the safety-related side, all four divisions use sensor trip data from all of the other divisions; unless one of the divisions is bypassed, the loss of any two divisions of like sensors causes an RPS trip. The loss of any single divisional sensor does not prevent two-out-of-four trip logic from occurring in any division – even the division with the failed sensor. Sensor data from the four divisions are continuously (not just for surveillance tests) compared and discrepancies are alarmed to the operator. The alarm warns the operator to repair the failed sensor in a timely manner.
- Physical Separation - Physical separation is provided between the four redundant Q-DCIS divisions of equipment. Likewise, the four divisions are separated from nonsafety-related systems and the DPS. There are four safety-related DCIS equipment rooms in the CB that provide physical, fire and electrical separation of the four divisions. Physical separation meets the requirements of IEEE-384 (Reference 6-6). The PIP A and PIP B N-DCIS systems are located in two physically separate N-DCIS rooms to provide the same physical, fire and electrical separation. The DPS controller is physically separated from PIP A, PIP B, and Q-DCIS. This physical separation provides protection from CMF induced by physical phenomena.
- Equipment Qualification - Equipment in the I&C architecture is qualified to environmental requirements, including temperature, humidity, radiation, vibration/seismic, electro-magnetic interference/radio frequency interference (EMI/RFI), Electrostatic Discharge (ESD) and surge withstand criteria commensurate with its safety-related classification and intended usage; specifically the safety-related DCIS

components are qualified with the understanding that the passive nature of the ESBWR does not take credit for any active heat removal for 72 hours. The environmental qualification program provides assurance that physical phenomena do not introduce CMF unless design requirements are exceeded. The equipment qualification program is described in Tier 2 Chapter 3 of Reference 6-3.

- Power - The Q-DCIS components are always powered with two power supplies and two separate power feeds appropriate to the division. The component power supplies act as an “isolator” such that most power source problems are not propagated into the component and the redundancy allows the component to both continue operation and generate alarms should one power supply or power feed be lost. The N-DCIS components are also powered with two or three inverter (uninterruptible) power sources and are provided with the same protection. The inverter or regulating transformers prevent a single divisional or non-divisional power problem from causing the loss of safety-related functions or nonsafety-related control or power generation.
- Other Features - The I&C architecture also contains other design features such as ac power line protection and filtering, EMI/RFI design, and surge withstand networks at signal conditioning board inputs, which prevent failures from specific causes. These features assure that the causes of multiple failures must exceed design and qualification test limits.

#### 4. EVALUATION OF NUREG/CR-6303 GUIDELINES

Reference 6-1 describes a method for analyzing computer-based RPS vulnerability to postulated software CMFs and provides fourteen guidelines for performing a diversity and defense-in-depth analysis. The following sections describe the results of applying these guidelines.

Section	Title	Guideline
4.1	Identifying system blocks	1, 5
4.2	Determining diversity	2
4.3	System failure types	3
4.4	Echelons of defense	4
4.5	Postulated common-mode failure of blocks	6
4.6	Use of identical hardware and software modules	7
4.7	Effect of other blocks	8
4.8	Output signals	9
4.9	Diversity for anticipated operational occurrences and accidents	10, 11
4.10	Diversity among echelons of defense	12
4.11	Plant monitoring	13
4.12	Manual operator action	14

##### 4.1 IDENTIFYING SYSTEM BLOCKS - GUIDELINES 1 AND 5

The safety-related instrumentation that provides the protective functions is divided into four redundant divisions. Table 2 shows how the cabinets and subsystems within each division can be mapped into blocks.

The N-DCIS uses redundant sensors and redundant subsystems to provide defense-in-depth functions and diverse actuation functions.

In this evaluation, however, CMFs are postulated to cause complete failure of similar or identical equipment. This failure mode is assumed to cause the loss of one platform within the Q-DCIS, but not simultaneous loss of all of Q-DCIS or DPS functionality due to the diversity of the logic platforms.

##### 4.2 DETERMINING DIVERSITY- GUIDELINE 2

Reference 6-1 identifies six aspects of diversity to address the issue of potential common mode effects and CMFs:

(1) Design Diversity

In the nonsafety-related DPS, energize to trip or actuate logic is used. In the Q-DCIS, de-energize to trip or actuate logic is used for the RPS and NMS and energize to trip logic is used for the SSLC/ESF and ICP. RTIF-NMS, SSLC/ESF, ICP and DPS platform each employ diverse hardware/software designs.

(2) Equipment Diversity

For the DPS, the hardware and software used to provide the automatic actions and sensor monitoring is diverse from the equipment used for safety-related functions in the Q-DCIS. For example, a DPS scram is processed using triple redundant logic that actuates discrete output switches that are diverse from the RPS reactor scram load drivers. The DPS and RPS monitor diverse sets of sensors and provide a reactor scram by operating their respective switches in the HCU scram solenoid 120 VAC circuit supply (in the case of RPS) or return leg (in the case of DPS).

(3) Functional Diversity

The ESBWR design uses multiple levels of defense for each anticipated operational occurrence and accident described in Reference 6-3. Control rods can be inserted hydraulically or electrically to cause a reactor shutdown with additional diverse shutdown capability provided by sodium pentaborate injection. Core cooling can be provided either by forced flow or hydraulic head (pools and gravity convection). The Q-DCIS is a safety-related system with four-way divisional separation. Two-out-of-four voting is used for the reactor trip function and SSLC/ESF actuation functions. Multiple reactor trip functions and SSLC/ESF actuations are provided for each anticipated operational occurrence and accident, generally using diverse signals, as described in Tier 2 Chapters 5, 6 and 7 of Reference 6-3. The DPS uses triple redundant processors and two-out-of-four parameter voting logic to determine a trip condition; signals to two of three processors must agree to actuate a trip. The functional logic for the automatic Q-DCIS functions is shown in Tier 2 Chapter 7 of Reference 6-3.

(4) Human Diversity

Human diversity is implemented by the diversity of the organization(s) on the project, project plans, and procedures to meet the expectations of Reference 6-1, but there are times when a more experienced, but possibly less diverse individual, is utilized to maintain quality.

(5) Signal Diversity

Signal diversity for specific events is provided within the safety-related reactor trip and ESF actuation echelons. For example, RPV level and drywell pressure are used as inputs to support the containment isolation ESF function. The signals used to produce digital protection system software CCF mitigating reactor trips and ESF actuations within the DPS originate from a diverse set of sensors that are electrically independent from the sensors used by the Q-DCIS platforms.

(6) Software Diversity

The DPS contains triple redundant signal processing units that use hardware and software that is diverse from the hardware and software used in the Q-DCIS.

### **4.3 SYSTEM FAILURE TYPES - GUIDELINE 3**

Reference 6-1 describes three different instrumentation failure types that are applicable to the ESBWR.

#### **4.3.1 Type 1 Failure**

Type 1 failures are those postulated in one echelon that result in a plant transient that requires a protection function to mitigate it. Generally, the postulated failure is assumed to occur in the control system echelon such that a plant transient occurs that results in an automatic reactor trip or ESF actuation. However, there may be postulated failures in the protection systems that necessitate protective action.

Type 1 failures will be analyzed during detailed system design.

The primary defense against Type 1 failures is to ensure that a protection function exists to mitigate each postulated credible failure that can occur in a plant control or protection system and result in a plant transient requiring protective action. A substantial defense against these failures is provided by requiring that the control system echelon be single-failure proof and self-diagnosing such that only (postulated) common cause failures (CCF) are "credible".

#### **4.3.2 Type 2 Failure**

Type 2 failures are undetected failures and are manifested only when a demand is received to actuate a component or system. Failure to respond is due to a postulated CMF of redundant divisions or trains.

The primary defense against a Type 2 failure is to provide diversity within and between the four echelons of defense. The goal is to design a system in which all functions associated with an echelon of defense and the four echelons of defense are not susceptible to a postulated CMF. A substantial defense against these failures is provided by requiring that the ESBWR Q-DCIS echelon be redundantly powered and self-diagnosing and include features such as monitoring for the existence and continuity of the final actuators (squib, scram solenoids) so that only (postulated) CMF are "credible".

#### **4.3.3 Type 3 Failure**

Type 3 failures occur because either the plant process does not respond in a predictable manner or the sensors measuring plant process parameters respond in an anomalous manner.

The primary defense against a Type 3 failure is to provide diverse signals for measuring the plant response to an initiating event, e.g., using drywell pressure and RPV water level for a Loss of Coolant Accident (LOCA) indication or reactor pressure and core inlet temperature for measuring moderator temperature. A substantial defense against these failures is provided by requiring (for example) that the ESBWR Q-DCIS and N-DCIS level measurement systems incorporate both reference and variable leg temperature measurements so that indicated level is correct until reference leg boiling occurs and is alarmed. (Reference leg boiling may occur as a result of elevated containment temperature and reactor depressurization during postulated LOCA events.) Similarly SRV and squib valve positions are measured rather than assuming that an "open" command has resulted in the correct valve behavior.

#### **4.4 ECHELONS OF DEFENSE - GUIDELINE 4**

The I&C architecture is divided into four echelons of defense. The control echelon is provided by the N-DCIS, with NMS inputs provided from the Q-DCIS by means of isolated data links.

The DPS and the Q-DCIS provide the reactor trip echelon. The plant protection subsystems, the voting logic, dedicated data links, load drivers and HCU scram solenoids provide the reactor trip function in the Q-DCIS. The backup scram valve solenoids in the HCU scram solenoid air header and safety-related ATWS/SLC System logic provide an additional means of reactor trip. The nonsafety-related DPS actuation of switches in the return side of the HCU scram solenoid circuit, ARI and motor driven FMCRD run in provide a diverse reactor trip function. In addition, the N-DCIS redundant control systems enable the plant to avoid the need to trip (including a 100% load rejection) by maintaining it within acceptable limits.

The Q-DCIS and DPS provide the SSLC/ESF echelon. The SSLC/ESF subsystems comprising the ECCS, the SSLC/ESF coincidence logic, the SSLC/ESF actuation subsystems, dedicated data links, and data highways provide the majority of ESF function in the Q-DCIS. RTIF-NMS (LD&IS - MSIV isolation) and ICP (VBIF) provide other isolation functions. The DPS provides a diverse means to actuate some ESF functions. In addition, the Q-DCIS and N-DCIS actuate defense-in-depth plant systems to avoid the need for actuating the passive safety-related systems.

The Q-DCIS and N-DCIS also provide features of the Monitoring and Indicator echelon. Both the Q-DCIS (via SSLC/ESF) and N-DCIS provide monitoring and indication via VDUs to support operation of the respective systems, system status assessment, as well as monitoring and indication of critical safety functions. The N-DCIS via isolated gateways has the capability to monitor all of the available Q-DCIS parameters.

#### **4.5 POSTULATED COMMON-MODE FAILURE OF BLOCKS – GUIDELINE 6**

The postulated CMF of processor-based subsystems 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 mode is assumed to cause the complete loss of function of the Q-DCIS, but not the coincident loss of any DPS functions due to the diversity of the implementation. The result of this failure is that the entire system or systems fail to perform any protective actions. The evaluation of the I&C architecture response to this failure is contained in Section 5.

#### **4.6 USE OF IDENTICAL HARDWARE AND SOFTWARE MODULES – GUIDELINE 7**

The PRA considers CMFs within the I&C architecture, in conjunction with random failures. Although final results will not be available until the hardware/software is chosen, preliminary PRA results have evaluated the contribution to core damage due to I&C CMF to be acceptably low. It is conservatively assumed in the PRA that all software modules or hardware modules of a type fail simultaneously. The diversity between the Q-DCIS and DPS assures that the joint CMF probability is acceptably low.

#### **4.7 EFFECT OF OTHER BLOCKS - GUIDELINE 8**

In the ESBWR I&C architecture, input signals are not shared between DPS and any of the safety-related systems. For CMF within the Q-DCIS, the system is conservatively assumed to not initiate any of the protective actions needed to mitigate an event.

#### **4.8 OUTPUT SIGNALS - GUIDELINE 9**

Optical isolation is provided between subsystems to prevent propagation of an electrical failure in either direction. The majority of the individual data links are one-way without the receiving component being dependent on receipt of the data for correct operation. The four divisions of the Q-DCIS are physically separated for power, fire protection and (normal) HVAC (it is assumed that there is no active HVAC for accidents). Sensors are considered to be contained in a measured variable block for the purposes of the analyses in this report, so failure of signal conditioning equipment influencing sensor performance is not considered. (The I&C hardware contains features to minimize the occurrence of this failure mode, such as auto-calibration, A/D conversion and application software checksum diagnostics and parameter validation.)

#### **4.9 DIVERSITY FOR ANTICIPATED OPERATIONAL OCCURRENCES AND ACCIDENTS - GUIDELINES 10 AND 11**

The frequency of a postulated accident occurrence in conjunction with CMFs of the Q-DCIS and failures of the DPS is discussed in the PRA that also discusses Q-DCIS and DPS modeling. Section 5 provides a strategic evaluation of the ability of the I&C architecture to produce the following required protective actions to support the safety-related goals:

- Initiate Reactor shutdown,
- Initiate RCS inventory control,
- Initiate core decay heat removal,
- Initiate containment cooling, and
- Initiate containment isolation.

Note that the primary reactor coolant system can be depressurized in a controlled automatic or manual sequence to mitigate certain events.

#### **4.10 DIVERSITY AMONG ECHELONS OF DEFENSE - GUIDELINE 12**

##### **4.10.1 Control/Reactor Trip**

For the low probability simultaneous occurrence of an event that requires a reactor trip and a postulated CMF in the RPS function of Q-DCIS, the DPS initiates a reactor trip by a diverse method. The specific functions performed by the DPS are based on PRA methods but specific capabilities are discussed in Section 5. The DPS functional requirements are based on an assessment of the existing RPS capabilities, accident severity and I&C CMF probabilities combined with the event probability.

Additionally, both the Q-DCIS and DPS provide a manual means of tripping the reactor. To support manual reactor trip, both the Q-DCIS and the DPS provide plant information to the

operator. The Q-DCIS provides the safety-related measurements of the parameters that scram the reactor while the DPS provides similar nonsafety-related diverse indications.

#### **4.10.2 Control/Engineered Safety-Related Features (SSLC/ESF)**

For the low probability occurrence of an event that requires one or more ESF actuations and is coincident with a postulated CMF in the SSLC/ESF function of Q-DCIS, the DPS initiates selected ESF actuations in a diverse fashion. The specific functions performed by the DPS are based on PRA methods (and a qualitative deterministic analysis of DCD Tier 2 Chapter 15 events) but specific capabilities are discussed in Section 5 (and Appendix A). The DPS functional requirements are based on a qualitative assessment of the existing ESF capabilities, accident severity and I&C CMF probabilities combined with the event probability and reasonable operator actions.

Additionally, the Q-DCIS provides both system level and component level manual means of actuating ESF functions, and DPS provides a manual means of actuating selected ESF functions. To support manual ESF actuation, both the Q-DCIS and the DPS provide plant information to the operator. The Q-DCIS provides the safety-related measurements of parameters that initiate ESF and monitor its progress, and the DPS provides nonsafety-related diverse indications.

#### **4.10.3 Reactor Trip/ESFAS**

Generally isolated, independent interconnections exist between the RTIF-NMS and SSLC/ESF for safety-related display purposes. Since the RTIF-NMS and ESF functions (except for the LD&IS - MSIV isolation function) use separate sensors and diverse hardware/software, failure of the reactor trip function does not prevent the ESF actuation function from responding to other inputs. RPS and LD&IS-MSIV isolation function are part of the fail-safe RTIF-NMS platform. Failure of the ESF actuation function does not prevent the reactor trip function from responding to other inputs.

### **4.11 PLANT MONITORING - GUIDELINE 13**

Indications to support manual actions to maintain the plant within operating limits, trip the reactor, and actuate ESF functions are provided within the three layers of the I&C architecture. The N-DCIS provides nonsafety-related operator displays and alarms. Plant data for the nonsafety-related displays and alarms are obtained from the I&C architecture by means of the real-time data network. The SSLC/ESF within the Q-DCIS provides safety-related operator displays (safety-related information is also available on nonsafety-related displays through isolated gateways). In addition, the DPS provides nonsafety-related, diverse operator indications. Diverse and independent signal conditioning and data acquisition functions are performed in the RTIF-NMS, SSLC/ESF, ICP and DPS such that a postulated software CMF in one platform does not degrade the signal conditioning and data acquisition functions in the other platform.

Signals are transmitted from the Q-DCIS to the N-DCIS via one way isolated fiber connections that prevent failures in the N-DCIS from affecting operation of the Q-DCIS. Once signals leave the Q-DCIS through the isolation devices, they are no longer considered safety-related, and are not used to provide any safety-related functions.

The signals from Q-DCIS to N-DCIS are routed and isolated to meet the independence requirements of GDC-24 (Reference 6-12), IEEE-603 (Reference 6-9), IEEE-379 (Reference 6-10), and Reference 6-6.

No credible failure of the N-DCIS prevents the safety-related system from performing its safety-related function. Although Q-DCIS function monitoring is done within the self-diagnostic and self-test functions of the safety-related systems, the fiber optic gateways provide the connections used for additional plant monitoring and surveillance of the reactor trip and ESF actuation subsystems. The N-DCIS provides the software and hardware used for displaying plant parameters and monitoring system performance, for example by allowing all divisional data to be placed on a single screen – something not possible within the divisionally isolated safety-related systems. The nonsafety-related AMS is also used to direct attention to faults in the safety-related systems of which the operator may not be aware.

The automatic functions of the Q-DCIS are designed to protect the plant from potential operator induced transients which may result from failures in the N-DCIS, however unlikely, considering the redundancy of the nonsafety-related systems.

#### **4.12 MANUAL OPERATOR ACTION – GUIDELINE 14**

The manual reactor trip and ESF actuation functions performed by the monitoring and indication echelon of defense is included in the Q-DCIS. The nonsafety-related DPS also provides manual reactor trip and selected ESF actuation capabilities.

Both the Q-DCIS and DPS provide manual means of tripping the reactor. The Q-DCIS also provides a hardwired reactor trip to the HCU scram solenoids. The DPS provides a diverse manual reactor trip to switches on the 120 VAC return side of the HCU scram solenoids.

The Q-DCIS provides both system-level and component-level manual means of actuating ESF functions; the DPS provides a manual means of actuating selected ESF functions. Given the timing and low likelihood of occurrence, DPS provides manual GDCS suppression pool equalization capability in lieu of automatic actuation. Additionally, in lieu of delayed automatic logic, manual ADS initiation and GDCS injection sequencing in response to a high drywell pressure condition is provided to mitigate small and medium-break LOCA conditions that do not result in a low RPV water level - ECCS initiation signal.

## **5. EVALUATION OF DIVERSITY WITHIN THE ESBWR INSTRUMENTATION AND CONTROL ARCHITECTURE**

### **5.1 INTRODUCTION**

The plant fluid systems are designed with multiple levels of defense for a wide range of events. The designs of both the safety-related and the nonsafety-related systems support this multiple level design philosophy. The ESBWR I&C systems architecture reflects this multiple level of defense approach by including safety-related and nonsafety-related systems that provide safety-related and nonsafety-related means of initiating protective functions that both shut down the reactor and provide for core cooling.

This section discusses the functions provided to protect the core and limit the spread of radioactivity during an event by initiating:

- Reactor Shutdown,
- RCS Inventory Control,
- Core Decay Heat Removal,
- Containment Cooling, and
- Containment Isolation.

### **5.2 DIVERSITY OVERVIEW OF THE ESBWR INSTRUMENTATION AND CONTROL ARCHITECTURE**

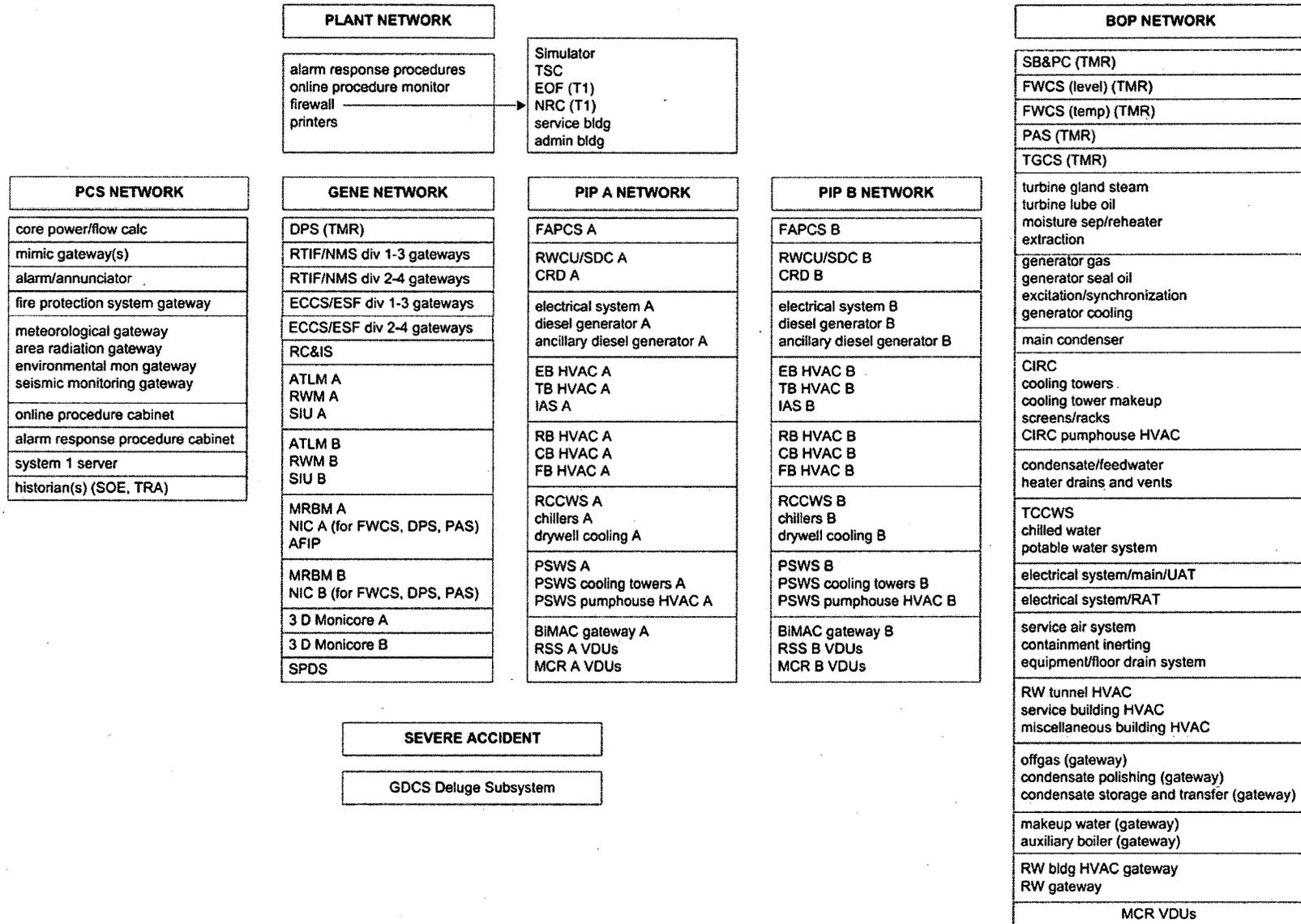
#### **5.2.1 ESBWR DCIS Hierarchy**

For diversity, the ESBWR I&C system is organized into three layers. The first layer contains the nonsafety-related N-DCIS that provides the monitoring, and the automatic and manual control of nonsafety-related functions. The N-DCIS, specifically the PIP A, PIP B and BOP control functions, includes sensors, rod control and information system (RC&IS) cabinets, control logic cabinets, RPV water level and pressure control, turbine generator control, power generation and automation control, and heat cycle and support systems control.

The N-DCIS also provides operator displays and alarm/annunciators in the MCR and RSS area. Dedicated functional processors perform display and alarm processing associated with the AMS; dedicated processors also provide the historian, SPDS, core thermal power and flow calculations and core thermal limits calculations. All of these processors acquire information from the other plant I&C systems (including the safety-related systems through isolated fiber gateways) by means of the real-time data network which is also part of N-DCIS.

Figure 7 is a simplified block diagram of the first layer (N-DCIS) control systems.

Figure 7 N-DCIS Control Systems



The second layer contains the Q-DCIS including separate reactor trip and SSLC/ESF processors. The Q-DCIS provides the safety-related reactor trip function, ESF actuation functions, and safety-related plant monitoring function. In the Q-DCIS, both automatic and manual means are provided to trip the reactor and actuate the engineered safety features. The Q-DCIS contains sensors, plant protection subsystems, RPS and SSLC/ESF coincidence logic, ESF actuation subsystems (solenoids and squib valves, logic buses, reactor scram solenoids, RMUs, operator monitoring and controls via safety-related VDUs).

The third layer contains the DPS that provides nonsafety-related reactor trip functions, actuation of engineered safety features, and operator displays. In the DPS, both automatic and manual means are provided to trip the reactor and actuate selected engineered safety features; automatic actuation uses two-out-of-four sensor trip information and triple redundant processors. The DPS also provides monitoring of plant parameters required to ascertain the state of the plant and provide guidance for manual actions by the operator. The DPS is specifically implemented in hardware and software that is diverse from that used in the Q-DCIS.

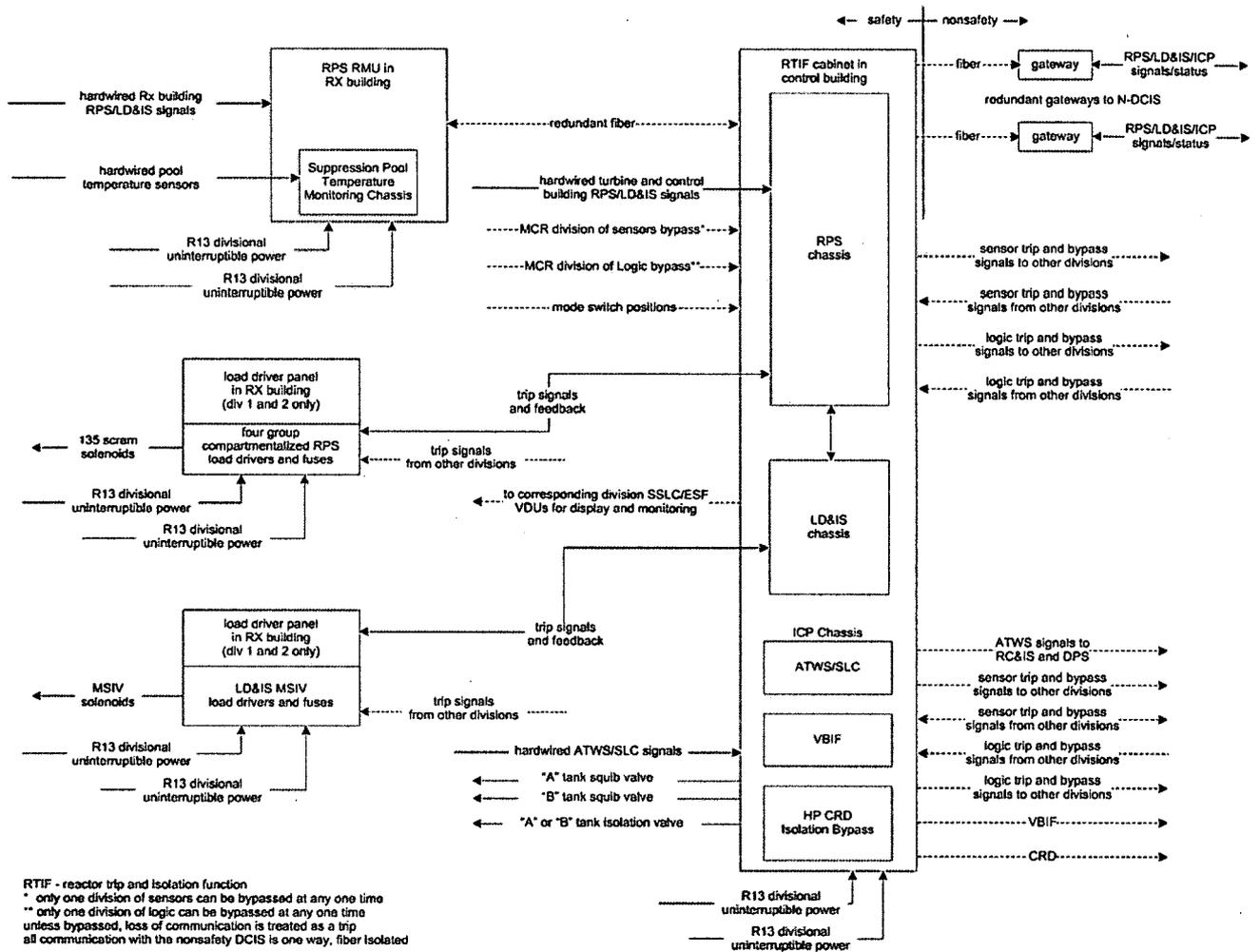
Figure 3 shows the integration of sensors, systems and power into the I&C architecture.

### 5.3 REACTOR SHUTDOWN

Reactor shutdown is the process of safely bringing the reactor to a sub-critical state in a timely manner and maintaining an adequate shutdown margin. This function is normally provided by inserting control rods into the core in a controlled manner, either by hydraulic insertion (safety-related/RPS and nonsafety-related/DPS) or electrically (nonsafety-related/DPS). The reactor can also be shut down by automatic or manual soluble boron injection into the coolant.

- The control rods can be hydraulically inserted into the core using stored nitrogen pressure (in scram accumulators). Control rod hydraulic insertion can be initiated by the RPS function of Q-DCIS or by the diverse scram and ARI functions of the DPS. The safety-related processors evaluate two-out-of-four sensor trip decisions and separately provide two-out-of-four scram decisions; the scram is initiated by using load drivers to interrupt the 120 VAC power to the scram solenoids on the HCUs. A backup scram circuit is simultaneously energized that picks up the solenoids that blow down the air headers common to all the HCUs and eventually causes a scram should the load drivers fail to open. The Q-DCIS also provides controls for manual insertion of the control rods by using contactors to directly interrupt the HCU scram solenoid current without any microprocessor involvement. ARI logic is executed by triple redundant DPS processors using two-out-of-four scram decision logic. A DPS scram output command results when two of the three redundant processors agree. The diverse ATWS/SLC logic automatically injects soluble boron and can independently shut down the reactor; ATWS/SLC also has the capability for manual initiation of ATWS mitigation (via Feedwater runback, ARI, electrical insertion control rod insertion (fine motion control rod drive [FMCRD] run-in), and SLC injection). The manual scram and ATWS/SLC system represent diversity within the Q-DCIS, which is in addition to the diversity provided by the DPS. Figure 8 illustrates the RPS function of the Q-DCIS.

Figure 8 Reactor Trip and Isolation Function of Q-DCIS



- The nonsafety-related RC&IS provides the capability to automatically or manually insert all of the control rods using their electric motors. Coincident with a hydraulic scram, RPS transmits a “scram follow” signal to RC&IS that causes an electric insertion of the control rods (if the hydraulic insertion fails) or that drives the ball-nut (that separates from the hollow piston of the control rod) to the full-in position to allow re-engagement of the hydraulically inserted control rod. DPS provides a similar scram follow signal and the ATWS mitigation logic also provides electrical run-in of the control rods through the DPS.
- The DPS provides automatic reactor shutdown by also providing hydraulic scram capability and the capability to insert control rods electrically. This nonsafety-related system uses a diverse set of sensors that are electrically independent from the Q-DCIS sensors, and uses processors and output devices that are diverse from those in Q-DCIS. Specifically the triple redundant processors of DPS make two-out-of-four sensor trip decisions and when two of the inputs to the three processors agree, the reactor is scrammed. The scram is initiated by interrupting the current from the 120 VAC return of the HCU scram solenoids. The DPS also provides for a manual scram independent of the Q-DCIS manual scram. The DPS uses a subset of Q-DCIS scram parameters to meet the requirements of Branch Technical Position (BTP) HICB-19 (Reference 6-2). The DPS scram parameters are further discussed in section 2.4.

#### 5.4 REACTOR COOLANT SYSTEM INVENTORY CONTROL

RCS inventory control is the process of maintaining sufficient water in the RPV to maintain reactor core heat removal capability.

- During normal and abnormal plant operation, RPV water level is automatically maintained from startup to rated power operation to shutdown by the FWCS. This control system and the mechanical Feedwater System is a triple redundant control design using four sensors and an N-1 feed pump arrangement that is single-failure proof for power generation. The system has a capacity of at least 135% feedwater flow that can accommodate even large leaks without requiring the use of the other safety-related and nonsafety-related systems. The system is available at all times that offsite power is available and can be operated manually.
- During normal and abnormal plant operation when offsite power is assumed to be unavailable but the PIP diesel generators are available, the nonsafety-related High Pressure Control Rod Drive Injection System is capable of injecting water against any reactor pressure up to the SRV setpoints. Similarly the FAPCS can inject water at medium reactor pressures available after reactor pressure has been reduced manually or automatically. Each of these systems utilize redundant trains with one train controlled by the PIP A N-DCIS segment and the other train by the PIP B N-DCIS segment, and each train can be operated independently.
- During accident situations when offsite power is not available, the Q-DCIS SSLC/ESF automatically initiates the four safety-related ICs. The ICs add inventory, and provide cooling/decay heat removal capability. At lower reactor power levels without offsite or diesel power, the Q-DCIS SSLC/ESF can automatically initiate an RPV depressurization (using both SRVs and DPVs) and then automatically drain the contents of the GDSCS pools into the RPV. SLC injection also occurs, coincident with the actuation of the first

DPV group, to provide additional inventory and buffering. This ECCS initiation keeps the core covered throughout the initial stages of the accident; later, the Q-DCIS can drain (“equalize”) the suppression pool water into the RPV for long term cooling. The ICs, RPV depressurization and GDCS can also be initiated manually.

- The DPS provides diverse coolant system inventory control by automatically initiating the ICs, SLC System, the ADS and GDCS Injection. The DPS uses sensors, processors and actuators that are diverse from those in Q-DCIS. Specifically the triple redundant processors of the DPS make two-out-of-four sensor trip decisions and when two of the three inputs to the processors agree, the required systems are initiated. The IC and SRV initiation is provided by opening nonsafety-related solenoids located “in parallel” with the existing safety-related solenoids. The explosive (squib) valves, the DPVs, GDCS and SLC System valves are fired by separate squib initiators “in parallel with” but isolated from the Q-DCIS squib initiators on those same valves. Automatic GDCS suppression pool equalizing function is not provided by the DPS because the earliest this function is required is 30 minutes following a LOCA and only in the unlikely event that RPV level reaches level 0.5; therefore, manual actuation is acceptable. DPS also provides for manual ADS initiation and GDCS injection sequencing for high drywell pressure conditions resulting from small and medium-break LOCA conditions since this logic is not required for approximately 60 minutes. The DPS also provides for manual initiations of these various systems diverse from the Q-DCIS manual initiations. Several scenarios are further discussed in Section 5.8.

## 5.5 CORE DECAY HEAT REMOVAL

Core decay heat removal is the process of maintaining a heat sink that is capable of cooling the reactor core after a reactor shutdown. A number of different systems can provide core decay heat removal including the nonsafety-related normal power heat sink and RWCU/SDC system and the safety-related ICs. Core decay heat removal is also facilitated by the fluid injection systems discussed in Section 5.4.

- During normal plant operation from startup to rated power operation to shutdown, core decay heat removal is accomplished with the bypass valves, the main turbine control valves, and the main condenser under the control of the SB&PC System and Turbine Generator Control System (TGCS); if offsite power is available, these systems also function during plant accidents. These control system designs are triple redundant using four sensors and an N-1 (at least) bypass valve and condenser shell arrangement that is single failure proof for power generation. The system has a capacity of at least 110% reactor steam flow and can easily accommodate any level of post scram decay heat without requiring the use of the other safety-related and nonsafety-related systems. The system is available at all times that offsite power is available and can be operated manually.
- During normal and abnormal plant operation when offsite power is assumed to be unavailable but the PIP diesel generators are available, the nonsafety-related RWCU/SDC system is capable of removing post shutdown decay heat at any reactor pressure up to the SRV setpoints. One train of the RWCU/SDC system is controlled by the PIP A N-DCIS segment and the other redundant train by the PIP B N-DCIS segment; each train can be operated independently.

- During accident situations offsite power is not available, Q-DCIS SSLC/ESF automatically initiates the four safety-related ICs. These systems passively remove core decay heat without inventory loss by transferring the heat to the IC/PCCS pools and, through pool boiling, to the atmosphere that represents the ESBWR ultimate heat sink. If the ICs fail or are otherwise inadequate, the resulting lower reactor water levels cause the Q-DCIS SSLC/ESF to automatically initiate an RPV depressurization (using both SRVs and DPVs) and then automatically drain the contents of the GDCS pools, SLC accumulators, and eventually the suppression pools, into the RPV. This keeps the core covered and decay heat is removed by sensible heat addition to the added water and later boiling. The GDCS pools and suppression pool are designed to supply long-term heat removal. The ICs, RPV depressurization, SLC and GDCS systems can also be initiated manually.
- The DPS provides diverse core decay heat removal by its ability to automatically initiate the same systems as the Q-DCIS, specifically ICs, the RPV depressurization system, the GDCS, and SLC. The IC and SRV initiation is provided by initiating nonsafety-related solenoids located “in parallel with” the existing safety-related solenoids. The explosive valves on the DPVs, GDCS and SLC system are fired by separate squib initiators “in parallel with” but isolated from the Q-DCIS inputs to the squib initiators on those same valves. The DPS also provides for manual initiations of these various systems of the Q-DCIS manual initiations. Manual action is required to drain (“equalize”) the suppression pool water into the RPV. Several scenarios are further discussed in Section 5.8.

## 5.6 CONTAINMENT COOLING

Containment cooling is the process of removing heat from the containment atmosphere.

- In normal or abnormal operation with offsite power or diesel generator power available, drywell cooling is provided by the PIP A and PIP B drywell cooling systems. The fans of the drywell coolers, the supporting chilled water, the RCCWS, and the PSWS can maintain the drywell within its design temperature. One train of the drywell cooling system is controlled by the PIP A N-DCIS segment and the other redundant train by the PIP B N-DCIS segment; each train can be operated independently.
- During normal or abnormal operation without offsite or diesel generator power available, the passive containment cooling system maintains containment cooling. There is a permanently open connection between the containment and the PCCS heat exchangers in the IC/PCCS pools above the containment. As containment temperatures increase the PCCS automatically removes more heat that is ultimately dissipated in pool temperature increase and boiling to the atmosphere. The connections to the between the equipment storage pool and IC/PCCS pools are required to ensure sufficient coolant for the initial 72 hours of an accident. The ICS automatically opens these connections when a low water level is detected in either of the IC/PCCS expansion pools. In addition to the Q-DCIS level and measurements and valve actuation, DPS uses diverse sensors for level measurement and opens the cross connect valves using actuators “in parallel with” the existing safety-related actuators controlled by the Q-DCIS.

## 5.7 CONTAINMENT ISOLATION

Containment isolation is the process of closing safety-related valves in fluid lines that penetrate the containment, to minimize the potential release of radioactivity from the containment, following an accident.

- During normal operation many containment isolation valves are open and can be automatically closed by the Q-DCIS; depending on the system different signals are used to initiate automatic closure. Manual isolation is also provided by the Q-DCIS.
- The MSIVs, certain steam line drain valves, and the vacuum breaker isolation valves are controlled by the RTIF-NMS and ICP portions of Q-DCIS respectively; the SSLC/ESF portion of Q-DCIS controls other isolation valves. The actuation logic typically uses a combination of low RPV water level, high drywell pressure, high area temperatures, high system flows or high differential flows to automatically close the affected valves. The logic is described in Tier 2 Chapter 7 of Reference 6-3.
- The DPS does not provide automatic isolation of all ESBWR containment isolation valves but isolates those that either present a potentially large leakage path to the plant environs or that provide a path for mass-energy influent which could challenge containment integrity. The choice of valves includes the MSIVs, the feedwater line isolation valves, the RWCU/SDC isolation valves, and the HP CRD isolation valves. The MSIVs are closed by the DPS on low RPV water level, low reactor pressure, or high steam line flow; the actuators are switches in the 120 VAC MSIV solenoid return circuit. The feedwater line isolation valves are closed when high differential pressure is sensed between feedwater lines coincident with high drywell pressure, or on high-high drywell pressure; the actuators are nonsafety-related solenoids "in parallel with" the existing safety-related solenoids controlled by the Q-DCIS. The RWCU/SDC isolation valves are closed by high differential flow; the actuators are nonsafety-related solenoids "in parallel with" the existing safety-related solenoids controlled by Q-DCIS. HP CRD is isolated on low GDCS pool level (two out of three GDCS pools) or high drywell pressure coincident with lower drywell high water level. The DPS also provides for manual isolation of these valves.

## 5.8 EVENT SCENARIOS

Appendix A provides a discussion of the Reference 6-3, Tier 2 Chapter 15 events evaluated to determine the effectiveness and scope of the DPS. The following sections provide a qualitative evaluation of DPS response to the same events used to evaluate the ATWS/SLC System, which has a similar (partial) function.

### **5.8.1 MSIV closure**

This event is effectively mitigated by the DPS. The DPS scrams the reactor directly on MSIV closure (on two or more main steam lines) and initiates the ICs on either low RPV water level or MSIV closure when needed to provide core cooling. Additionally the feedwater system and main condenser remain available with offsite power. The CRD, FAPCS and RWCU/SDC systems remain available to provide inventory and heat removal with diesel generator power – none of which are affected by a Q-DCIS failure.

### **5.8.2 Loss of Condenser Vacuum**

This event is effectively mitigated by the DPS. The main turbine, which is controlled by a triple redundant N-DCIS control system, trips on high condenser vacuum (insufficient vacuum), and is unaffected by the loss of the Q-DCIS. With the reactor effectively isolated, the DPS scrams the reactor directly on the resulting high pressure and initiates the ICs needed to provide core cooling. Additionally the CRD, FAPCS and RWCU/SDC systems remain available to provide inventory and heat removal with diesel generator backup power – none of which are affected by a Q-DCIS failure.

### **5.8.3 Loss of Feedwater Heating**

Since there is no DPS flux scram, this event is controlled by the amount of feedwater heating lost/reactor power increase and by SCRRI/SRI logic. Since the N-DCIS remains operational the situation is alarmed to the operator and control rods automatically inserted by the SCRRI/SRI logic from the DPS and ATLM. Even assuming the unlikely failure of the Q-DCIS manual scram, the reactor can be manually scrammed by the DPS. Since there is no coincident breach of piping or main condenser, the radiation consequences of fuel damage are concentrated in the power plant rather than offsite. There should be little or no offsite consequences.

### **5.8.4 Loss of Normal AC Power to Station Auxiliaries**

This event is effectively mitigated by the DPS. The DPS scrams the reactor directly on either low RPV water level from loss of feedwater flow or the high RPV pressure resulting from the turbine trip and bypass valve closure. Both the bypass valves and turbine are controlled by triple redundant N-DCIS control systems unaffected by the loss of Q-DCIS. The DPS initiates the ICs on low reactor level when needed to provide core cooling. Additionally, the CRD, FAPCS and RWCU/SDC systems remain available to provide inventory and heat removal with diesel generator power – none of which are affected by a postulated Q-DCIS failure.

### **5.8.5 Loss of Feedwater Flow**

This event is effectively mitigated by the DPS. The DPS scrams the reactor directly on low RPV water level from loss of feedwater flow; unlike the previous transient, the main condenser and bypass valve pressure control remains available. The turbine is eventually tripped either manually or on reverse power; both the bypass valves and turbine are controlled by triple redundant N-DCIS control systems unaffected by the loss of Q-DCIS. The DPS initiates the ICs on low RPV water level when needed to provide core cooling, if the level falls below the IC initiation set point. Additionally the CRD, FAPCS and RWCU/SDC systems remain available to

provide inventory and heat removal with offsite or diesel generator backup power – none of which are affected by a Q-DCIS failure.

#### **5.8.6 Generator Load Rejection with a Single Failure in the Turbine Bypass System**

This event is effectively mitigated by the DPS. The accident scenario depends on whether the Q-DCIS failure either does or does not scram the reactor (the scram is automatically bypassed if the bypass valves open). The single bypass system failure does not affect the SB&PC triple redundant control system nor the high-pressure electrohydraulic control (EHC) system (a standby pump automatically starts) so the failure is that one of the twelve bypass valves does not open. If the Q-DCIS scrams the plant, the remaining bypass valves, main condenser and feedwater allow/maintain normal RPV water level, reactor pressure and a normal shutdown. If the Q-DCIS does not scram the plant but the resulting steam flow is within the capacity of the eleven open bypass valves, then the above scenario is repeated. If the remaining bypass capacity is insufficient, the DPS scrams the plant on the resulting high RPV pressure.

If there is a loss of offsite power, the DPS scrams the reactor directly on low RPV water level from loss of feedwater flow or high RPV pressure resulting from the turbine and bypass valve trip (these control systems are unaffected by the Q-DCIS failure). The DPS initiates the ICs on low RPV water level when needed to provide core cooling, if the level falls below the IC initiation set point. Additionally, the CRD, FAPCS and RWCU/SDC systems remain available to provide inventory and heat removal with offsite or diesel generator backup power – none of which are affected by a Q-DCIS failure.

#### **5.8.7 Inadvertent Isolation Condenser Initiation**

This transient does not require mitigation by DPS since the result of the inadvertent actuation is the loss of some power generation as steam is diverted from the turbine. If a level transient resulted, the DPS would scram the reactor on level. The SB&PC should prevent a pressure transient since it is unaffected by the Q-DCIS failure. In any case, the IC pools begin heating. The IC pools cooling function will not be affected by the Q-DCIS failure. Since feedwater and the normal heat sinks remain available, the plant can be manually scrammed (from the DPS if necessary) and shut down normally. If offsite power is lost, the CRD, FAPCS and RWCU/SDC systems remain available to provide inventory and heat removal with diesel generator backup power – none of which are affected by a Q-DCIS failure.

#### **5.8.8 Turbine Trip with Full Bypass**

This event is effectively mitigated by the TMR SB&PC and SCRRI/SRI. This scenario depends on whether the Q-DCIS failure either does or does not scram the reactor (the scram is automatically bypassed if the bypass valves open). A manual DPS scram is available to shutdown the plant if needed. The bypass valves, normal heat sink and feedwater flow allow/maintain normal RPV water level, reactor pressure and a normal shutdown.

The DPS can also initiate the ICs on low RPV water level when needed to provide core cooling if the level falls below the IC initiation level set point. Additionally the CRD, FAPCS and RWCU/SDC systems remain available to provide inventory and heat removal with offsite or diesel generator backup power – none of which is affected by a Q-DCIS failure.

### 5.8.9 Opening of One Control or Turbine Bypass Valve

The open bypass valve transient generally does not require DPS mitigation since a Q-DCIS failure does not affect the TMR turbine control or SB&PC systems. The SB&PC and turbine control systems close a turbine control valve(s) to match the open bypass valve steam flow without level or pressure changes.

If the transient involves an opening turbine control valve or the turbine or bypass valve opening is too sudden for proper pressure control, a decreasing reactor pressure transient should result. This could eventually cause a low pressure MSIV isolation but the assumed Q-DCIS failure would prevent that. If the DPS did not isolate the reactor on low pressure, the low reactor (turbine inlet) pressure would be alarmed and the operator could use the DPS manual controls to scram to trip and isolate the reactor. (The operator could also manually trip the turbine and the stop valves would terminate the open control valve steam flow.) Whether or not the plant is scrammed, the remaining bypass valves, normal heat sink and feedwater flow allow/maintain normal RPV water level, reactor pressure and a normal shutdown. The DPS initiates the ICs on low reactor level when needed to provide core cooling if the level falls below the IC initiation level setpoint. Additionally, the CRD, FAPCS and RWCU/SDC systems remain available to provide inventory and heat removal with offsite or diesel generator backup power – none of which are affected by a Q-DCIS failure.

## 6. REFERENCES

- 6-1 US NRC NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems," October 21, 1994.
- 6-2 US NRC NUREG-0800, Appendix 7-A, Branch Technical Position HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," Revision 4, June 1997.
- 6-3 GEH ESBWR Design Control Document, Tier 1 and Tier 2
- 6-4 GEH NEDE-33245P LTR "ESBWR Software Quality Assurance Program Manual."
- 6-5 GEH NEDE-33226P, LTR "ESBWR I&C Software Management Program Manual."
- 6-6 IEEE 384-1981, "IEEE Criteria for Independence of Class 1E Equipment and Circuits."
- 6-7 GEH NEDO-33201, "ESBWR Certification Probabilistic Risk Assessment."
- 6-8 US NRC NUREG-0493, "A Defense-in-Depth & Diversity Assessment of the RESAR-414 Integrated Protection System," March 1979.
- 6-9 IEEE 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
- 6-10 IEEE 379-2000, "IEEE Standard Application of the Single-failure Criterion to Nuclear Power Generating Station Safety Systems – Description."
- 6-11 US NRC RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," May 1973.
- 6-12 Title 10, Code of Federal Regulations, Chapter 1, Appendix A to Part 50, General Design Criterion 24, Separation of Protection and Control Systems.
- 6-13 US NRC RG 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident."
- 6-14 US NRC DI&C-ISG-02, "Interim Staff Guidance on Diversity and Defense-in-Depth Issues", Revision 1, September 2007.

## **APPENDIX A: ESBWR INSTRUMENTATION & CONTROL DEFENSE-IN-DEPTH AND DIVERSITY (D3) EVALUATION OF REFERENCE 6-3, CHAPTER 15 EVENTS ASSUMING COMMON MODE FAILURE OF A DIGITAL PROTECTION SYSTEM**

### **INTRODUCTION**

This evaluation determines the effect of digital protection system common-cause/common mode failures on the events documented in Design Control Document Tier 2 Chapter 15, Safety Analyses (Reference 6-3), as required by Branch Technical Position (BTP) HICB-19 (Reference 6-2).

Reference 6-2 provides acceptance criteria for two sets of events (Abnormal Operating Occurrences (AOOs) and Design Basis Accidents). Some events are bounded and this conclusion is documented as part of the evaluation. For the purposes of this evaluation, the acceptance criteria for AOOs are applied to Infrequent Events.

This evaluation needs to be updated when the final design details of the protection system logic platforms (e.g., actual hardware and details of the hardware components are documented, and failure modes and effects reflect the final hardware and detailed logic design).

#### **Conclusions:**

Applying realistic assumptions, the following DPS functions mitigate the effects of digital protection system software common-cause failure scenarios applied to the Reference 6-3 design basis events:

Diverse reactor scram on the following signals:

- High RPV pressure,
- High drywell pressure,
- High suppression pool temperature,
- High RPV water level (L8),
- Low RPV water level (L3), or
- Inboard or outboard MSIV closure on two or more main steam lines.

Diverse ECCS (i.e., ICS, ADS, GDCS injection, and SLC) sequenced actuation on low RPV water level (Level 1).

Diverse manual ADS initiation and GDCS injection sequencing capability to respond to a high drywell pressure under conditions that do not result in a low RPV water level.

Diverse manual GDCS suppression pool equalizing function is provided in lieu of automatic actuation under the ECCS sequence because the earliest this function is required is 30 minutes following a LOCA and only in the unlikely event that RPV level reaches level 0.5.

Diverse opening of the IC/PCCS expansion pool to equipment storage pool cross-connect valves on low IC/PCCS expansion pool level.

Diverse ICS operation - reactor pressure control on the following signals:

- Inboard or outboard MSIV closure on two or more main steam lines
- Delayed high RPV pressure, or
- Delayed low RPV level (Level 2).

Diverse MSIV closure on the following signals:

- Low RPV water level,
- High reactor steam flow, and
- Low reactor pressure (i.e., turbine inlet pressure).

Diverse closure of the RWCU/SDC isolation valves on high differential flow.

Diverse closure of the feedwater isolation valves and tripping of the ASD controller circuit breaker for the feedwater pumps on either high drywell pressure coincident with high feedwater line differential pressure, or high-high drywell pressure, or high drywell pressure coincident with high drywell level.

Feedwater pump trip on high RPV level (Level 9)

Diverse Isolation of the CRD system high pressure makeup water injection to the RPV (HP CRD) on either high drywell pressure coincident with high drywell level, or low level in two out of three GDCS pools.

Acceptance Criteria:

Per BTP HICB-19 (Section 3: Acceptance Criteria)

- (1) *For each anticipated operational occurrence in the design basis which occurs in conjunction with each single postulated common-mode failure (CMF), the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding 10% of the 10 CFR 100 guideline value<sup>2</sup> or violate the integrity of the primary coolant pressure boundary.*
- (2) *For each postulated accident in the design basis which occurs in conjunction with each single postulated CMF, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding the 10 CFR 100 guideline values, violate the integrity of the primary coolant pressure boundary, or violate the integrity of the containment (i.e., exceed coolant system or containment design limits).<sup>3</sup>*

*For 1 and 2 above the analysis should either (1) demonstrate that sufficient diversity exists to achieve these goals, or (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies actions not taken.*

<sup>2</sup> The evaluations against the referenced 10 CFR 100 guidelines are formally evaluated against 10 CFR 52.47(a)(2)(iv).

<sup>3</sup> NUREG/CR-6303: has slightly different acceptance criteria wording: for each limiting fault in the design basis which occurs in conjunction with each postulated CCF, the combined action of all echelons of defense should ensure that equipment provided by the design and required to mitigate the effects of the accident is promptly initiated, supported by necessary auxiliary equipment, and operated for the necessary period of time. This guideline covers instrumentation system CCFs of types 2 and 3 (Guideline 3) for accidents. The plant response calculated using best-estimate (using realistic assumptions) analyses should not exceed the 10 CFR 100 dose limits, violate the integrity of the primary coolant pressure boundary, or violate the integrity of the containment.

- (3) *When a failure of a common element or signal source shared between the control system and the ESFAS is postulated, and (1) this common-mode failure results in a plant response that requires ESF, and (2) the common-mode failure also impairs the ESF function, then diverse means that are not subject to or failed by the postulated failure should be provided to perform the ESF function. The diverse means should ensure that the plant response calculated using best-estimate (realistic assumptions) analyses does not result in radiation release exceeding 10% of the 10 CFR 100 guideline value, or violation of the integrity of the primary coolant pressure boundary.*

*Interconnections between reactor trip and ESFAS (for interlocks providing for (1) reactor trip if certain ESFs are initiated, (2) ESF initiation when a reactor trip occurs, or (3) operating bypass functions) are permitted provided that it can be demonstrated that functions required by the ATWS rule (10 CFR 50.62) are not impaired.*

- (4) *No failure of monitoring or display systems should influence the functioning of the reactor trip system or the ESFAS. If plant monitoring system failure induces operators to attempt to operate the plant outside safety limits or in violation of the limiting conditions of operation, the analysis should demonstrate that such operator-induced transients will be compensated by protection system function.*

Note(s): The ESBWR Instrumentation & Control systems are designed such that there are no common elements or signal sources shared between the nonsafety-related control systems and the safety-related engineered safety features actuation system (ESFAS) or between the nonsafety-related control system and the safety-related reactor protection system. Additionally, there are no interconnections between the reactor trip system and ESFAS (SSLC/ESF, RTIF-LD&IS (MSIV), and ICP-VBIF logic). Therefore, acceptance criterion B.3.3 in BTP HICB-19 is satisfied based on the diversity of the ESBWR I&C platforms.

## Chapter 15 Event Analysis

### 15.2 Analysis of Anticipated Operational Occurrences

#### 15.2.1 Decrease in Core Coolant Temperature (Event Category)

##### 15.2.1.1 Loss of Feedwater Heating (AOO)

Systems / functions required (DCD Table 15.1-5: System Event Matrix): SCRRI/SRI

Automatic Trip (from DCD Table 15.1-6): None

Event Diagram: 15.1-2

Event Analysis: Non-limiting event. No reactor scram is assumed for this event (which results in a slow power increase). SCRRI/SRI, which is initiated by DPS and ATLM separately, is available to mitigate the event. Bypass valves are assumed to remain functional. No barrier breaches occur. No radiological consequences associated with this event.

Conclusion: No radiological consequences and no significant pressure challenge are associated with this event.

##### 15.2.2 Increase in Reactor Pressure

#### 15.2.2.1 Closure of One Turbine Control Valve (AOO)

Systems / functions required (DCD Table 15.1-5: System Event Matrix): None

Automatic Trip (from DCD Table 15.1-6): None

Event Diagram: 15.1-3

Event Analysis: Event bounded by load reject. SB&PC failure escalates event to infrequent event, but is not credible. SB&PC uses a triple modular redundant (TMR) controller and a discussion on the likelihood of its failure is presented in Section 15.2.4.2 of Reference 6-3. SB&PC acts to open remaining TCVs and some TBVs to maintain reactor pressure. The plant stabilizes at a new steady state. No barrier breaches occur and this event results in neutron flux within acceptable limits. This event does not result in fuel failure. Overpressure protection is available but not challenged.

Conclusion: No radiological consequences and no significant pressure challenge are associated with this event.

#### 15.2.2.2 Generator Load Rejection With Turbine Bypass (AOO)

Systems / functions required (DCD Table 15.1-5: System Event Matrix): TBV Initiation – TCV Fast Closure; SCRRI/SRI

Automatic Trip (from DCD Table 15.1-6): None

Event Diagram: 15.1-4

Event Analysis: Event bounded by load rejection with a single failure in the Turbine Bypass. SB&PC produces a fast opening of the TBVs and plant stabilizes at new steady state with a slight pressure increase. SCRRI/SRI assumed to function. Neutron flux may reach reactor scram setpoint (but CCF precludes trip). There is a possibility of a DPS high RPV pressure scram. However, SB&PC acts to mitigate event. This event does not result in fuel failure. No barrier breaches occur.

Conclusion: No radiological consequences are associated with this event. This event results in a slight pressure increase within the control range of SB&PC. Overpressure protection is available from the ICS and SRVs.

### **15.2.2.3 Generator Load Rejection With a Single Failure in the Turbine Bypass System (AOO)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): ICS initiation – MSIV position ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV closure – RPV Low Water Level (L2 + 30 sec delay); MSIV closure – Low Turbine Inlet/Main Steamline Pressure; TBV Initiation – TCV Fast Closure; Automatic Trip (from DCD Table 15.1-6): TCV Fast Closure (with insufficient bypass available)

Event Diagram: 15.1-5

Event Analysis: Only 50% of the BPVs are assumed to be available; pressurization is less severe than MSIV closure event and the event does not challenge scram setpoints. This event is bounded by MSIV closure event. Peak neutron flux and average simulated thermal power may increase but the event does not result in fuel failure.

Conclusion: No radiological consequences and no significant pressure challenge are associated with this event. Overpressure protection is available from the ICS and SRVs.

### **15.2.2.4 Turbine Trip With Turbine Bypass (AOO)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): TBV Initiation – TSV Closure; SCRRI/SRI

Automatic Trip (from DCD Table 15.1-6): None

Event Diagram: 15.1-6

Event Analysis: This event is bounded by Turbine trip with a Single Failure in the Turbine Bypass system. This event is similar to the generator load rejection with turbine bypass event. The pressure increase is mitigated by SB&PC, which in turn limits the thermal power increase.

Conclusion: No radiological consequences and no significant pressure challenge are associated with this event. Overpressure protection is available from the ICS and SRVs.

### **15.2.2.5 Turbine Trip With a Single Failure in the Turbine Bypass System (AOO)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): ICS initiation– MSIV Position; ICS – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV closure – RPV Low Water Level (L2 + 30 sec delay); MSIV closure – Low Turbine Inlet/Main Steamline Pressure; TBV Initiation –TSV Closure;

Automatic Trip (from DCD Table 15.1-6): TSV Closure (with insufficient bypass available)

Event Diagram: 15.1-7

Event Analysis: This event is bounded by the MSIV closure event. This event is similar to the generator load rejection with a single failure in the turbine bypass system event. In this event the single failure assumed results in the worst-case scenario of 50% of the bypass valves failing. A realistic failure is failure of one bypass valve to open (a TMR controller failure discussion is provided in Section 15.2.4.2 of Reference 6-3). The pressurization resulting from this event is

less severe than all MSIV closure event. The credited RPS flux scram is assumed to fail. SCRRRI/SRI is available to reduce power to avoid fuel failure.

Conclusion: No radiological consequences are associated with this event. Overpressure protection is available from the ICS and SRVs.

#### **15.2.2.6 Closure of One Main Steamline Isolation Valve (AOO)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): ICS initiation – MSIV position; MSIV Closure – High Steamline Flow

Automatic Trip (from DCD Table 15.1-6): MSIV Position

Event Diagram: 15.1-8

Event Analysis: This event is bounded by closure of all MSIVs.

Conclusion: No radiological consequences are associated with this event. Overpressure protection is available from the ICS and SRVs.

#### **15.2.2.7 Closure of All Main Steamline Isolation Valves (AOO)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): ICS initiation – MSIV position

Automatic Trip (from DCD Table 15.1-6): MSIV Position

Event Diagram: 15.1-9

Event Analysis: In this event, assume RPS (i.e., the RTIF-NMS platform including LD&IS – MSIV logic) does not function. The DPS MSIV position trip and ICS initiation occurs to mitigate the event. Additionally, the DPS high RPV pressure trip is reached within seconds and serves to limit the pressure transient. Pressure transient is bounded by the ATWS scenario. High neutron flux and vessel pressure are anticipated for this event.

Conclusion: No radiological consequences are associated with this event. DPS MSIV position scram occurs. ICS is initiated on MSIV position to limit the pressure increase, and results in no radiological consequences. Pressure response is bounded by ATWS analysis (discussed in DCD Section 15.5.4). Implementation of an MSIV closure trip in DPS provides margin. ICS operation prevents a challenge to the SRVs.

#### **15.2.2.8 Loss of Condenser Vacuum (AOO)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): ICS initiation – MSIV position; TSV Closure – Low Condenser Vacuum; MSIV Closure – Low Condenser Vacuum

Automatic Trip (from DCD Table 15.1-6): Low Condenser Vacuum

Event Diagram: 15.1-10

Event Analysis: If RPS CCF is assumed, vessel pressurization and peak cladding temperature may approach MSIV closure event which is bounding. Overpressure protection is available (with peak pressure controlled by the SRVs). An RPS CCF is the worst case for this event. With an RPS CCF, it may be possible that ATWS/SLC may fail to function due to unavailability of the NMS neutron flux permissive (same platform for RPS and NMS), but this function is not required for event mitigation. DPS MSIV closure and high RPV pressure scrams function to provide negative reactivity insertion within seconds. DPS initiates ICS on high RPV pressure to

avoid challenging the SRVs. The DPS MSIV closure and high RPV pressure scrams and ICS initiation attenuate the pressure transient. Manual scram from RPS or DPS is available to mitigate this event. (ATWS/SLC sensor indication and DPS sensor indication are available for operators to assess and determine an ATWS event has occurred and manual action is required.)

Conclusion: No radiological consequences are associated with this event. Overpressure protection is available from the ICS and SRVs.

### 15.2.2.9 Loss of Shutdown Cooling Function of RWCU/SDC (AOO)

Systems / functions required (DCD Table 15.1-5: System Event Matrix): ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation – RPV Low Water Level (L2 + 30 sec delay); GDCS

Automatic Trip (from DCD Table 15.1-6): None

Event Diagram: 15.1-11

Event Analysis: Not a significant event or limiting event. Operating systems function to mitigate this event. One train of SDC still assumed to function. In the unlikely event that both RWCU/SDC trains are lost, ICS is initiated by the DPS as a backup to SSLC/ESF. Fuel and Auxiliary Pools Cooling System (FAPCS) is available to provide alternate shutdown cooling in the event ICS is unavailable during Refueling mode. GDCS (initiation via the DPS) provides an additional layer of protection if RPV level approaches Level 1.

Conclusion: No radiological consequences are associated with this event and this event does not challenge the RCPB.

### 15.2.3 Reactivity and Power Distribution Anomalies (Event Category)

#### 15.2.3.1 Control Rod Withdrawal Error During Startup (AOO)

Systems / functions required (DCD Table 15.1-5: System Event Matrix): None

Automatic Trip (from DCD Table 15.1-6): No automatic trip credited. Rod Block – SRNM Period, RWM, ATLM Parameter Exceeded, or MRBM Parameter Exceeded

Event Diagram: 15.1-24a

Event Analysis: The Control Rod Withdrawal Error During Startup with Failure of Control Rod Block event, which is discussed in 15.3.8, bounds this event.

Conclusion: No radiological consequences are associated with this event and this event does not challenge the RCPB.

#### 15.2.3.2 Control Rod Withdrawal Error During Power Operation (AOO)

Systems / functions required (DCD Table 15.1-5: System Event Matrix): None

Automatic Trip (from DCD Table 15.1-6): No automatic trip credited. Rod Block – SRNM Period, RWM, ATLM Parameter Exceeded, or MRBM Parameter Exceeded

Event Diagram: 15.1-25b

Event Analysis: The Control Rod Withdrawal Error During Power Operation with ATLM Failure event, which is discussed in 15.3.9, bounds this event.

Conclusion: No radiological consequences are associated with this event and this event does not challenge the RCPB.

#### **15.2.4 Increase in Reactor Coolant Inventory (Event Category)**

##### **15.2.4.1 Inadvertent Isolation Condenser Initiation (AOO)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): FWCS (Level Controller)

Automatic Trip (from DCD Table 15.1-6): None

Event Diagram: 15.1-12

Event Analysis: This event is potentially limiting for OLMCPR; however no significant effect is experienced and plant control systems (i.e., water level control and SB&PC) respond to mitigate this event.

Conclusion: No radiological consequences are associated with this event. Startup of the isolation condenser causes a slight pressure decrease; therefore the event does not challenge the RCPB.

##### **15.2.4.2 Runout of One Feedwater Pump (AOO)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): FWCS (Level Controller)

Automatic Trip (from DCD Table 15.1-6): None

Event Diagram: 15.1-13

Event Analysis: The Feedwater Control System acts to reduce flow from other pumps to maintain desired water level. Neither RPS nor SSLC/ESF is credited. With failure of RPS, DPS is available to produce a high water level L8 reactor scram as a worst-case scenario. This is not a significant or limiting event.

Conclusion: No radiological consequences are associated with this event and this event does not result in an RCPB challenge.

#### **15.2.5 Decrease in Reactor Coolant Inventory (Event Category)**

##### **15.2.5.1 Opening of One Turbine Control or Bypass Valve (AOO)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): None

Automatic Trip (from DCD Table 15.1-6): None

Event Diagram: 15.1-14

Event Analysis: SB&PC mitigates event by modulating of other TCVs and/or TBVs to stabilize the transient. No protection systems are credited.

Conclusion: No radiological consequences are associated with this event and no RCPB challenge is associated with this event.

##### **15.2.5.2 Loss of Non-Emergency AC Power to Station Auxiliaries (AOO)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): ICS initiation – Loss of Power Generation Bus (Loss of Feedwater Flow); MSIV closure – RPV Low Water Level (L2 +

30 sec delay); TBV Initiation – TCV Fast Closure; TCV Fast Closure – Load rejection; MSIV Closure – Low Condenser Vacuum;

Automatic Trip (from DCD Table 15.1-6): Loss of Power on Power Generation Buses - Loss of Feedwater Flow

Event Diagram: 15.1-15

Event Analysis: This event is similar to the loss of all feedwater flow event. Level approaches L3 very quickly due to loss of power to the feedwater pump motors. Condenser vacuum is lost due to circulating water pump trips. Brief operation of bypass valves is assumed until vacuum decays. If RPS fails to process scram signals, DPS (L3) scram is available to provide negative reactivity insertion quickly. SCRRI/SRI is also available for power reduction prior to the DPS scram. DPS can initiate ICS on a delayed L2 signal to maintain level. HP CRD flow to the RPV is available for level recovery after diesel generator start (i.e., within 145 seconds).

Conclusion: No radiological consequences are associated with this event and no RCPB challenge is associated with this event.

### 15.2.5.3 Loss of All Feedwater Flow (AOO)

Systems / functions required (DCD Table 15.1-5: System Event Matrix): ICS initiation –Loss of Power Generation Bus (Loss of Feedwater Flow); MSIV closure – RPV Low Water Level (L2 + 30 sec delay)

Automatic Trip (from DCD Table 15.1-6): Loss of Power on Power Generation Buses- Loss of Feedwater Flow

Event Diagram: 15.1-16

Event Analysis: (This event is similar to loss of power generation bus, which trips power to all feedwater pump motors.) If CCF of RPS assumed, DPS provides scram at L3. It is possible that the loss of all feedwater flow resulted from the trip of the feedwater pumps on high RPV level. In this case, DPS provides a scram at L8, with a resultant level decrease. DPS also starts ICS on delayed L2 signal. HP/CRD pumps also start on a delayed L2 signal to provide level recovery. Not a limiting event.

Conclusion: No radiological consequences are associated with this event and no RCPB challenge is associated with this event.

### 15.2.6 AOO Analysis Summary

Conclusions are provided within each event evaluation.

### 15.2.7 COL Information (Event Category) - Not Applicable

## 15.3 Analysis of Infrequent Events

### 15.3.1 Loss of Feedwater Heating With Failure of SCRRI and SRI (Infrequent Event)

Systems / functions required (DCD Table 15.1-5: System Event Matrix): High Radiation MCR EFU Initiation

Automatic Trip (from DCD Table 15.1-6): APRM High Simulated Thermal Power

Event Diagram: 15.1-17

Event Analysis: ATLM and DPS independently initiate SCRRI/SRI on a loss of feedwater heating event. Failure of SCRRI/SRI and RPS simultaneously is of extremely low probability, especially when combined with the failure of the feedwater temperature controller. (In the unlikely scenario of both SCRRI/SRI failure and RPS CCF, a percentage of fuel may fail.)

Conclusion: Worst case dose is within 10% of 10 CFR 52.47(a)(2)(iv) dose limits. The ESBWR is designed such that no single operator error or equipment failure shall cause a loss of more than 55.6 °C (100 °F) feedwater heating. The assumption of 1000 rods entering transition boiling and subsequently failing is conservative. Using realistic assumptions, acceptance criteria are met, without crediting DPS action.

### **15.3.2 Feedwater Controller Failure – Maximum Flow Demand (Infrequent Event)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): ICS initiation – MSIV Position; ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV closure – RPV Low Water Level (L2 + 30 sec delay); TBV Initiation – TSV Closure; TSV Closure – RPV high water Level (L8); MSIV Closure – Low Turbine Inlet/Main Steamline Pressure

Automatic Trip (from DCD Table 15.1-6): RPV High Water Level (L8)

Event Diagram: 15.1-18

Event Analysis: Assume RPS failure for this event, DPS provides scram on L8 to mitigate this event. FW runback occurs. As a backup, DPS trips the feedwater pumps at L9. SB&PC is available to control pressure.

Conclusion: No radiological consequences associated with this event. SB&PC controller failure mode not assumed credible, using realistic assumptions. DPS initiated scram on L8 occurs early enough to limit neutron flux peak and fuel thermal transient so that no fuel damage occurs. This event does not challenge RCPB pressure and temperature limits.

### **15.3.3 Pressure Regulator Failure Opening of All Turbine Control and Bypass Valves (Infrequent Event)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): ICS initiation – MSIV Position; MSIV Closure – Low Turbine Inlet Pressure

Automatic Trip (from DCD Table 15.1-6): MSIV Position

Event Diagram: 15.1-19

Event Analysis: Using realistic assumptions, a complete failure of the SB&PC is not assumed credible. SB&PC should function to mitigate this event. Failure of RPS requires DPS MSIV closure scram and/or L3 scram to mitigate the event.

If SSLC/ESF CCF assumed, RPS scrams on MSIV closure from low turbine inlet pressure. Diverse ICS initiation occurs on decreasing level (delayed L2). If level drops to L1, diverse ESF (ECCS) initiation occurs.

Conclusion: No radiological consequences are associated with this event and no RCPB challenge associated with this event.

### **15.3.4 Pressure Regulator Failure – Closure of All Turbine Control and Bypass Valves (Infrequent Event)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): ICS initiation – MSIV Position; ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV Closure - RPV Low Water Level (L2 + 30 Sec delay); MSIV closure – Low Turbine Inlet/Main Steamline Pressure

Automatic Trip (from DCD Table 15.1-6): APRM High Neutron Flux

Event Diagram: 15.1-20

Event Analysis: Using realistic assumptions, a complete failure of the SB&PC is not assumed as a credible event. Therefore, reactor power and pressure should be controlled by SB&PC. This event is bounded by closure of all MSIVs for over pressure (an analysis of this event is provided in DCD Section 15.5.4). Reactor pressure is maintained below ASME Service Level C limit (<120% of design pressure). In the event of an unlikely SB&PC failure, a turbine trip is generated with a failure of RPS to scram as the worst-case scenario. DPS scrams on high pressure and initiates ICS to limit the pressure transient. Overpressure protection is available from ICS and SRVs.

Conclusion: No radiological consequences are associated with this event. With failure of the RPS flux scram fuel failure is more likely to occur. The dose acceptance criterion (10% of 10 CFR 52.47(a)(2)(iv) dose limits) is not challenged. Overpressure protection is available from ICS and SRVs to protect the RCPB.

### **15.3.5 Generator Load Rejection with Total Turbine Bypass Failure (Infrequent Event)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): ICS initiation – MSIV Position; ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV Closure - RPV Low Water Level (L2 + 30 Sec delay); TCV Fast closure – Load Rejection; MSIV closure – Low Turbine Inlet/Main Steamline Pressure; High Radiation MCR EFU Initiation

Automatic Trip (from DCD Table 15.1-6): TCV Fast Closure (with insufficient bypass available)

Event Diagram: 15.1-21

Event Analysis: Using realistic assumptions, a complete failure of the SB&PC not assumed. Bounded by closure of all MSIV event for overpressure. If RPS CCF assumed, DPS provides high –RPV pressure scram. ICS and HP-CRD are still available to stabilize the plant. If SSLC/ESF CCF assumed, RPS scram occurs on TCV fast closure with insufficient bypass capacity and RPS high neutron flux scram and high RPV pressure scram are available as backups.

Conclusion: Although not likely to occur if realistic assumptions are applied, there is a fuel failure analysis in DCD 15.3.1.5 for this event which is bounding. With failure of the TCV/flux scram fuel failure would be more severe.

Overpressure protection still available. Radiological consequences are bounded by the analytical assumption of 1000 rods entering transition boiling and subsequently failing, with off-site dose below the acceptance criterion (i.e., less than 10% of 10 CFR 52.47(a)(2)(iv) dose limits). Overpressure protection is available from the ICS and SRVs.

### **15.3.6 Turbine Trip with Total Turbine Bypass Failure (Infrequent Event)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): ICS initiation – MSIV Position; ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV Closure - RPV Low Water Level (L2 + 30 Sec delay); MSIV closure – Low Turbine Inlet/Main Steamline Pressure; High Radiation MCR EFU Initiation

Automatic Trip (from DCD Table 15.1-6): TSV Closure (with insufficient bypass available)

Event Diagram: 15.1-22

Event Analysis:

Using realistic assumptions, a complete failure of the SB&PC is not assumed. If RPS CCF assumed, DPS provides high-pressure trip and can initiate ICS on high RPV pressure. If SSLC/ESF CCF is assumed, RPS available for high –RPV pressure scram, high neutron flux scram and TSV closure with insufficient bypass scrams.

Conclusion: There is a fuel failure analysis in DCD 15.3.1.5 for this event. With failure of the TSV closure and flux scrams, fuel failure is more severe. This event is assumed to be bounded by the load rejection with no bypass. Radiological consequences are bounded by the analytical assumption of 1000 rods entering transition boiling and subsequently failing, with off-site dose below the acceptance criterion (i.e., less than 10% of 10 CFR 52.47(a)(2)(iv) dose limits).

Overpressure protection is available from the ICS and SRVs to protect RCPB.

### **15.3.7 Control Rod Withdrawal Error During Refueling (Infrequent Event)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): None

Automatic Trip (from DCD Table 15.1-6): No automatic trip credited. Rod Block – SRNM Period, RWM, ATLM Parameter Exceeded, or MRBM Parameter Exceeded

Event Diagram: 15.1-23

Event Analysis: Core is designed to meet shutdown requirements and remain subcritical with one control rod pair or one rod of maximum worth withdrawn. Event is a low probability event that is mitigated by RC&IS interlocks that prevent additional withdrawals.

Conclusion: Not analyzed based on core design and RC&IS interlocks.

### **15.3.8 Control Rod Withdrawal Error During Startup with Failure of Control Rod Block (Infrequent Event)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): None

Trip/Protection (from DCD Table 15.1-6): SRNM Period

Event Diagram: 15.1-24

Event Analysis: Tightly controlled evolution with monitoring and feedback. Although withdrawal error postulated, recovery from error crediting operator action to manually scram the reactor and place the plant in a safe condition is assumed. Operability verified just prior to the event. Any aberrant indication requires the operator to stop and verify information and place the plant in a safe condition, before significant reactivity excursion occurs. Either APRM or SRNM assumed to fail but not both.

Conclusion: No radiological consequences are associated with this event. No RCPB challenge associated with this event.

### **15.3.9 Control Rod Withdrawal Error During Power Operations with ATLM Failure (Infrequent Event)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): High Radiation MCR EFU Initiation

Automatic Trip (from DCD Table 15.1-6): No automatic trip credited. Rod Block – SRNM Period, RWM, ATLM Parameter Exceeded, or MRBM Parameter Exceeded

Event Diagram: 15.1-25

Event Analysis: Simultaneous failure of RC&IS and RPS/NMS is extremely low. If a failure of both ATLM channels occurs which does not inhibit rod movement as designed, MRBM prevents control rod withdrawal from continuing. The radiological analysis performed in DCD 15.3.1.5 which conservatively assumes 1000 rods enter transition boiling and subsequently fail, bounds this event.

Conclusion: Radiological consequences associated with this event if conservative assumptions are used are still below the acceptance criterion (i.e., less than 10% of 10 CFR 52.47(a)(2)(iv) dose limits). No RCPB challenge associated with this event.

### **15.3.10 Fuel Assembly Loading Error, Mislocated Bundle (Infrequent Event)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): None

Automatic Trip (from DCD Table 15.1-6): None

Event Diagram: 15.1-26

Event Analysis: Tightly controlled evolution with procedural steps for error checking. DPS not required.

Conclusion: No safety systems are credited in mitigating this event. The existing DCD Chapter 15 analysis applies.

### **15.3.11 Fuel Assembly Loading error, Misoriented Bundle (Infrequent Event)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): None

Automatic Trip (from DCD Table 15.1-6): None

Event Diagram: 15.1-27

Event Analysis: Tightly controlled evolution with procedural steps for error checking. DPS not required.

Conclusion: No safety systems are credited in mitigating this event. The existing DCD Chapter 15 analysis applies.

### **15.3.12 Inadvertent SDC Function Operation (Infrequent Event)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): None

Automatic Trip (from DCD Table 15.1-6): APRM High Neutron Flux

Event Diagram: 15.1-28

Event Analysis: If RPS CCF assumed, SB&PC is available to mitigate this event. This event is characterized by a slow power rise. Operator action can be credited for tightly controlled startup/shutdown scenario where the largest effects are manifested.

Conclusion: No radiological consequences are associated with this event. No RCPB challenge is associated with this event.

### **15.3.13 Inadvertent Opening of a Safety/Relief Valve (Infrequent Event)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): None

Automatic Trip (from DCD Table 15.1-6): High Suppression Pool Temperature

Event Diagram: 15.1-29

Event Analysis: SB&PC available to stabilize pressure prior to occurrence of a scram, after which time the pressure will decrease. If RPS CCF assumed, DPS available to scram on high suppression pool temperature. FAPCS provides suppression pool cooling.

Conclusion: This event should not result in a release. Therefore no radiological consequences are associated with this event.

### **15.3.14 Inadvertent Opening of a Depressurization Valve (Infrequent Event)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): SRV – Power Actuated Mode (ADS); DPV – Actuation; GDCCS; Passive Containment Cooling System (PCCS).

Automatic Trip (from DCD Table 15.1-6): High Drywell Pressure

Event Diagram: 15.1-30

Event Analysis: SB&PC is available to stabilize pressure prior to occurrence of scram after which time the pressure decreases. If RPS CCF assumed, DPS is available to scram on high drywell pressure. PCCS is available to limit containment pressure. Transient controlled by SB&PC and high drywell pressure trip. Diverse ESF is available and may be required if conditions degrade

Conclusion: No fuel damage anticipated for this event, only coolant activity is a concern. Worst-case dose is within 10% of 10 CFR 52.47(a)(2)(iv) dose limits Radiation monitoring and isolation can be credited.

### **15.3.15 Stuck Open Safety/Relief Valve (Infrequent Event)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): SRV – Power Actuated Mode (ADS); DPV – Actuation; ICS initiation – MSIV Position; MSIV Closure – Low Turbine Inlet /Main Steamline Pressure; GDCCS; PCCS

Automatic Trip (from DCD Table 15.1-6): None

Event Diagram: 15.1-31

Event Analysis: This event assumes the SRV is stuck after lifting from a high RPV pressure condition, where an RPS scram on high RPV pressure as part of the initial conditions. If RPS CCF assumed DPS scrams on high RPV pressure with high suppression pool temperature as a backup. FAPCS provides suppression pool cooling.

If SSLC/ESF CCF assumed, RPS provides scram on high RPV pressure with high suppression pool temperature as a backup.

Conclusion: No fuel failure occurs in this event, only coolant activity is a concern. Worst-case dose within 10% of 10 CFR 52.47(a)(2)(iv) dose limits. Radiation monitoring and isolation can be credited.

### **15.3.16 Liquid Containing Tank Failure (Infrequent Event)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): High Radiation MCR EFU Initiation

Automatic Trip (from DCD Table 15.1-6): None

Event Diagram: 15.1-32

Event Analysis: All normally operating systems assumed available to mitigate this event. This event does not involve the RPV or containment and requires no actions from RPS. A 5-rem onsite dose is assumed which could potentially impact control room habitability. Area and process radiation monitors are assumed to function to annunciate any potential release. If SSLC/ESF fails to automatically isolate the control room and start the EFUs, manual actuation of the EFUs is assumed to be available.

Conclusion: This event results in potential adverse consequences to the main control room operators, if there is a failure to maintain control room habitability, due to a failure of SSLC/ESF logic processors. SSLC/ESF capability to manually provide control room habitability is assumed due to the diversity between the VDU controls and the automatic logic.

### **15.3.17 COL Information - Not Applicable**

## **15.4 Analysis of Accidents (Event Category)**

### **15.4.1 Fuel Handling Accident (Accident)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): None

Automatic Trip (from DCD Table 15.1-6): None

Event Diagram: 15.1-33

Event Analysis: Tightly controlled evolution; ventilation systems assumed available to mitigate this event. Credit taken for Radiation Monitoring System. This event does not involve the RPV or containment and requires no actions from RPS, SSLC/ESF, or DPS.

Conclusion: Worst-case dose within 10 CFR 52.47(a)(2)(iv) dose limits.

### **15.4.2 Loss-of-Coolant Accident Inside Containment (Accident)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): SRV – Power Actuated Mode (ADS); DPV – Actuation; ICS initiation – MSIV position; ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L1); ICS initiation – Loss of Power Generation Bus (Loss of Feedwater Flow); Feedwater Isolation Signals; HP CRD Isolation Signals; SLC System - DPV Open; GDCS; GDCS Equalizing Lines; High Radiation MCR EFU Initiation; PCCS

Automatic Trip (from DCD Table 15.1-6): RPV Low Water Level (L3); Loss of Power Generation Bus- Loss of Feedwater Flow; High Drywell Pressure

Event Diagram: 15.1-34

Event Analysis: If RPS CCF assumed, DPS provides scram on low water level (L3) or high drywell pressure. LD&IS (MSIV) isolation failure assumed because of the same platform as RPS and DPS provides MSIV isolation (on low reactor pressure or high steamline flow or low RPV level) to limit consequences. SSLC/ESF initiation occurs to mitigate the event. Non-MSIV LD&IS isolation occurs. If SSLC/ESF CCF is assumed, diverse ESF initiation (at L1) is required to mitigate the event. In the event of a feedwater line break inside containment, the DPS is also capable of isolating the feedwater lines on high differential pressure between the feedwater lines coincident with high drywell pressure.

Conclusion: The worst-case dose does not exceed 10 CFR 52.47(a)(2)(iv) dose limits. Diverse ECCS initiation available to mitigate the event. Diverse containment or feedwater system isolation may be required to mitigate the event, either of which is provided by the DPS.

#### **15.4.3 Loss-of-Coolant Accident ECCS Performance Analysis (Accident)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): SRV – Power Actuated Mode (ADS); DPV – Actuation; ICS initiation – MSIV Position; ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L1); ICS initiation – Loss of Power Generation Bus (Loss of Feedwater Flow); Feedwater Isolation Signals; HP CRD Isolation Signals; SLC System - DPV Open; GDCS; GDCS Equalizing Lines; High Radiation MCR EFU Initiation; PCCS

Automatic Trip (from DCD Table 15.1-6): RPV Low Water Level (L3); Loss of Power Generation Bus-Loss of Feedwater Flow; High Drywell Pressure

Event Diagram: 15.1-34

Event Analysis: Refer to 15.4.2

Conclusion: Refer to 15.4.2

#### **15.4.4 Loss-of-Coolant Accident Inside Containment Radiological Analysis (Accident)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): SRV – Power Actuated Mode (ADS); DPV – Actuation; ICS initiation – MSIV Position; ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L1); ICS initiation – Loss of Power Generation Bus (Loss of Feedwater Flow); Feedwater Isolation Signals; HP CRD Isolation Signals; SLC System - DPV Open; GDCS; GDCS Equalizing Lines; High Radiation MCR EFU Initiation; PCCS

Automatic Trip (from DCD Table 15.1-6): RPV Low Water Level (L3); Loss of Power Generation Bus-Loss of Feedwater Flow; High Drywell Pressure

Event Diagram: 15.1-34

Event Analysis: Refer to 15.4.2

Conclusion: Refer 15.4.2

#### **15.4.5 Main Steamline Break Accident Outside Containment (Accident)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): SRV – Power Actuated Mode (ADS); DPV – Actuation; ICS initiation – MSIV Position; ICS initiation – RPV High

Dome Pressure (10 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L1); ICS initiation – Loss of Power Generation Bus (Loss of Feedwater Flow); MSIV Closure – Low Turbine Inlet/Main Steamline Pressure; MSIV Closure – High Steamline Flow; SLC System - DPV Open; GDCS; GDCS Equalizing Lines; High Radiation MCR EFU Initiation

Automatic Trip (from DCD Table 15.1-6): RPV Low Water Level (L3); MSIV Position; Loss of Power Generation Bus-Loss of Feedwater Flow

Event Diagram: 15.1-35

Event Analysis: If RPS CCF is assumed, DPS provides scram on low water level (L3). LD&IS (MSIV) isolation failure is assumed because of the same platform as RPS and DPS isolates the MSIVs (on low reactor pressure or high steamline flow or low RPV level) to limit consequences. SSLC/ESF initiation occurs. If SSLC/ESF CCF assumed, diverse ESF initiation (at L1) is required to mitigate the event.

Conclusion: Worst-case dose does not exceed 10 CFR 52.47(a)(2)(iv) dose limits. Diverse ECCS initiation and diverse MSIV isolation mitigate the event.

#### **15.4.6 Control Rod Drop Accident (Accident)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): No systems credited.

Automatic Trip (from DCD Table 15.1-6): Rod Block – SRNM Period, RWM, ATLM Parameter Exceeded, or MRBM Parameter Exceeded

Event Diagram: 15.1-36

Event Analysis: No clad failures are predicted and no automatic trip or ESF is credited.

Conclusion: This event does not result in any fuel failures or any radiological consequences, and does not challenge the RCPB.

#### **15.4.7 Feedwater Line Break Outside Containment (Accident)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): SRV – Power Actuated Mode (ADS); DPV – Actuation; ICS initiation – MSIV Position; ICS initiation and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L1); ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation – Loss of Power Generation Bus (Loss of Feedwater Flow); SLC System - DPV Open; GDCS; GDCS Equalizing Lines; High Radiation MCR EFU Initiation; PCCS

Automatic Trip (from DCD Table 15.1-6): RPV Low Water Level (L3); MSIV Position; Loss of Power Generation Bus-Loss of Feedwater Flow

Event Diagram: 15.1-37

Event Analysis: If RPS CCF is assumed, DPS provides scram on low water level (L3). SSLC/ESF initiation occurs. If SSLC/ESF CCF assumed, diverse ESF initiation (at L1) is required to mitigate the event.

Conclusion: No fuel failure is assumed for this event. Worst-case dose does not challenge 10 CFR 52.47(a)(2)(iv) dose limits,.

#### **15.4.8 Failure of Small Line Carrying Primary Coolant Outside Containment (Accident)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): SRV – Power Actuated Mode (ADS); DPV – Actuation; ICS initiation – MSIV Position; ICS initiation and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L1); ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation – Loss of Power Generation Bus (Loss of Feedwater Flow); SLC System - DPV Open; GDCS; GDCS Equalizing Lines; High Radiation MCR EFU Initiation; PCCS

Automatic Trip (from DCD Table 15.1-6): RPV Low Water Level (L3); MSIV Position; Loss of Power Generation Bus-Loss of Feedwater Flow

Event Diagram: 15.1-38

Event Analysis: Leak detection by aberrant indication (radiation, temperature, humidity or noise) alerts operator to perform an orderly shutdown. If RPS CCF assumed, manual reactor scram is still available. DPS provides manual backup scram. Manually controlled orderly shutdown is performed to depressurize the reactor if leak is not isolable. Manual containment isolation and diverse ESF are available. CR habitability not impacted adversely.

Conclusion: This line break is bounded by larger breaks. Using realistic assumptions, excess flow check valves limit the release of coolant. Dose is within 10 CFR 52.47(a)(2)(iv) dose limits.

#### **15.4.9 RWCUC/SDC System Line Failure Outside Containment (Accident)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): SRV – Power Actuated Mode (ADS); DPV – Actuation; ICS initiation – MSIV Position; ICS initiation and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L1); ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation – Loss of Power Generation Bus (Loss of Feedwater Flow); SLC System - DPV Open; GDCS; GDCS Equalizing Lines; High Radiation MCR EFU Initiation; PCCS

Automatic Trip (from DCD Table 15.1-6): RPV Low Water Level (L3); MSIV Position; Loss of Power Generation Bus-Loss of Feedwater Flow

Event Diagram: 15.1-39

Event Analysis: If RPS CCF assumed, DPS available to scram on L3. If level continues to drop, ESF initiation occurs at L1, and differential flow sensors are available to isolate the RWCUC/SDC line. If SSLC/ESF CCF is assumed which results in failure of LD&IS to provide isolation signal, diverse ESF is available. Diverse initiation occurs at L1. Diverse differential flow sensors are available to isolate the RWCUC/SDC line.

Conclusion: Worst-case dose may challenge 10 CFR 52.47(a)(2)(iv) dose limits with CCF of LD&IS. Diverse RWCUC/SDC isolation and diverse ECCS are provided to mitigate. If exposure does not challenge 10 CFR 52.47(a)(2)(iv) dose limits, no additional DPS scope is required.

#### **15.4.10 Spent Fuel Cask Drop Accident (Accident)**

Systems / functions required (DCD Table 15.1-5: System Event Matrix): None

Automatic Trip (from DCD Table 15.1-6): None

Event Diagram: 15.1-40

Event Analysis: Controlled evolution. Normal operating systems are assumed to be available. This event does not involve the RPV or containment and requires no actions from RPS, SSLC/ESF, or DPS.

Conclusion: No adverse consequences.

**15.4.11 (COL Information) - Not Applicable**

**15.5 Special Event Evaluations (Event Category)**

The events in this section are beyond design basis events per DCD 15.0.1.2 and are not included in this evaluation.