



**GE Energy  
Nuclear**

NEDO-33251  
Class I  
eDRF# 0000-0055-9783  
July 2006

**LICENSING TOPICAL REPORT**

**ESBWR I&C**

**DEFENSE-IN-DEPTH AND DIVERSITY REPORT**

*Copyright 2006 General Electric Company*

**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 reference to the NRC Staff for the purpose of obtaining NRC approval of the ESBWR Certification and implementation. The only undertakings of General Electric Company with respect to information in this document are contained in contracts between General Electric Company 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, General Electric Company 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

<b>LIST OF ACRONYMS AND ABBREVIATIONS .....</b>	<b>vi</b>
<b>GLOSSARY OF TERMS.....</b>	<b>ix</b>
<b>1 INTRODUCTION.....</b>	<b>1</b>
1.1 PREFACE.....	1
1.2 ARCHITECTURE OVERVIEW .....	2
1.3 SCOPE .....	2
1.4 SUMMARY AND CONCLUSIONS .....	3
1.4.1 Complies with NUREG-0493 .....	3
1.4.2 Complies with NUREG/CR-6303.....	3
1.4.3 Meets Probabilistic Safety-Related Goals .....	3
<b>2 ESBWR INSTRUMENTATION AND CONTROL ARCHITECTURE / SYSTEMS DESCRIPTION .....</b>	<b>4</b>
2.1 ARCHITECTURE DESCRIPTION .....	4
2.2 SAFETY SYSTEM DISTRIBUTED CONTROL AND INSTRUMENTATION SYSTEM OVERVIEW .....	14
2.3 NON-SAFETY SYSTEM DISTRIBUTED CONTROL AND INSTRUMENTATION SYSTEM OVERVIEW .....	17
2.4 DIVERSE PROTECTION SYSTEM OVERVIEW.....	18
2.5 PCF (PLANT COMPUTER FUNCTIONS) OVERVIEW .....	20
2.6 CONFORMANCE TO THE NUREG/CR-6303 ECHELON OF DEFENSE STRUCTURE AND TO THE NUREG/CR-6303 BLOCK STRUCTURE .....	20
<b>3 DEFENSE-IN-DEPTH FEATURES OF THE ESBWR INSTRUMENTATION AND CONTROL ARCHITECTURE.....</b>	<b>24</b>
3.1 INTRODUCTION .....	24
3.2 DEFINITION OF COMMON-MODE FAILURES .....	24
3.3 OVERALL INSTRUMENTATION AND CONTROL FAULT TOLERANT DESIGN FEATURES.....	25
<b>4 EVALUATION OF NUREG/CR-6303 GUIDELINES .....</b>	<b>29</b>
4.1 IDENTIFYING SYSTEM BLOCKS - GUIDELINES 1 AND 5.....	29
4.2 DETERMINING DIVERSITY- GUIDELINE 2.....	29

4.3	SYSTEM FAILURE TYPES - GUIDELINE 3 .....	31
4.3.1	Type 1 Failure .....	31
4.3.2	Type 2 Failure .....	31
4.3.3	Type 3 Failure .....	31
4.4	ECHELONS OF DEFENSE - GUIDELINE 4 .....	32
4.5	POSTULATED COMMON-MODE FAILURE OF BLOCKS – GUIDELINE 6 .....	32
4.6	USE OF IDENTICAL HARDWARE AND SOFTWARE MODULES – GUIDELINE 7 .....	32
4.7	EFFECT OF OTHER BLOCKS - GUIDELINE 8 .....	33
4.8	OUTPUT SIGNALS - GUIDELINE 9 .....	33
4.9	DIVERSITY FOR ANTICIPATED OPERATIONAL OCCURRENCES AND ACCIDENTS - GUIDELINES 10 AND 11 .....	33
4.10	DIVERSITY AMONG ECHELONS OF DEFENSE - GUIDELINE 12 .....	33
4.10.1	Control/Reactor Trip .....	33
4.10.2	Control/Engineered Safety-Related Features (ESF) .....	34
4.10.3	Reactor Trip/ESFAS .....	34
4.11	PLANT MONITORING - GUIDELINE 13 .....	34
4.12	MANUAL OPERATOR ACTION – GUIDELINE 14 .....	35
<b>5</b>	<b>EVALUATION OF DIVERSITY WITHIN THE ESBWR INSTRUMENTATION AND CONTROL ARCHITECTURE.....</b>	<b>36</b>
5.1	INTRODUCTION.....	36
5.2	DIVERSITY OVERVIEW OF THE ESBWR INSTRUMENTATION AND CONTROL ARCHITECTURE.....	36
5.3	REACTOR SHUTDOWN .....	38
5.4	REACTOR COOLANT SYSTEM INVENTORY CONTROL.....	40
5.5	CORE DECAY HEAT REMOVAL.....	41
5.6	CONTAINMENT COOLING .....	42
5.7	CONTAINMENT ISOLATION.....	43
5.8	EVENT SCENARIOS .....	43
5.8.1	MSIV closure .....	44
5.8.2	Loss of Condenser Vacuum .....	44
5.8.3	Loss of Feedwater Heating .....	44
5.8.4	Loss of Normal AC Power to Station Auxiliaries .....	44
5.8.5	Loss of Feedwater Flow .....	45
5.8.6	Generator Load Rejection with a Single Failure in the Turbine Bypass System .....	45
5.8.7	Inadvertent Isolation Condenser Initiation.....	46

5.8.8	Turbine Trip with Full Bypass.....	46
5.8.9	Opening of One Control or Turbine Bypass Valve .....	46
<b>6</b>	<b>REFERENCES.....</b>	<b>48</b>
	<b>APPENDIX A - ESBWR Instrumentation &amp;Control Defense-in-Depth and Diversity (D3) Evaluation of Chapter 15 Events Assuming Common Mode Failure of a Digital Protection System .....</b>	<b>49</b>
	<b>APPENDIX B – Summary Table of DCD Chapter 15 Accidents Evaluated for D3 .....</b>	<b>68</b>

## List of Tables

<b>Table 1 ESBWR Instrumentation and Control Echelons of Defense.....</b>	<b>22</b>
<b>Table 2 Assignment of Instrumentation and Control Equipment to Defense-in-Depth Echelons .....</b>	<b>23</b>

## List of Figures

<b>Figure 1 ESBWR DCIS Architecture .....</b>	<b>6</b>
<b>Figure 2 Hardware/Software (Platform) Diversity.....</b>	<b>10</b>
<b>Figure 3 ESBWR Sensors and Power Diversity.....</b>	<b>11</b>
<b>Figure 4 Control Room Main Bench Boards.....</b>	<b>12</b>
<b>Figure 5 ESBWR DCIS and POWER Separation .....</b>	<b>12</b>
<b>Figure 5 ESBWR DCIS and POWER Separation .....</b>	<b>13</b>
<b>Figure 6 RPS, ESF/ECCS and DPS.....</b>	<b>16</b>
<b>Figure 7 NE-DCIS Control Systems.....</b>	<b>37</b>
<b>Figure 8 RPS Function of E-DCIS .....</b>	<b>39</b>

## LIST OF 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
AOO	Anticipated Operational Occurrence
APRM	Average Power Range Monitor
ARI	Automatic Rod Insertion
ASME	American Society of Mechanical Engineers
ATLM	Automatic Thermal Limit Monitor
ATWS	Anticipated Transients without SCRAM
BOP	Balance of Plant
BTP	Branch Technical Position
BWR	Boiling Water Reactor
CB	Control Building
CCF	Common Cause Failure
CMF	Common-Mode Failure
COL	Combined Operating License
CRD	Control Rod Drive
DAS	Data Acquisition System
DATALINK	A communication path between two systems – almost always fiber-optic.
DC	Direct Current
DCD	Design Control Document
DCIS	Distributed Control and Information System
DPS	Diverse Protection System
DPV	Depressurization Valve
DS	Deluge System
ECCS	Emergency Core Cooling System
E-DCIS	Essential Distributed Control and Information System
EQV	Equalizing Valve
EMI/RFI	Electromagnetic Interference/Radio Frequency Interference
EPA	Electric Protection Assembly
ESF	Engineered Safety Features
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
FWC	Feedwater Control System
GATEWAY	A device representing a “translator” between two datalinked

	systems.
GDC	General Design Criterion
GDCS	Gravity Driven Cooling System
GDS	Gated Diode Switch
HCU	Hydraulic Control Unit
HFE	Human Factors Engineering
HMI	Human Machine Interface
HP	High Pressure
HSI	Human-System Interface
HVAC	Heating, Ventilation and Air Conditioning
I&C	Instrumentation & Control
IC	Isolation Condenser
ICS	Isolation Condenser System
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	Low Power Range Monitor
MCC	Main Control Console
MRBM	Multi-Channel Rod Block Monitor
MSIV	Main Steam Isolation Valve
NE-DCIS	Non-Essential Distributed Control and Information System
NI	Nuclear Island
NMS	Neutron Monitoring System
NRC	Nuclear Regulatory Commission
NUMAC	Nuclear Management and Control
PAS	Plant Automation System
PCCS	Passive Containment Cooling System
PCF	Plant Computer Function(s) (Sub-system of NE-DCIS)
PIP	Plant Investment Protection
PLC	Programmable Logic Controller
PRA	Probabilistic Risk Assessment
PRHR	Passive Residual Heat Removal
PSWS	Plant Service Water System
RB	Reactor Building
RBM	Rod Block Monitor
RC&IS	Rod Control and Information System
RCCW	Reactor Closed Cooling Water System
RCS	Reactor Coolant System
RG	Regulatory Guide
RPS	Reactor Protection System
RTIF	Reactor Trip and Isolation System
RMU	Remote Multiplexing Unit
RWCU/SDC	Reactor Water Cleanup System/Shutdown Cooling System

RWM	Rod Worth Minimizer
SB&PC	Steam Bypass and Pressure Control
SBWR	Simplified Boiling Water Reactor
SCRRI	Selected Control Rod Run-In
SLCS	Standby Liquid Control System
SPDF	Safety Parameter Display Functions (Sub-system of NE-DCIS)
SRNM	Source Range Neutron Monitor
SRV	Safety-Relief Valve
SSC	Shift Supervisor's Console
SSLC	Safety System Logic and Control
TBV	Turbine Bypass Valves
TCCW	Turbine Component Cooling Water
TGCS	Turbine Generator Control System
TMI	Three Mile Island
TMR	Triple Modular Redundant
VDU	Visual Display Unit (touch screen display)
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 1). These definitions are provided to aid in understanding of the report text, instrumentation and control architecture, and conformance to guidelines. The definitions and clarifications may vary from corresponding definitions in NUREG/CR-6303 because of development and evolution of the ESBWR instrumentation and control architecture. *Definitions as stated in NUREG/CR-6303 are in italics.*

### 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)*

Section 15 of the ESBWR DCD (Reference 3), 'Classification of Plant Conditions,' 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 significant amount of radioactive material." (Standard Format, Section 15, "Accident Analysis," USNRC Reg. Guide 1.70)*

Section 15 of the ESBWR DCD (Reference 3). "Classification of Plant Conditions," 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"*

### Echelons of Defense

NUREG/CR-6303 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 instrumentation and control systems that accomplish the task.

#### 1. Control System (NE-DCIS)

*"The control echelon is that non-Class 1E 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 equipment to satisfy the ATWS rule (10 CFR 50.62) or the requirement for a remote shutdown panel. Examples of such equipment include high-quality non-Class 1E equipment for which credit may be taken solely for compensating rare common-mode failures of Class 1E reactor protection equipment..."*

The functions performed by the control system echelon of defense are included in the nonsafety-related control systems (NE-DCIS). These systems normally function to maintain the plant within operating limits to avoid the need for a reactor trip or Engineered Safety Features (ESF) actuation.

#### 2. Reactor Trip or SCRAM System (RPS SSLC)

*"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 control systems (E-DCIS); specifically the RPS SSLC. As will be later described, the nonsafety-related diverse protection system (DPS) also provides automatic and manual reactor trip capabilities.

3. ESF Actuation System (ECCS and (non-MSIV) LD&IS SSLC):

*"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 automatic ESF actuation functions performed by the ESF/ECCS SSLC echelon of defense are included in the safety-related distributed control and information systems (E-DCIS). The nonsafety-related DPS also provides automatic actuation capability for a subset of ECCS component actuations. ESBWR is a passive plant and does not require emergency generators, motors, or pumps to perform the ECCS functions.

4. Monitoring and Indicator System (NE-DCIS, E-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 Class 1E and non-Class 1E manual controls, monitors, and indicators required to operate nominally assigned to the other three echelons."*

Monitoring and indication functions are provided by both the nonsafety-related and safety-related distributed control and information systems (NE-DCIS and E-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 safety-related distributed control and information system. The nonsafety-related DPS also provides manual reactor trip and a subset of manual ESF actuation capabilities.

### 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 instrumentation and control architecture:

- Nonsafety-related distributed control and information systems including:
  - Plant Investment Protection A
  - Plant Investment Protection B
  - Diverse Protection System
  - Severe Accident (deluge) Control System
  - Balance of Plant Control
  - Plant Computer Functions (Sub-system of NE-DCIS)
  
- Safety-related distributed control and information systems including:
  - RTIF (includes Reactor Protection System and MSIV Leak Detection and Isolation System)
  - ATWS/SLCS (also includes some nonsafety-related functions)
  - ESF [includes ECCS (Isolation Condensers, Automatic Depressurization System, Gravity-Driven Cooling System and Standby Liquid Control System) and Non-MSIV Leak Detection and Isolation System.]

# 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 instrumentation systems with a slow but continuous introduction of retrofit safety-related and nonsafety-related digital control systems into operating nuclear 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 ALWR Utility Requirements Document. A good starting point for Distributed Control and Information System (DCIS) reliability and safety-related system challenges as 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 ABWR DCIS in Japan and, most recently Taiwan (where U.S. standards were closely followed) has been incorporated into the Economically Simplified Boiling Water Reactor (ESBWR) DCIS systems.

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

- Probabilistic Risk Assessment (PRA) methods were used to consider the role of both safety-related and nonsafety-related equipment in the prevention and mitigation of transients and faults. For the ESBWR 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 a reactor trip and Engineered Safety Features (ESF) actuations diverse from the Essential Distributed Control and Information System (E-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 NUREG/CR-6303 (Reference 1), which described a deterministic method of analyzing computer-based nuclear reactor protection systems that identifies and evaluates design vulnerabilities to CMF. The ESBWR instrumentation and control system functions follow the SBWR instrumentation and control systems and the ABWR hardware and software applications, which were designed and analyzed before NUREG/CR-6303 was published. As with the SBWR design, PRA methods were used for the analysis of systems used to provide diversity and defense-in-depth for ESBWR, rather than the

deterministic methods described in NuREG/CR-6303. These PRA methods are consistent with NUREG/CR-6303 and allow the designers to concentrate on situations that are the largest contributors to the predicted core melt frequency.

## **1.2 ARCHITECTURE OVERVIEW**

The E-DCIS is a Class 1E instrumentation and control 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) (Reference 3). The E-DCIS is designed to comply with NEDO-33230 – Software Safety Plan (Reference 4) and specifically to meet plant-licensing requirements by including design features such as:

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

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

The ESBWR DPS is a nonsafety-related instrumentation and control system whose functions are in addition to the Anticipated Transients without SCRAM/Standby Liquid Control System (ATWS/SLCS) system included in the ESBWR and the ABWR. The DPS is included to enable the ESBWR distributed control and information systems to meet reliability goals in the ESBWR PRA, where the E-DCIS is assumed to fail as a result of postulated failures beyond design basis, such as CMF.

## **1.3 SCOPE**

Diversity is a principle in instrumentation of sensing different variables, using different technology, using different logic or algorithms, or using different actuation means to provide different ways of responding to postulated plant conditions. NUREG/CR-6303 segregates the types of diversity into six different areas:

- Human
- Design
- Software
- Functional
- Signal
- Equipment

NUREG/CR-6303 defines echelons of defense as:

*“...specific applications of the principle of defense-in-depth to the arrangement of instrumentation and control 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 of the ESBWR Instrumentation and Control Defense-in-Depth and Diversity Report describe the type of diversity that exists among the four echelons of defense for ESBWR and identify dependencies among the echelons. Also discussed will be redundancy and segregation.

## **1.4 SUMMARY AND CONCLUSIONS**

### **1.4.1 Complies with NUREG-0493**

The ESBWR instrumentation and control architecture meets the expectations of NUREG-0493, in particular, Section 2, “Technical Discussion:” and Section 3.3 “Guidelines,” which contain guidelines, requirements, and recommendations.

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

The ESBWR instrumentation and control architecture complies with NUREG/CR-6303, in particular, Section 3 “Guidelines,” which contains guidelines, requirements, and recommendations.

### **1.4.3 Meets Probabilistic Safety-Related Goals**

The analysis to protect against CMF in the ESBWR was interactive with the development of the ESBWR PRA. In the PRA, failures of the instrumentation and control architecture, including common cause failures, will be analyzed. The ESBWR PRA report (Reference 10) will describe these analyses of the ESBWR instrumentation and control systems. The conclusion is that the ESBWR instrumentation and control 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 instrumentation and control systems and functions of the ESBWR have been structured into the architecture shown in Figure 1; this figure is a very simplified representation of the ESBWR instrumentation and control architecture that illustrates the interactions between its various safety-related and nonsafety-related components. It should be understood that divisional E-DCIS cabinets are located in one of the four dedicated DCIS rooms appropriate to their division. The non-safety Non-Essential Distributed Control and Information System (NE-DCIS) cabinets and components are located in one of two non-safety DCIS rooms.

All communication between safety-related and nonsafety-related DCIS is through fiber optics and one-way [the only exception is Average Power Range Monitor/Low Power Range Monitor (APRM/LPRM) calibration which can only be done by making the affected instrument inoperable (INOP)]. All communication between divisions (to perform 2/4 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.

Almost all communication to/from the field Remote Multiplexing Units (RMUs) is fiber and almost all communication from the DCIS rooms to the control room safety-related and nonsafety-related displays are via fiber optics. The few hard-wired exceptions are for signals like main turbine trip or reactor SCRAM. These control room considerations are important because the communications protocol is such that a melting or otherwise compromised fiber will not cause erroneous operation nor affect the continued operation of all automatic safety-related or non-safety systems. This is also supported by the fact that touch screen operation of the Video Display Units (VDUs) deliberately 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.

Very broadly the major functional groupings of the DCIS include:

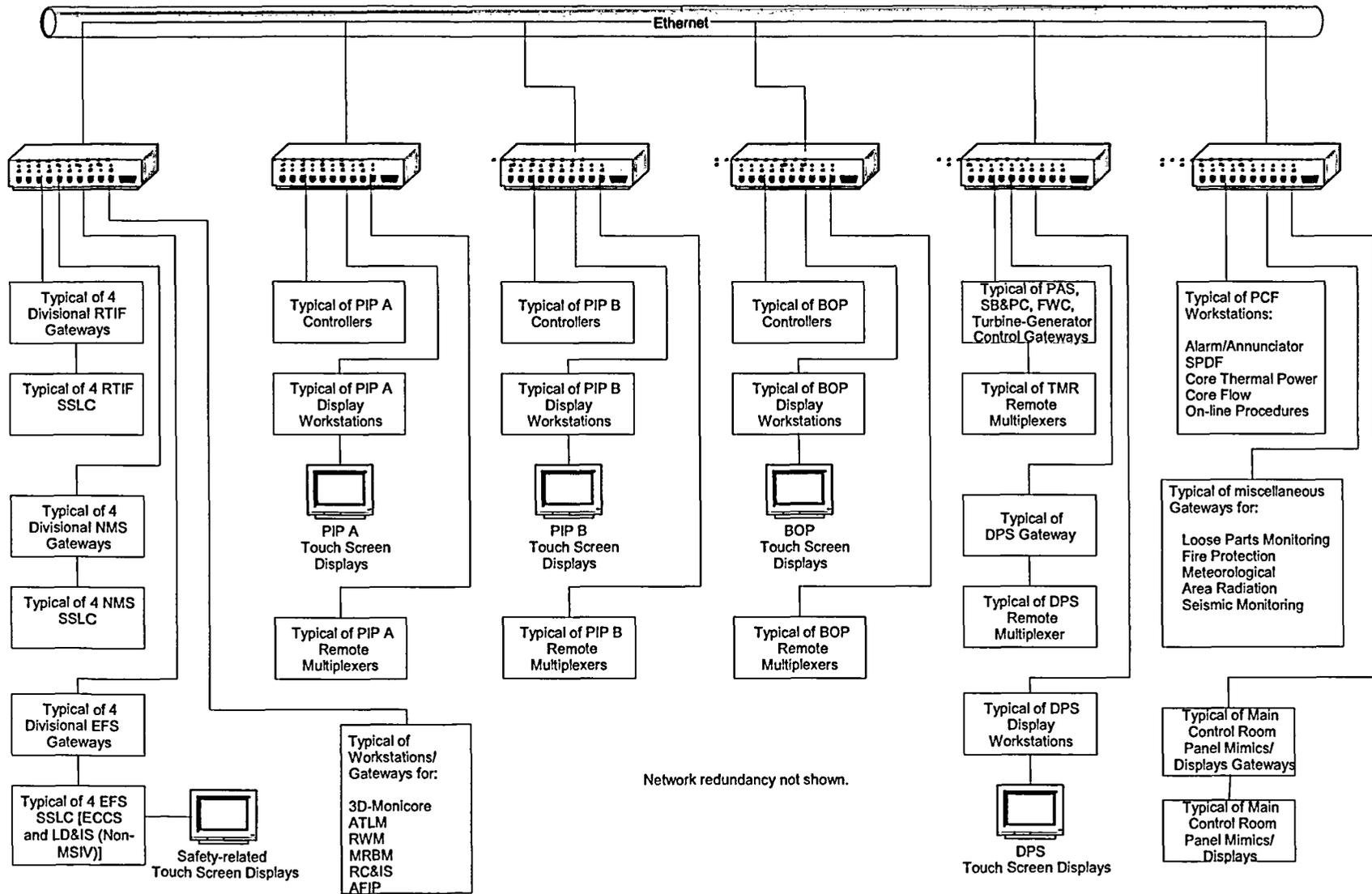
- Nuclear Management and Control (NUMAC) derived functions (four divisions)
  - [Reactor Protection System (RPS), MSIV Leak Detection and Isolation System (LD&IS) , Neutron Monitoring System (NMS)]
  - (Non-microprocessor based ATWS/SLCS)
- ESF/Emergency Core Cooling System (ECCS) functions (four divisions)
  - [Isolation Condenser System (ICS), Safety Relief Valve (SRV), Depressurization Valve (DPV), Gravity-Driven Cooling System (GDCS) and Standby Liquid Control System), isolation function performed by the LD&IS (non-MSIV)]
- Nuclear functions [3D-Monitore, ATLM, RBM, Rod Worth Minimizer (RWM), AFIP, Rod Control and Information System (RC&IS)]
- Plant Investment Protection (PIP) A functions
- PIP B functions

Balance of Plant (BOP) functions

Process Computer Functions [Safety Parameter Display Functions (SPDF), Alarms,  
Historian, etc.]

Severe Accident (two train) (Deluge System which is a GDCS subsystem)

Figure 1 ESBWR DCIS Architecture



The DCIS hardware and software architecture is compliant with NEDO-33226 – Software Management Plan (Reference 8), NEDO-33229 – Software Development Plan (Reference 7) and NEDO-33227 – Software Configuration Management Plan (Reference 5). The configuration supports:

- Controlling and monitoring of the safety-related systems on the safety-related displays whatever the status of the NE-DCIS
- The display and alarming of safety-related systems on the NE-DCIS (through isolated data links from the four divisions (control of E-DCIS from NE-DCIS is not possible “backwards” through the data links)
- Dual and triple redundancy for all important plant computer functions and for control of power generation systems
- Segmented PIP systems

The ESBWR distributed control and information systems use all the methodologies described by the various regulations to maximize control system reliability and safety; these include redundancy, diversity, segmentation and isolation. Diversity is indicated for the various control systems:

- Safety-related distributed control and information systems including:
  - Reactor Trip and Isolation System (RTIF) [includes Reactor Protection System and Main Steam Isolation Valve (MSIV) LD&IS]
  - NMS [including APRMs, LPRMs and Source Range Neutron Monitor (SRNMs)]
  - ATWS/SLCS (also includes some nonsafety-related functions)
  - ESF/ECCS (includes Isolation Condenser System, Automatic Depressurization System, Gravity-Driven Cooling System, SLCS and Non MSIV Leak Detection and Isolation System).
- Nonsafety-related distributed control and information systems including:
  - PIP A
  - PIP B
  - DPS
  - Severe Accident (deluge) Control System
  - BOP Control
  - Plant Computer Functions (Subsystem of NE-DCIS)

As indicated in Figure 2, within the E-DCIS, the RPS, LD&IS (MSIV) and NMS use different hardware and software than the ECCS processors. In turn both the RPS and ECCS DCIS systems use different hardware and software than the NE-DCIS systems, specifically including the DPS, which represents a completely diverse backup design to most protection functions in the E-DCIS. The severe accident deluge system is also diverse from both E-DCIS and NE-DCIS.

On the NE-DCIS side, the important nuclear instrumentation and control systems, like DPS, are triplicated 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.

Figure 3 indicates power and sensor relationships between the various diverse instrumentation and control systems.

The control schemes assigned to the specific DCIS cabinets represented by this architecture 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 is in a different cabinet than reactor level control (this will be discussed below). These cabinets/systems are connected into systems by means of hardwired conductors, data links/gateways, and data highways (real time networks).

The instrumentation and control architecture is arranged in a hierarchical manner. "Above" the real time data network are the plant computer functions whose purpose is to provide and facilitate the interaction between the plant operators and the DCIS; these specifically include the plant alarm system, the operator displays and the SPDF. "Below" the real time data network are those systems itemized above that perform the protective, control and monitoring functions of the ESBWR.

The operator interface functions, of the DCIS, define the arrangement of the main control room, the layout of the DCIS equipment on the main bench boards (and remote shutdown panels) and contains the design process for the layout and content of operating and safety-related displays, alarms, controls, and procedures for the Human System Interface (HSI). The HSI functions, developed under the formal Human Factors Engineering (HFE) plans, are covered in the appropriate instrumentation and control system sections of the DCD.

Figure 4 is a functional representation of the main control room panels. There are three main control room panels – the wide display panel that is mainly nonsafety-related except for four compartmentalized sections on the left side housing four VDUs (one per division) and generally used for (but not dedicated to) surveillance testing and calibration. Other than the safety-related VDUs, the wide display panel (WDP) houses the plant mimic, large variable display, various nonsafety-related VDUs, synchronizing equipment for the main and diesel generators and fire protection. The WDP also houses the plant annunciators, generally one per systems, which are part of the advanced alarm system.

The main control console is the primary operator interface and also houses compartmentalized (one per division) sections on the left side housing VDUs and various manual switches for ECCS equipment and ECCS/RPS bypass and initiation. The remainder of the main control console houses the non-safety VDUs and a few hard controls [for example, main turbine trip, control rod insert/withdraw (in manual mode)] that are used for normal plant operation. Although the nonsafety-related displays are segmented in that they are driven by the PIP A, PIP B and BOP portions of the nonsafety-related DCIS, in normal operation they appear "seamless" to the operator and all displays can control and monitor all nonsafety-related equipment as 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 fiber).

Both the Wide Display Panel (WDP) and Main Control Console (MCC) have four divisional VDUs from which safety-related systems can be both monitored and controlled. The safety-related VDUs, although still using touch screen technology and having the same operator “look and feel”, are diverse technology than the nonsafety-related VDUs. The safety-related VDUs are completely isolated from the nonsafety-related DCIS.

The third bench board is the Shift Supervisor console that contains the nonsafety-related VDUs from which the supervisor can monitor safety-related and nonsafety-related systems. All of the nonsafety-related displays are part of the plant computer function (sub-system nonsafety-related DCIS) and are implemented using a distributed architecture. The safety-related displays are electrically and logically isolated from the nonsafety-related DCIS. The distributed computer subsystem obtains input from the real-time data network and delivers output over the network to other users and to the nonsafety-related displays.

The bench boards also contain the various hard control and bypass switches that also contribute to ESBWR diversity. The plant can be manually scrammed and (MSIV) isolated from MCC switches that are independent of software; similarly the main turbine and reactor feedwater pumps can be tripped without software.

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 various ESBWR raceways, conduits and duct banks fully support the divisional and non-divisional separation criteria. Note that 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. Finally the signals representing the Hydraulic Control Unit (HCU) 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.

The raceway drawing also indicates other safety-related and non-safety signal, fiber and power separation. An example safety-related separation is the ECCS separation into the four divisions whose fibers and wires are in four separated raceways/conduits. An example of nonsafety-related separation are the plant investment protection DCIS “A” and “B” whose dual redundant fibers are in separate raceways/conduits.

Figure 2 Hardware/Software (Platform) Diversity

Safety Category	Safety-Related		Nonsafety-Related				
	EEDGIS		NE - DCIS				
System Families	RPS NMS	ECCS ESF	DPS	NUCLEAR CONTROL SYSTEMS	Balance of any NE-DCIS Systems	PCF	Severe Accident
Architecture	NUMAC Derived	Redundant	Triple Redundant	Triple Redundant	Dual Redundant	Workstations **	PLCs
Systems/ Subsystems	RPS LD&IS (MSIV) NMS ATWS/SLCS*	ICS SRV/DPV GDCS SLCS LD&IS (Non-MSIV)	RPS ECCS Backup	FWC, PAS (Automation SB&PC, T/G Control)	PIP A, PIP B Balance Of Plant (Power Generation)	HMI, Alarms, SPDF, Historian, 3D- Monicore	Deluge System (GDCS Subsystem)

\* Non -Microprocessor based

\*\* Dual redundant as necessary

**Diversity Strategy**

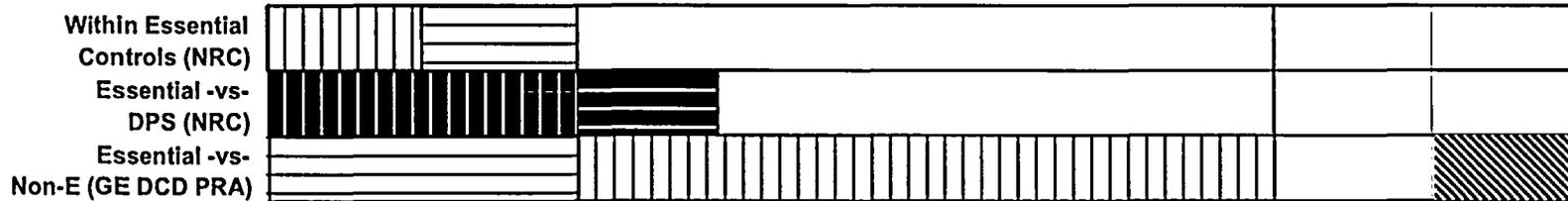
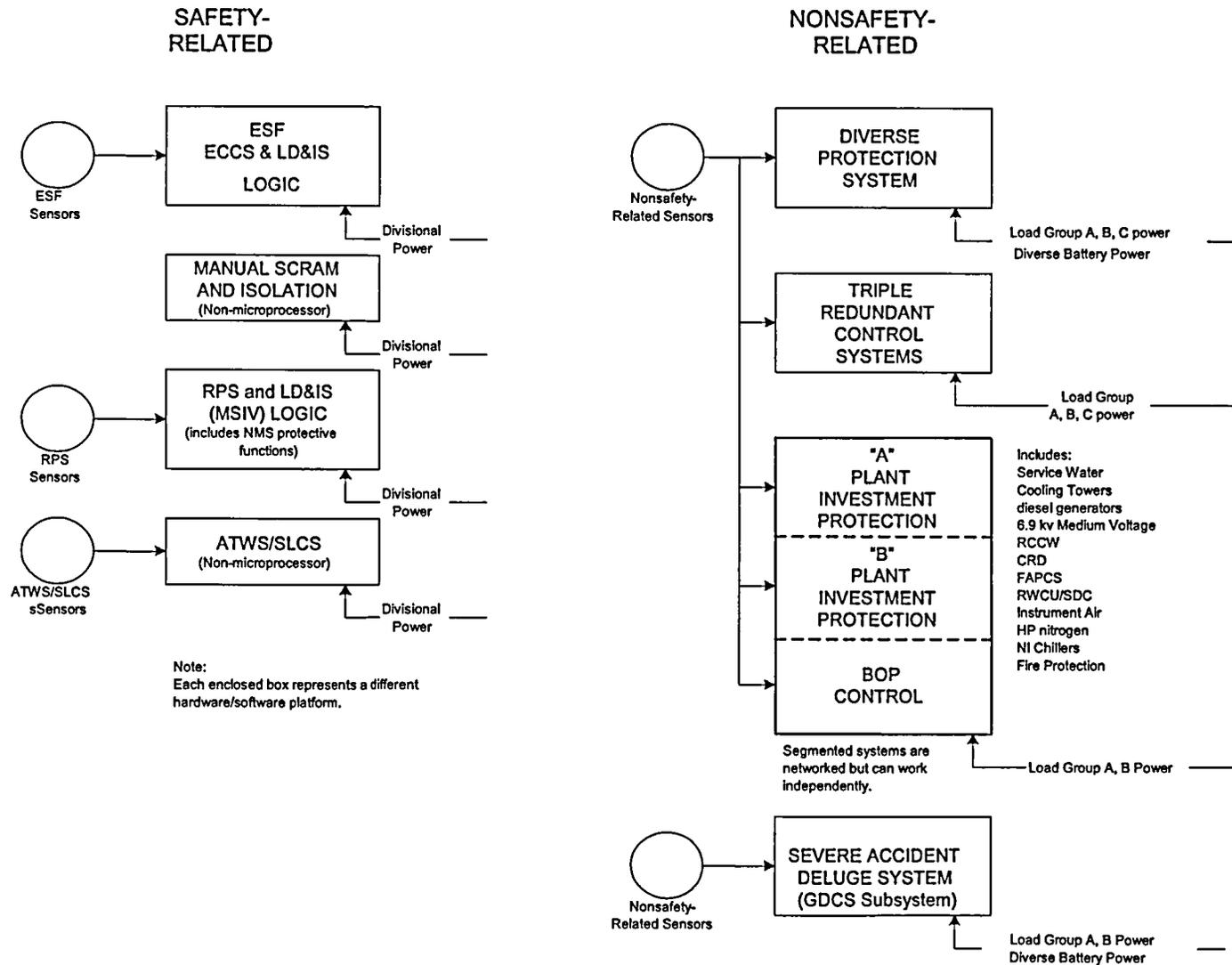
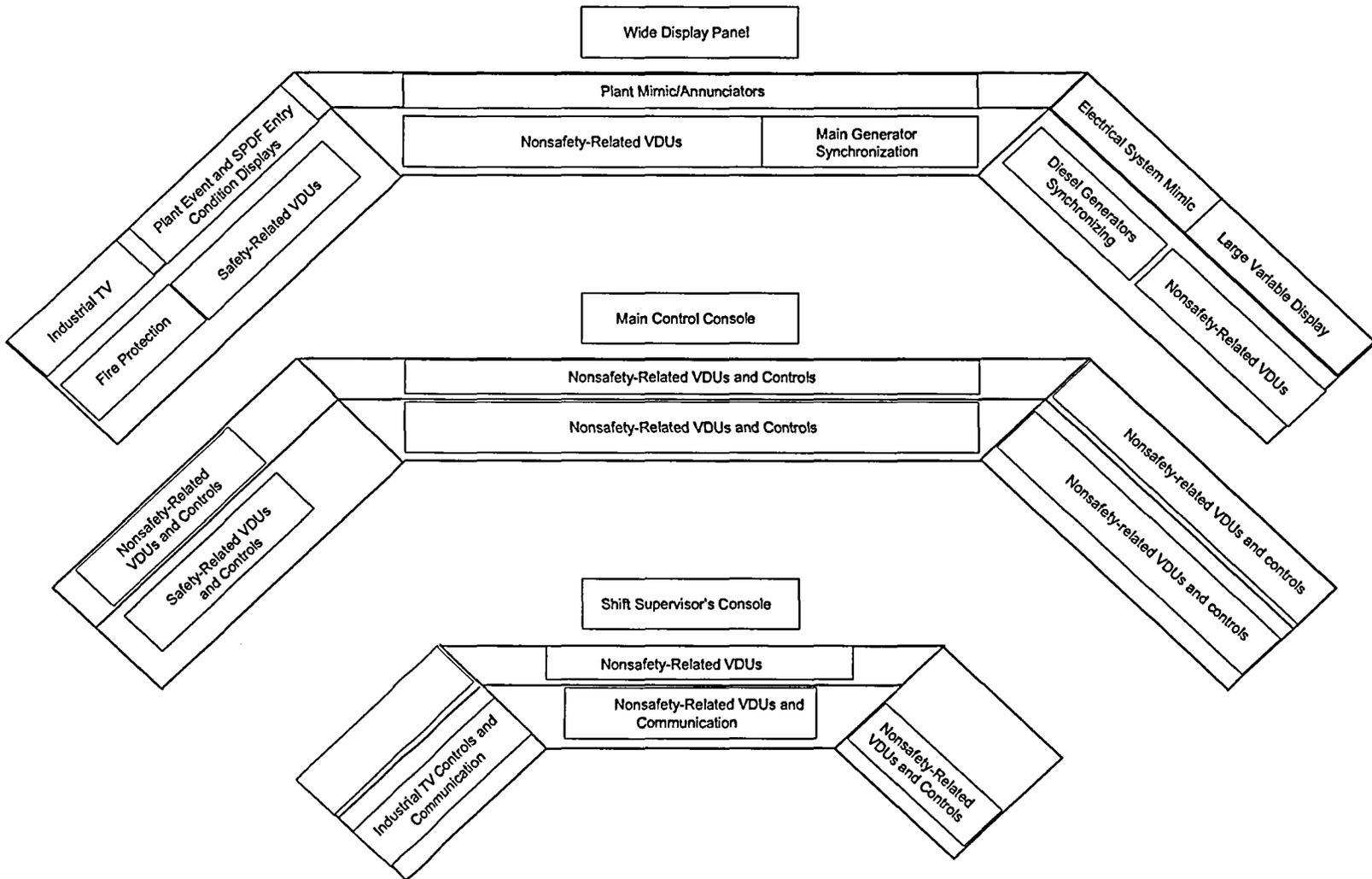


Figure 3 ESBWR Sensors and Power Diversity



**Figure 4 Control Room Main Bench Boards\*  
(\*Contingent upon final HFE Analysis)**

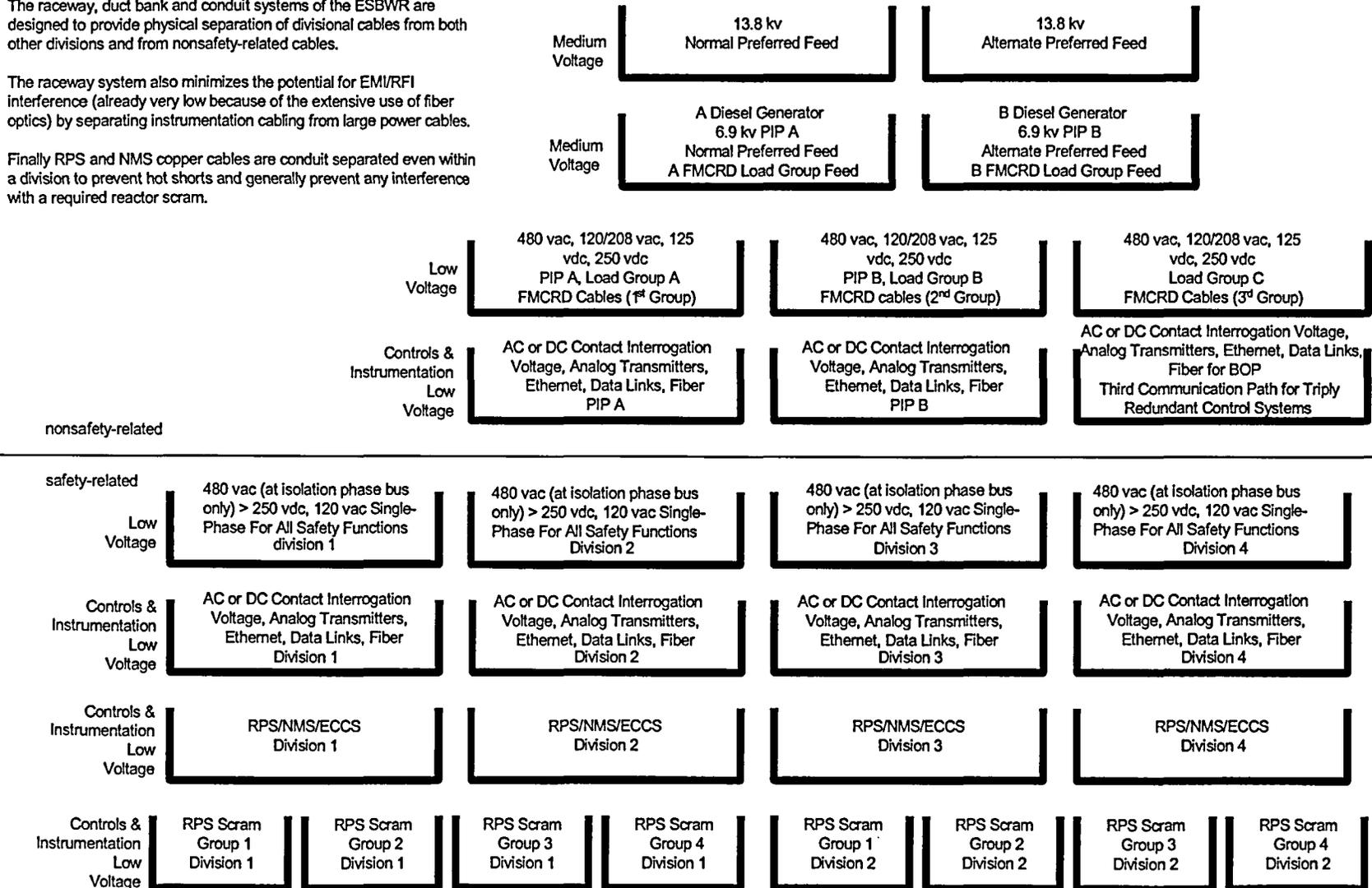


**Figure 5 ESBWR DCIS and POWER Separation**

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 within a division to prevent hot shorts and generally prevent any interference with a required reactor scram.



## 2.2 SAFETY SYSTEM DISTRIBUTED CONTROL AND INSTRUMENTATION SYSTEM OVERVIEW

As previously described the E-DCIS consists of the RPS (including MSIV isolation), the NMS and the ECCS. These systems and their associated sensors are organized into four divisions; the touch screen displays associated with each division provide for the control of the safety-related 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.

The RPS is a hardware/software sub function of Safety System Logic and Control (SSLC), which is, in turn a sub function of the E-DCIS; the general relationship is shown in Figure 6. The RPS controllers/logic are located in a cabinet (one per division in separate E-DCIS rooms) that combines the RPS, LD&IS (for MSIVs and drains only) and ATWS/SLCS functions; the cabinet is called the RTIF cabinet. Although all equipment located in the RTIF cabinet is appropriate to the division and everything in the cabinet is powered by the appropriate divisional R13 (uninterruptible) and R14 (I&C power) and R16 power (battery), the ATWS/SLCS function is segregated to a separate chassis and does not use programmable logic. All of the RTIF functions are implemented in safety-related hardware/software platforms diverse from the DPS.

The ESBWR RPS design has several important differences from most existing 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.

All communication with nonsafety-related DCIS is one-way (E-DCIS to NE-DCIS) through fiber optics; the loss of this communication will not affect RPS functionality.

All communication with other RPS divisions is one-way, fiber isolated, and does not mix divisional data.

Since all signals are actively transported, “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 (unless that division is bypassed) and loss of communication with a bypass joystick switch is interpreted as “no bypass”.

All RPS logic is powered by R16 battery (divisions 1 and 2) to R13 (uninterruptible AC 120V) and redundantly backed by R14 (regulated AC supplied by Normal, Alternate or diesel backup/non-safety).

The HCU solenoid power is local to the reactor building and switched by fiber driven 2/4 logic from the RPS (RTIF) cabinet in the control building. 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 (EPAs). Loss of communication from the control building RTIF cabinets is interpreted as a trip.

The hardware, software and solenoid switching for the RPS is both diverse and separate from the DPS (diverse protection system).

The ESF/ECCS DCIS is also, like RPS, a hardware/software sub function of safety-related SSLC that is, in turn, a sub function of the E-DCIS; for diversity the ECCS and non-MSIV LD&IS logic use different sensors and is implemented on a different hardware/software platform than RPS/(MSIV) LD&IS and the DPS. Since it is highly desirable to avoid the consequences of inadvertent actuation of ECCS (specifically automatic depressurization) while still important to reliably actuate ECCS when required, the ECCS logic is implemented on a triply redundant hardware/software platform per division. The ESF/ECCS functions are described in more detail in the DCD but include the following systems controlled by the ESF/ECCS DCIS:

Automatic depressurization (SRVs and DPVs) - the safety-related relief valves are actuated by solenoids and the depressurization valves are actuated by explosive squibs). These valves are used to force the reactor to a low enough pressure for the GDCS to work.

GDCS (also Squib Actuated Valves) - These valves allow the water stored in the inside-containment gravity pools to drain into the depressurized vessel.

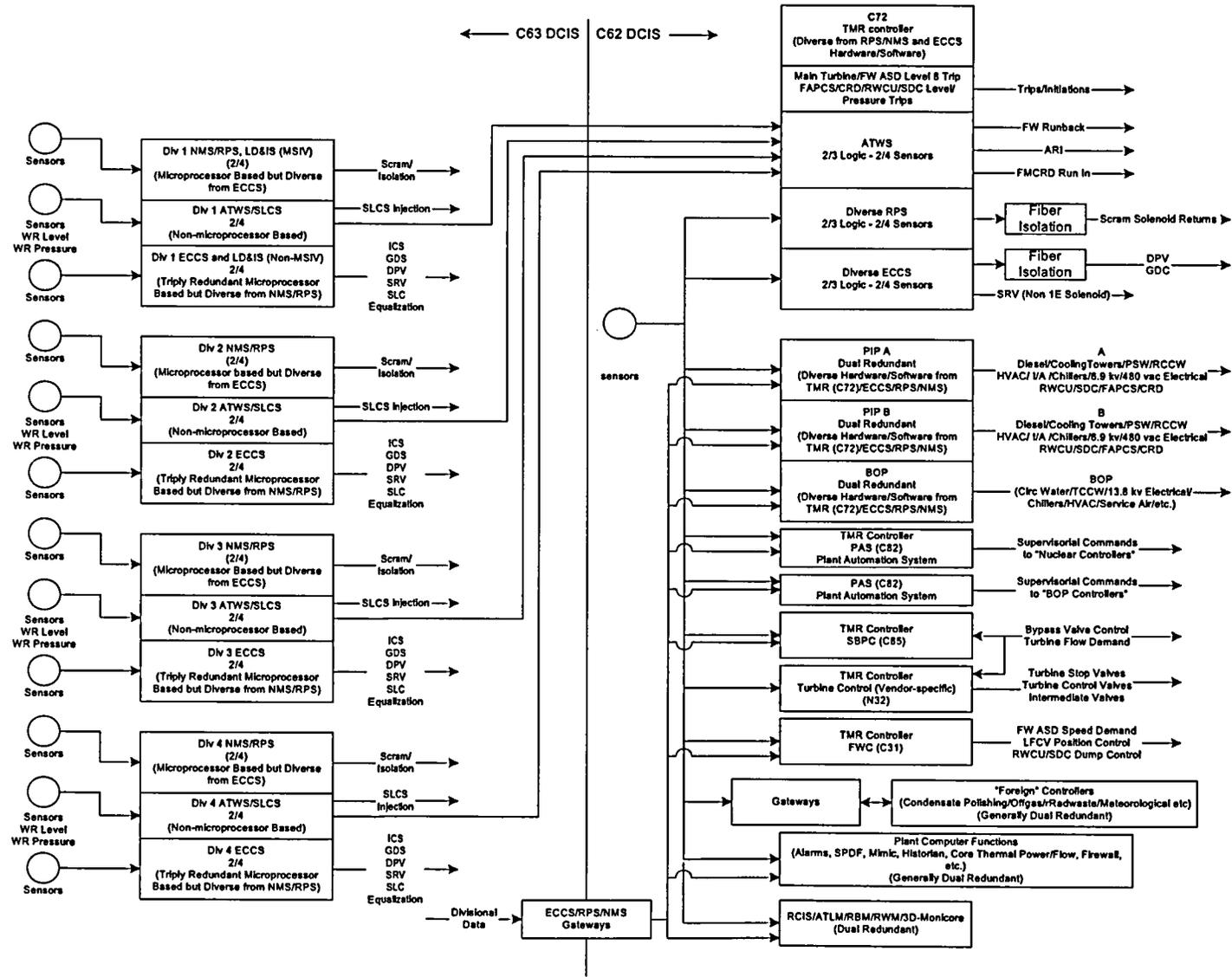
Suppression Pool Subsystem of GDCS (also Squib Actuated Valves) - These equalizing valves allow the water stored in the suppression pool to drain into the depressurized vessel well after a postulated accident event to compensate for long term boil-off.

Standby Liquid Control System (also Squib Actuated Valves) - These valves allow soluble boron to be injected into the vessel from two accumulator tanks for additional coolant inventory.

Isolation Condenser System - 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, will condense reactor steam and return it to the vessel. The system operates at high reactor pressures and provides cooling and depressurization without inventory loss.

Leak Detection and Isolation - The ESF/ECCS processors perform the inboard and outboard isolation function for all isolation valves other than the MSIVs and certain steam line drain valves.

Figure 6 RPS, ESF/ECCS and DPS



The general arrangement of the ESBWR ESF/ECCS DCIS is also shown in Figure 6. There are four divisions of redundant logic; each division has a main chassis located in the control room 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 main control room displays and (one way) connections to the nonsafety-related DCIS. All chassis are redundantly powered by both R13 (uninterruptible) and R14 (regulated but interruptible) power and all four divisions can be powered by either diesel generator through the isolation load centers.

Per division a two-out-of-three (2/3) logic is used to determine whether an ECCS actuation condition exists and then two of four divisions must agree before all four divisions are signaled to operate the final actuators. The squib and solenoid actuators are designed such that any one of the four divisions (after the 2/3 logic and 2/4 logic) can operate the actuator; however the actuator cannot be operated from a single failure within the division.

### **2.3 NON-SAFETY SYSTEM DISTRIBUTED CONTROL AND INSTRUMENTATION SYSTEM OVERVIEW**

As previously described the NE-DCIS contains the DPS and provides for control and monitoring of the plant investment protection systems, the balance of plant (power generation) control systems, the plant computer functions and the severe accident (deluge system) functions. The NE-DCIS plant computer functions also provide the main operator HMI interface. (The DPS is also discussed in the following subsection.)

The NE-DCIS provides the functions necessary for normal operation of the plant from cold shutdown through full power. The NE-DCIS controls nonsafety-related components and systems in the plant that are operated from the main control room or remote shutdown 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 Busses
- Plant Service Water System (PSWS)
- Reactor Closed Cooling Water (RCCW)
- Reactor Building Chillers
- Instrument Air
- Reactor Water Cleanup System/Shutdown Cooling System (RWCU/SDC)
- Fuel and Auxiliary Pools Cooling System (FAPCS)
- Control Rod Drive (CRD)
- PIP A and PIP B DCIS
- Nonsafety-related Battery and Uninterruptible Power
- Drywell Cooling
- Reactor Building (RB), Fuel Building (FB), Control Building (CB), Switchgear Building
- Heating Ventilation and Air Conditioning (HVAC)

Generally the PIP systems are organized mechanically into two trains (i.e., pump “A” and pump “B”) with each train powered by a different diesel and 6.9 KV bus. The two trains are controlled by a deliberately segmented NE-DCIS, for example 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 mainly for power generation and are not generally used for shutting down the plant nor monitoring the more important plant parameters. They specifically include the triply redundant systems used to control the turbine, reactor pressure, reactor level and plant automation and dual redundant systems like 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's defense-in-depth automatic and manual functions.

The plant computer system function of NE-DCIS provide for the plant annunciator and alarm systems, the rod blocks for 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 safety-related parameter display functions; these functions are implemented redundantly. A major function of the plant computer functions of NE-DCIS is to provide information to and receive demands from the nonsafety-related touch screen displays. The NE-DCIS also provides sensors for nonsafety-related plant monitoring functions.

Finally the NE-DCIS supports the severe accident deluge system using hardware, software and sensors diverse from both the safety-related and nonsafety-related DCIS systems. The deluge system uses squib valves to drain GDCS pool water to underneath the vessel should all other core cooling and shutdown systems fail. The valves are actuated by sensed containment floor temperatures attributable to the postulated core and vessel melt.

## **2.4 DIVERSE PROTECTION SYSTEM OVERVIEW**

The diverse protection system is a triply redundant, nonsafety-related, diverse (from RPS/ECCS) system that provides an alternate means of initiating reactor trip and actuating selected engineered safety-related features and providing plant information to the operator; the relationship is shown in Figure 6. The DPS receives signals directly from sensors diverse from the safety-related reactor protection and ECCS. Specifically the DPS uses hardware, software and power that are different (diverse) from the safety-related systems. The DPS is described further in Chapter 7 of the ESBWR DCD.

The DPS system performs several major/minor functions: It will SCRAM the plant using a subset of the safety-related RPS.

- It will initiate selected ECCS.
- It will pass through ATWS/SLCS logic signals to initiate the run in of all the Fine Motion Control Rod Drives (FMCRDs) on their motors and cause the Feedwater Control System to run back feedwater flow and will be diversely able to activate SLCS.
- It will trip the feedwater pumps on high level (after they have been run back to zero flow on level 8).

The DPS will initiate a plant SCRAM on a per parameter 2/4 coincidence of:

- Detection of high or low reactor level
- Detection of high reactor pressure
- Detection of high drywell pressure
- Detection of high suppression pool temperature
- Closure of the MSIVs

Using sensors diverse from those used by the RPS. The DPS causes a SCRAM by interrupting the current in the 120 VAC return power from the HCU solenoids using the same switches used to perform individual control rod SCRAM timing. The 2/3 SCRAM decision of the triply redundant processors is sent via three isolated fiber optics to the SCRAM timing panel where they are 2/3 voted to open all the solenoid return power switches. The operator will also have the ability to initiate a manual DPS SCRAM from either hard switches or the DPS touch screen display.

The DPS will also be able to initiate:

- The isolation condensers on low reactor level
- The SRVs and DPVs on low reactor level
- The GDCS squib valves on low reactor level
- The SLCS squib valves on low reactor level
- The suppression pool equalizing valves on low reactor level

The 2/4-sensor logic and 2/3-processing logic is similar to the SCRAM logic and the operator will also have the ability to initiate the above actions from the DPS touch screen display. The ECCS subsystems that use four divisional solenoids to initiate flow (SRVs and ICs), will also

have a fifth nonsafety-related solenoid to also cause initiation from the DPS (after a 2/3 vote). The ECCS systems, which use squibs, will use redundant fiber isolation between the DPS and the squib logic to fire the squibs; each redundant fiber is operated with 2/3 logic and both are required to actuate the squibs. Although the DPS does not input to all squib divisions, all squib valves are opened by the DPS logic.

The DPS will also provide the following major isolations:

- Closure of the MSIVs on detection of high steam flow, low reactor pressure or low reactor level
- Closure of the IC isolation valves on high steam flow
- Closure of the RWCU/SDC isolation valves on high differential flow using 2/4 sensor logic and 2/3 processing logic.

Note that DPS does not violate the general rule of avoiding nonsafety-related systems communicating with safety-related systems; except where loss of reliability would occur, DPS has its own "actuators" (SRV and IC solenoids or 120 VAC HCU solenoid return switches. Where separate actuators cannot be used, DPS will command safety-related actuators (squibs) "in parallel" with the E-DCIS. The DPS does not interface with the RPS or ECCS logic or processors. For both RPS and ECCS functions, the failure of DPS cannot prevent the E-DCIS from performing its safety-related functions and the communication path from nonsafety-related to safety-related is always by fiber.

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

The nonsafety-related DCIS plant computer functions which are a subsystem of the NE\_DCIS provides the equipment used for processing data that will 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 logging and historical storage and retrieval, and providing operational support for plant personnel. It should be noted that the alarm and annunciator systems are conditioned with both plant operating modes and events to prevent the operator from being presented with alarms and information unnecessary in transient and accident scenarios. Additionally alarm response procedures and operating/emergency procedures are available on line. Finally, although a traditional set of SPDF displays is available on the touch screen monitors, the important SPDF parameters are also permanently available on the mimic on the WDP.

The NE-DCIS also contains the real-time data network, which is a redundant data network that links the elements of the ESBWR instrumentation and control architecture.

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

The ESBWR instrumentation and control architecture conforms to the echelon of defense structure defined in Section 2.2 of NUREG/CR-6303 and the block structure described in Section 2.5 of NUREG/CR-6303. 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 these echelons.

The functions assigned to the instrumentation and control 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 instrumentation and control architecture. The echelons are divided into a nonsafety layer, a safety-related layer, and a diverse layer to reflect the means provided by the systems to implement the functions of each echelon. Table 2 illustrates the relationships between these subsystems and cabinets and the block structure described in NUREG/CR-6303. This table shows the assignment of equipment to the blocks for each level within the echelons of defense.

Due to the nature 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 instrumentation and control architecture. The NE-DCIS provides nonsafety-related operator displays and alarms. Plant data for the nonsafety-related displays and alarms is obtained from across the instrumentation and control architecture by means of the real-time data network. The E-DCIS provides safety-related operator displays. In addition, the DPS provides nonsafety-related, operator indications that are derived from sensors diverse from the E-DCIS sensors.

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

Table 1 ESBWR Instrumentation and Control Echelons of Defense

	<b>LAYER 1 NONSAFETY- RELATED SYSTEMS</b>	<b>LAYER 2 SAFETY- RELATED SYSTEMS</b>	<b>LAYER 3 DIVERSE NONSAFETY- RELATED SYSTEMS</b>
<b>CONTROL ECHELON</b>	NE-DCIS (PIP A, PIP B, BOP)		
<b>REACTOR TRIP ESCHELON</b>		E-DCIS RTIF SSLC (RTIF – RPS, NMS, LD&IS, ATWS/SSLC)	Diverse Protection System (DPS – some RPS, some LD&IS)
<b>ESF ACTUATION ECHELON</b>		E-DCIS ESF SSLC (ECCS – ICS, ADS, GDCCS, Suppression Pool Equalizing, Misc. Isolation)	Diverse Protection System (DPS – ICS, ADS, GDCCS, SLCS, some LD&IS)  Severe Accident (Deluge System (GDCCS subsystem))
<b>MONITORING AND INDICATION ECHELON</b>	NE-DCIS Plant Computer Functions	E-DCIS ESF SSLC	DPS

For monitoring/indication applications, DPS will be able to indicate the appropriate critical safety-related functions needed to operate DPS manually; this information will be available on segmented DPS displays that will work even if PIP or BOP displays are not functional.

Table 2 Assignment of Instrumentation and Control Equipment to Defense-in-Depth Echelons

Echelon	ESBWR Function	Measured and Derived Variable Blocks	Command Block	Manual Actions
Plant Control	Nonsafety-related	Sensors, Signal Conditioning, Network, Isolated NMS Inputs	Network, Output Signal Conditioning, Analog/Discrete Output	Network, Touch Screen Display, Soft Control, Some Hard Control
	Safety-related	N/A	N/A	N/A
	Diverse	Level 9 trip	Level 9 trip	N/A
Reactor Trip	Nonsafety-related	N/A	N/A	N/A
	Safety-related	Sensors, Signal Conditioning, SSLC, ATWS/SLCS Non-Microprocessor Logic	2/4 voting logic, Load Drivers, HCU SCRAM Solenoids, Backup SCRAM Solenoids, SLCS Squib Valves	Hardwired Manual Reactor Trip, HCU SCRAM Solenoids
	Diverse	Sensors, Signal Conditioning, Diverse Processor Platform	2/4 and 2/3 Voting Logic, Load Drivers, HCU SCRAM Solenoids (120 VAC return), FMCRD Run-In, Feedwater Runback	Hardwired DPS Reactor SCRAM Switches, Soft DPS Touch Screen Controls
ESF Actuation	Nonsafety-related	N/A	N/A	N/A
	Safety-related	Sensors, Signal Conditioning, SSLC (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 Logic, some Hardwired Switches
	Diverse	Sensors, Signal Conditioning, Diverse Processor Platform	2/4 and 2/3 Voting Logic, Load Drivers, IC, SRV and Isolation Valve Solenoids, Squib Valves for Automatic Depressurization System (ADS), GDCS and SLCS, and Misc. Isolations	Soft DPS Touch Screen Controls
Monitoring and Indication	Nonsafety-related	Sensors, Signal Conditioning, Network	Network, Mimic, Alarm/Annunciator System, Touch Screen Displays	Touch Screen Displays, some Hardwired Indications
	Safety-related	Sensors, Signal Conditioning, SSLC	Safety-related Touch Screen Displays	Safety-related Touch Screen Displays, some Hardwired Indications
	Diverse	Sensors, Signal Conditioning, Diverse Processor Platform	Network, Touch Screen Displays	Touch Screen Displays

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

#### **3.1 INTRODUCTION**

This section describes features of the instrumentation and control architecture that provide redundant design, fail-safe design, and self-diagnostics/failure detection and repair. Section 5 of this document discusses design diversity.

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

For the purpose of this report, 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 is 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 instrumentation and control architecture such that redundant design is ineffective in enabling the system to tolerate the failure.
- The failures are such that fail-safe design is ineffective in enabling the system to tolerate the failure.
- 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 the failures.
- The failures can occur simultaneously in only related hardware/software platforms.

An instrumentation and control system, or a portion of a system, can be capable of tolerating some combinations of CMFs because:

- Diverse design exists within the system (for example RPS and ATWS/SLCS)
- Redundant design exists within the system (most nonsafety-related control logic, most safety-related logic divisions)
- Fail-safe design exists within the system (RPS and MSIV isolation).
- The failure is detectable and sufficient time exists between instances of failure that automatic or manual response to the failure occurs (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 ECCS logic but not loss of function of the diverse protection

system. A digital protection system CMF of both the RPS or ESF/ECCS logic simultaneously is not assumed due to the diversity between the platforms.

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

The instrumentation and control architecture contains design features which enhance plant reliability and availability. However, these features also provide a degree of protection against CMFs, and, as a result, decrease the probability that a CMF will render any portion of the ESBWR instrumentation and control architecture unable to respond to a transient, accident or plant fault. Among these design features that protect against failures, including CMF are:

- The Design, Verification, and Validation Process - The design of the instrumentation and control system hardware and software components are controlled by a design, verification, and validation process that is described in the DCD and NEDO-33228 – Software Verification and Validation Plan (reference 6). These processes are formal, rigorous means to detect and correct design errors before they can result in common-mode errors in the plant.
- Fail Safe/Fault Tolerant Design - Fail-safe design features in the instrumentation and control architecture, such as de-energizing to trip or actuate or, most important in distributed systems, loss of communications, provide the capability to automatically or manually, put the plant into a safe condition following single failures. Certain types of multiple failures can also be accommodated, for example two divisions of RPS can be lost without losing the ability to SCRAM. Fault tolerant design features such as functional diversity and redundancy, also provide the capability to automatically and manually put the plant into a safe condition.
- Redundancy – While redundant design of itself does not prevent CMFs, use of redundant subsystems can enable the plant to detect and respond to failures, including CMFs in those instances where sufficient time exists between occurrence of the individual failures. For example the four divisions of ECCS SSLC are not time synchronized nor dependent on other divisions for correct operation, this indicates that non-simultaneous (non time related) CMFs can be detected by surveillance testing.
- Modular Design - Modular design enhances the rapid isolation and repair of failures. For instances where failures, including CMFs, occur, but sufficient time between failure instances exists for detection and repair, modular design enables the redundant or diverse subsystems to be available for response to events. The redundant components of the NE-DCIS can be changed on line without affecting plant control and divisional systems can be made inoperable and chassis replaced on line without affecting plant operation.
- Use of Distributed Processing Architecture - Instrumentation and control functions are divided among multiple subsystems so that diverse functions are separated into different subsystems. This, in conjunction with other design features such as divisional isolation and independence, has the effect of localizing certain CMFs to a single subsystem. For instances where functional diversity exists in the instrumentation and control architecture,

complete system failure may not occur as a result of CMF. For example reactor level and pressure control are implemented in different cabinets where each cabinet uses triply redundant processors. It is very unlikely that both functions would be lost simultaneously. The reactor pressure control function is implemented on the safety side by the SRVs and the isolation condensers (ECCS SSLC) and on the non safety side by the triply redundant Steam Bypass and Pressure Control System (SB&PC - NE-DCIS); given the diversity of these systems it is highly unlikely that the reactor pressure control function could be completely or simultaneously lost.

- Alarm System - The ESBWR alarm/annunciator system is capable of alerting the operator to not only process failures, but also DCIS failures including multiple failures, in other parts of the instrumentation and control system. The main ESBWR alarm/annunciator system is part of the plant computer function of NE-DCIS, which uses different hardware and software from the E-DCIS.
- Continuous Self-Diagnostics - In the ESBWR instrumentation and control architecture, the subsystems continuously execute self-diagnostic software routines. Other self-diagnostic features, such as read-backs and watchdog timers continuously monitor operation of critical subsystems. These self-diagnostic features are designed to detect and report hardware failures, enabling the operator to appropriately respond. For example all safety-related DCIS and most nonsafety-related DCIS use redundant power supplies; a detected power supply failure allows replacement before the second power supply fails. An additional example is the adjustable speed drives in the feedwater system that continuously report back to the feedwater control system the received speed demand. When the Feedwater Control System (FWC) determines 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.
- 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 failures detected by the continuous self-diagnostic features.
- Circuit Isolation - Circuit isolation is used to electrically isolate segments of the instrumentation and control architecture and to prevent propagation of electrical faults. This feature helps to limit the propagation of faults caused by failures, including CMFs. For example all interdivisional communication (for 2/4 trip decisions) is via isolated fiber optic cable; similarly all safety-related to nonsafety-related communication is also via fiber optic cable; the fiber communication is monitored to implement both fail safe and self diagnostic schemes. Finally, both the safety-related and nonsafety-related DCIS communicate with their remote multiplexing (data acquisition) units using redundant fiber optic cables to prevent circulating ground currents that could adversely (and commonly) affect all DCIS within one area.
- Control of Setpoint and Tuning Adjustments - The instrumentation and control 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 a system. Another safety-related example is the requirement to make NMS or RPS divisions inoperable before setpoints may be changed; the rendering a division inoperable generates a plant alarm as required by RG 1.47 (Reference 13).

- Use of Engineering Units for Setpoints and Tuning Constants - Setpoints and tuning constants in the instrumentation and control architecture are entered in engineering units rather than as scaled values. This eliminates a potential common-mode error by removing 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 failure (or its power supply) will cause 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 data from all of the other divisions; unless one of the divisions is bypassed, the loss of any two divisions of like sensors will cause an RPS trip. It should be noted that the loss of any single divisional sensor will not prevent 2/4 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 alarmed to the operator. The alarm is intended to cause the operator to repair the failed sensor in a timely manner.
- Physical Separation - Physical separation is provided between the four redundant divisions of equipment for the safety-related DCIS, which in turn, are separated from nonsafety-related systems and the diverse protection system. There are four safety-related DCIS equipment rooms in the control building that provide physical, fire and power separation of the four divisions. Physical separation meets the requirements of IEEE-384 (Reference 9). The PIP A and PIP B nonsafety-related DCIS systems are located in two physically separate nonsafety-related DCIS rooms to provide the same physical, fire and power separation. This physical separation provides protection from CMF induced by physical phenomena.
- Equipment Qualification - Equipment in the instrumentation and control architecture is qualified to environmental requirements, including temperature, humidity, radiation, vibration/seismic, Electro-Magnetic Interference/Radio Frequency Interference (EMI/RFI) 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 will not introduce CMF until design requirements are exceeded.
- Power – The safety-related DCIS components are always powered with two power supplies and two separate power feeds appropriate to the division. The two feeds are either two separate inverters or an inverter and regulated power supply. 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 instrument to both

continue operation and provide alarms should one power supply or power feed be lost. The nonsafety-related 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 control or power generation.

- Other Features - The instrumentation and control 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 will prevent failure from specific causes. Due to these features, the causes that would induce multiple failures must be in excess of design and qualification test limits.

## 4 EVALUATION OF NUREG/CR-6303 GUIDELINES

NUREG/CR-6303 (Reference 1) describes a method for analyzing computer-based reactor protection system vulnerability to postulated software CMFs. NUREG/CR-6303 provides fourteen guidelines for performing a diversity and defense-in-depth analysis. The following sections describe the results of applying these guidelines to the ESBWR.

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 nonsafety-related DCIS uses redundant sensors and redundant subsystems to provide defense-in-depth functions. The nonsafety-related DPS uses redundant sensors and redundant subsystems to provide 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 complete loss of function of the E-DCIS, but not loss of DPS functionality due to the diversity of implementation.

### 4.2 DETERMINING DIVERSITY- GUIDELINE 2

NUREG/CR-6303 identifies six aspects of diversity to address the issue of potential common mode effects and failures:

1. Design Diversity

In the nonsafety-related DPS, energize to trip or actuate logic is used. In the E-DCIS, de-energize to trip or actuate logic is used for the RPS SSLC, and energize to trip logic is used for the ECCS SSLC.

2. Equipment Diversity

For the DPS, the hardware and software used to provide the automatic actions and sensor monitoring will be diverse from the equipment used for safety-related functions in the E-DCIS. For example, the DPS monitors different sensors than RPS and provides a reactor trip by operating the switches in the HCU SCRAM solenoid 120 VAC returns. This means it is diverse from the RPS load drivers used in the RPS SSLC for reactor SCRAM.

3. Functional Diversity

The ESBWR is designed with multiple levels of defense for each anticipated operational occurrence and accident. These multiple levels of defense are described in the DCD (Reference 3). The E-DCIS is a class 1E system with four-way divisional separation. Two-out-of-four voting is used for the reactor trip function and ESF actuation functions. Multiple reactor trip functions and ESF actuations are provided for each anticipated operational occurrence and accident, generally using diverse sensors, as described in DCD Chapter 15. The DPS uses triply redundant processors and 2/4 parameter voting logic to determine a trip condition; two of three processors (and load drivers) must agree to actuate a trip. The functional logic for the automatic E-DCIS functions is shown in Chapter 7 of the DCD.

4. Human Diversity

Human diversity is implemented based on diversity of the organization(s) on the project, project plans, and procedures to meet the expectations of NUREG/CR-6303 (Reference 1) but it should be noted that there will be times when a more experienced, but possibly less diverse individual will be utilized to obtain quality when a diverse individual may not provide the quality although guaranteeing diversity.

5. Signal Diversity

Signal diversity for specific events is provided within the safety-related level of the reactor trip and ESF actuation echelons. The signals used to produce reactor trips and ESF actuations within the DPS originate from different types of (or different vendor) sensors; the DPS receives signals directly from its own sensors that are not used for any safety-related functions.

6. Software Diversity

The DPS contains triply redundant signal processing units that use hardware and software that is different (diverse) from the hardware and software used in the E-DCIS.

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

NUREG/CR- 6303 describes three different instrumentation failure types that are applicable to the ESBWR.

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

Type 1 failures are postulated failures in one echelon that result in a plant transient that require a protection function to mitigate the transient. 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 are also postulated failures in the ESF that necessitate protective action.

Type 1 failures will be analyzed during detailed system design of the DPS.

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 plant control or protection systems and can result in a plant transient and requires protective action. It should also be noted that a substantial defense against these failures is provided by requiring that the ESBWR control system echelon be single failure proof and self diagnosing such that only (postulated) Common Cause Failure (CCF) are really "credible".

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

Type 2 failures are undetected failures that 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. It should also be noted that a substantial defense against these failures is provided by requiring that the ESBWR E-DCIS echelon be redundantly powered and self diagnosing and include features like monitoring for the existence and continuity of the final actuators (squib, SCRAM solenoids) such that only (postulated) CCF are really "credible".

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

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

The primary defense against a Type 3 failure is to provide diverse sensors for measuring the plant response to an initiating event, e.g., using drywell pressure and reactor level for a Loss of Coolant Accident (LOCA) indication or reactor pressure and core inlet temperature for measuring moderator temperature. It should also be noted that a substantial defense against these

failures is provided by requiring (for example) that the ESBWR E-DCIS and NE-DCIS level measurement systems incorporate both reference and variable leg temperature measurements so that indicated level is correct until reference leg boiling occurs – and reference leg boiling is alarmed. (Reference leg boiling may occur as a result of elevated containment temperature and reactor depressurization during postulated loss of coolant events.) Similarly SRV and squib valve positions are measured rather than assuming that an “open” command has resulted in correct behavior.

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

The instrumentation and control architecture is divided into four echelons of defense, as defined in NUREG/CR-6303. The control echelon is provided by the NE-DCIS, with certain inputs (NMS) provided from the E-DCIS by means of isolated data links.

The DPS and the E-DCIS provide the reactor trip echelon. The plant protection subsystems, the voting logic, dedicated data links, load drivers and HCU solenoids provide the reactor trip function in the safety-related E-DCIS. The backup SCRAM solenoids in the HCU solenoid air header and safety-related ATWS/SLCS logic provide an additional means of reactor trip. The nonsafety-related DPS, switches in the return side of the HCU solenoid and motor driven FMCRD run in provide a diverse reactor trip function. In addition, the NE-DCIS redundant control systems will enable the plant to avoid the need to trip for certain events (including a 100% load rejection) by maintaining the plant within acceptable limits.

The E-DCIS and DPS provide the ESF echelon. The ESF subsystems within the ECCS SSLC, the ESF coincidence logic, the ESF actuation subsystems, dedicated data links, and data highways provide the ESF function in the E-DCIS. The DPS provides a diverse means to actuate some ESF functions. In addition, the E-DCIS and NE-DCIS actuate defense-in-depth plant systems to enable the plant to avoid the need for actuating the passive safety-related systems.

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

The CMF of processor-based subsystems postulated for this document is a failure that occurs in all similar subsystems. This postulated failure could be caused by failure of a common hardware element, or failure of a common software element. This failure mode is assumed to cause the complete loss of function of the E-DCIS, but not the loss of any DPS functions due to the diversity of the implementations. The result of this failure is that the entire system or systems fail to produce any protective actions. The evaluation of the instrumentation and control architecture based on this failure is contained in Section 5 of this document.

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

The PRA will consider CMFs within the instrumentation and control architecture, in conjunction with random failures. Although final results will not be available until the DCIS is finalized and the hardware/software chosen, preliminary PRA results have evaluated the contribution to core damage due to instrumentation and control CMF to be acceptably low. It is conservatively assumed in the PRA that all software modules or hardware modules of a type will fail

simultaneously. The diversity between the E-DCIS and DPS assures that the joint CMF probability is acceptably low.

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

In the ESBWR instrumentation and control architecture, input signals are not shared between DPS and any of the safety-related systems. For CMF within the E-DCIS, the system is conservatively assumed to not initiate any of the protective actions needed during an event.

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

Optical isolation is provided between subsystems to prevent propagation of electrical failure in either direction; the individual data links (except for a very few functions) are one way without the receiving component being dependent on receipt of the data for correct operation. The four divisions of the E-DCIS are physically separated for power, fire protection and (normal) HVAC (it is assumed that there is no active HVAC for accidents). Since sensors are considered to be contained in a measured variable block for the purposes of the analyses in this report, failure of signal conditioning equipment influencing sensor performance is not considered. (Note that the instrumentation and control hardware contains features to minimize the occurrence of this failure mode, like auto-calibration and parameter validation.)

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

The frequency of a postulated accident occurring in conjunction with CMFs of the E-DCIS and failures of the DPS will be discussed in the PRA that also discusses E-DCIS and DPS modeling. Section 5 of this document provides a strategic evaluation of the ability of the instrumentation and control architecture to produce the following required protective actions to support the safety-related goals:

- Reactor shutdown
- Maintain reactor coolant inventory
- Initiate and maintain core decay heat removal
- Initiate and maintain containment cooling
- Initiate containment isolation

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

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

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

For the low probability circumstance where an event that requires a reactor trip occurs coincident with a postulated CMF in the RPS function of E-DCIS, the DPS initiates the reactor trip in a diverse fashion. The specific functions performed by the DPS will be finalized based on the PRA evaluation but specific capabilities will be discussed in Section 5 of this report. The DPS

functional requirements are based on an assessment of the existing RPS capabilities, accident severity and instrumentation CMF probabilities combined with the event probability.

Additionally, both the E-DCIS and DPS provide manual means of tripping the reactor. To support manual reactor trip, both the E-DCIS and the DPS provide plant information to the operator. The E-DCIS provides the class 1E 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 (ESF)**

For the low probability circumstance where an event that requires one or more ESF actuations occurs coincident with a postulated CMF in the ESF/ECCS SSLC function of E-DCIS, the DPS initiates selected ESF actuations in a diverse fashion. The specific functions performed by the DPS will be finalized based on the PRA evaluation (an quantitative analysis of DCD Chapter 15 events) but specific capabilities will be discussed in Section 5 of this report. The DPS functional requirements are based on a qualitative assessment of the existing ECCS capabilities, accident severity and instrumentation CMF probabilities combined with the event probability and reasonable operator actions.

Additionally, the E-DCIS provides both system level and component level manual means of actuating ESF functions, and DPS provides manual means of actuating selected ESF functions. To support manual ESF actuation, both the E-DCIS and the DPS provide plant information to the operator. The E-DCIS provides the class 1E measurements of parameters that initiate ESF and monitor its progress, while the DPS provides nonsafety-related diverse indications.

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

Generally only isolated, independent interconnections exist between the reactor trip and ESF actuation functions for safety-related display purposes only. Since the RPS and ECCS functions use separate sensors and hardware/software, failure of the reactor trip function will not prevent the ESF actuation function from responding to other inputs, nor will failure of the ESF actuation function 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 instrumentation and control architecture. The NE-DCIS provides nonsafety-related operator displays and alarms. Plant data for the nonsafety-related displays and alarms is obtained from across the instrumentation and control architecture by means of the real-time data network. The ECCS SSLC within the E-DCIS provides safety-related operator displays. In addition, the DPS provides nonsafety-related, diverse operator indications. No sensors are shared between the RPS/ECCS SSLC and the DPS. Diverse and independent signal conditioning and data acquisition functions will be performed in the RPS/ECCS SSLC and DPS such that a postulated software common mode failure in either platform will not degrade the signal conditioning and data acquisition functions in the other platform.

Signals are transmitted from the E-DCIS to the NE-DCIS via one way isolated fiber optic connections that prevent failures in the NE-DCIS from affecting operation of the E-DCIS. Once signals leave the E-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 E-DCIS to NE-DCIS are routed and isolated to meet the independence requirements of GDC-24 (Reference 14), IEEE-603 (Reference 11), IEEE-379 (Reference 12), and IEEE-384 (Reference 8).

No credible failure of the NE-DCIS will prevent the safety-related system from performing its safety-related function. Although E-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 NE-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 alarm/annunciator system is also used to direct attention to faults in the safety-related systems that the operator may otherwise not be looking at.

The automatic functions of the E-DCIS are designed to protect the ESBWR from potential operator induced transients which may result from failures in the NE-DCIS, however unlikely considering the redundancy built into 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 E-DCIS. The nonsafety-related DPS also provides manual reactor trip and selected ESF actuation capabilities.

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

The E-DCIS provides both system-level and component-level manual means of actuating ESF functions; the DPS provides manual means of actuating selected ESF functions.

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

### **5.1 INTRODUCTION**

The ESBWR 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 instrumentation and control systems architecture reflects this multiple level of defense approach by including safety-related and nonsafety-related instrumentation systems that provide safety-related and nonsafety-related means of initiating protective functions that both shutdown the reactor and provide for core cooling.

This section of the document 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
- Containment Isolation

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

For the purposes of discussing instrumentation and control diversity, the ESBWR instrumentation and control system can be organized into three layers. The first layer contains the nonsafety-related NE-DCIS that provides the monitoring, and the automatic and manual control of nonsafety-related functions. The NE-DCIS, specifically the PIP A, PIP B and BOP control functions, include sensors, rod control and information system cabinets, control logic cabinets, reactor level and pressure control, turbine generator control, power generation and automation control and heat cycle and support systems control.

The NE-DCIS also provides operator displays and alarm/annunciators in the main control room and remote shutdown area. Dedicated functional processors perform display and alarm processing; dedicated processors also provide the historian, SPDF, core thermal power and flow calculations and core thermal limits calculations. All of these processors acquire information from the other plant instrumentation and control systems (including the safety-related systems through isolated fiber gateways) by means of the real-time data network which is also part of NE-DCIS.

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

## Figure 7 NE-DCIS Control Systems

### NE-DCIS Control Systems

The nonsafety-related DCIS system for the ESBWR is divided into four "sub networks" each of which is dual or triply redundant.

Although when normally running, the division of networks is transparent to the plant operator, the sub-networks are capable of operating independently.

The sub-divisions are:

- Plant Investment Protection A (PIP A)
- Plant Investment Protection B (PIP B)
- GENE network
- Balance of Plant (BOP)

The systems/functions assigned to the sub-networks are indicated below

GENE network
RC&IS
Divisional Gateways
Core Thermal Power/flow
SPDS
ATLM
MRBM
RWM
3D-Monitore
AFIP (Gamma Thermometers)
SB&PC
FWC
DPS
Mimic Gateways
Historian

PIP A
PSWS A
RCCW A
Reactor/Control Building Chillers A
diesel generator A
6.9 kv Distribution A
480 vac Distribution A
Drywell Cooling A
FAPCS A
RWCU/SDC A
Instrument Air A
Uninterruptible AC/DC A
CRD A
Alarm System A
Firewall/TSC A
Area Radiation Monitoring
Process Radiation Monitoring
Historian

PIP B
PSWS B
RCWS B
Reactor/Control Building Chillers B
Diesel Generator B
6.9 kv Distribution B
480 vac Distribution B
Drywell Cooling B
FAPCS B
RWCU/SDC B
Instrument Air B
Uninterruptible AC/DC B
CRD B
Alarm System B
Firewall/TSC B
Area Radiation Monitoring
Process Radiation Monitoring
Historian

BOP
Offsite Power and Switchyard
Main, Unit, Reserve Transformers
13.8 kv Distribution
480 vac Distribution
Load Group C Vital AC/DC
TCCW
Non-Nuclear Chillers
Turbine Control and Protection
Turbine Seals
Main Generator
Moisture Separator/Reheater
Condensate
Feedwater
Condensate Polishing
Condenser
Circulating Water
Main Cooling Towers
Makeup Water
Condensate Transfer and Storage
Traveling Screens
Service Air
Sumps
Condensate Polishing
Radwaste
Plant Automation System
Loose Parts Monitoring
On-Line Procedure Monitor,
Nuclear, BOP, Turbine
Performance Monitor
Historian

The second layer contains the E-DCIS including separate reactor trip and ECCS processors. The E-DCIS provides the safety-related reactor trip function, ESF actuation functions, and safety-related plant monitoring function. In the E-DCIS, both automatic and manual means are provided to trip the reactor and actuate the engineered safety features. The E-DCIS contains sensors, plant protection subsystems, RPS and ESF coincidence logic, ESF actuation subsystems (solenoids and squib valves, logic buses, reactor SCRAM solenoids, remote multiplexers, operator monitoring and controls via safety-related touch screen displays.

The third layer contains the DPS; the DPS 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 2/4 sensor trip information and triply 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 the E-DCIS.

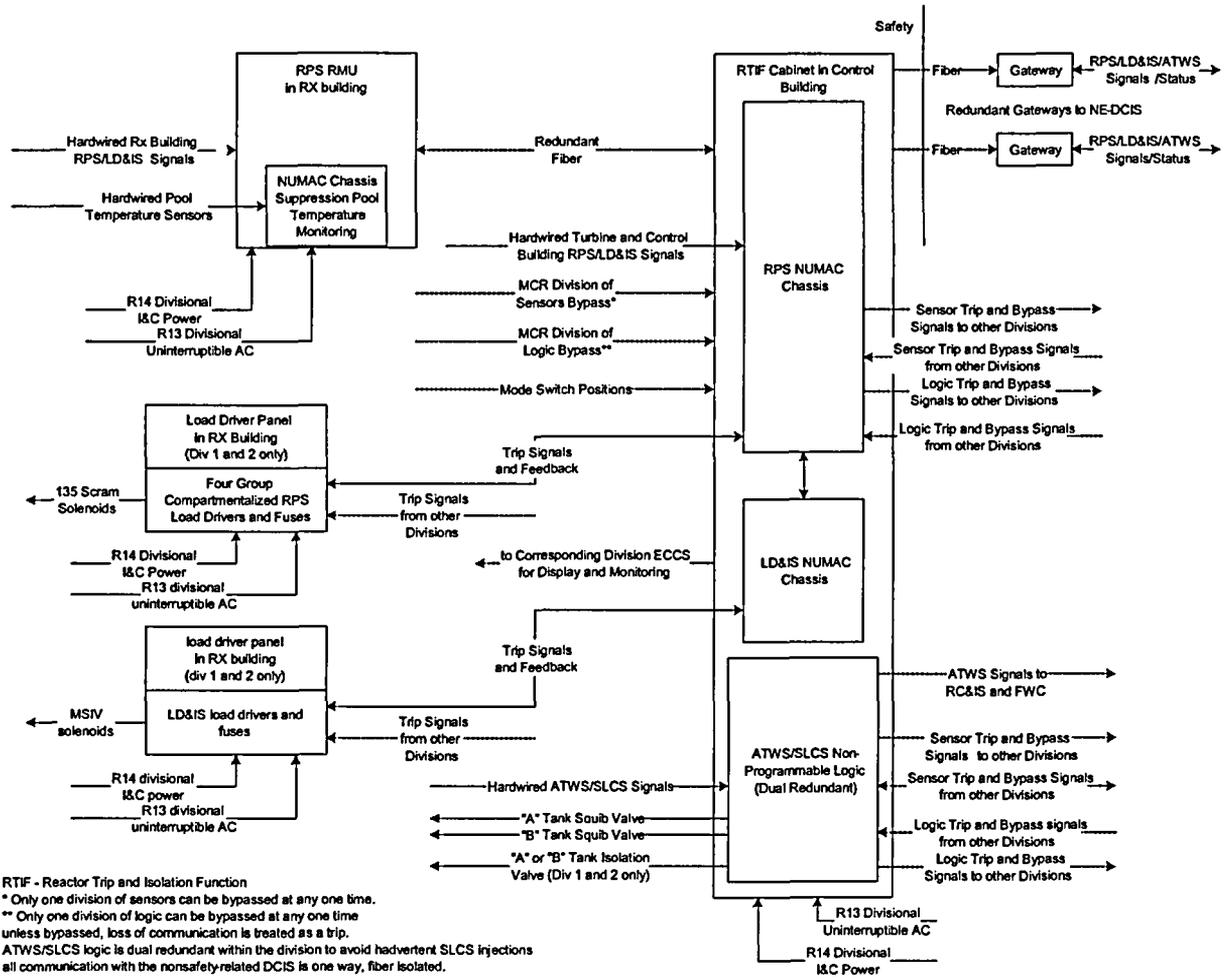
Figure 3 shows how diverse sensors, systems and power are integrated into the instrumentation and control architecture.

### 5.3 REACTOR SHUTDOWN

Reactor shutdown is the process of 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 the 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 boron injection.

- The control rods can be hydraulically scrammed into the core using stored nitrogen pressure initiated by the RPS function of E-DCIS. The safety-related SSLC processors evaluate 2/4 sensor trip decisions and separately provide 2/4 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 will eventually cause a SCRAM should the load drivers fail to open. The E-DCIS also provides controls for manual insertion of the control rods by using contactors to directly interrupt the HCU solenoid current without any microprocessor involvement. The non-microprocessor based ATWS/SSLC logic will automatically inject boron and can independently shut down the reactor; the manual SCRAM and ATWS/SLCS system represent diversity within the E-DCIS. Figure 8 illustrates the RPS function of E-DCIS.

Figure 8 RPS Function of E-DCIS



- The nonsafety-related RC&IS systems allow the operator to automatically or manually insert all of the control rods using their electric motors. Although the operator must usually initiate the process, it can also be automatically initiated by the “SCRAM follow” function of RC&IS (initiated automatically post SCRAM) or by the ATWS/SLCS logic through the DPS.
- The DPS provides automatic reactor shutdown by also hydraulically scrambling the control rods. This nonsafety-related system uses sensors, processors and actuators that are diverse from those in E-DCIS. Specifically the triply redundant processors of DPS make 2/4 sensor trip decisions and when two of 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 hardwired manual SCRAM diverse from the E-DCIS manual SCRAM. The DPS uses only a subset of E-DCIS SCRAM parameters that will be further evaluated during detailed design for their adequacy in meeting the requirements of Branch Technical Position (BTP) 19 (Reference 2). The DPS SCRAM parameters are further discussed in section 5.8 of this report.

#### **5.4 REACTOR COOLANT SYSTEM INVENTORY CONTROL**

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

- During normal and accident plant operation, reactor level is automatically maintained from startup to rated power operation to shutdown by the Feedwater Control System. This control system and the mechanical Feedwater System is a triply redundant control design using triplicated 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 offsite power is available and can be operated manually.
- During normal and accident 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 system can inject water at medium reactor pressures available after reactor pressure has been reduced manually or automatically. Each half of these systems is controlled by the PIP A and PIP B NE-DCIS respectively and each half can be operated independently.
- During accident situations when neither offsite power or the diesel generators are available, the safety-related E-DCIS ECCS SSLC can automatically initiate the four isolation condensers; although strictly the ICs will not add inventory, they do not lose inventory as they provide cooling at any but the lowest reactor pressures.

Finally at lower reactor levels without offsite or diesel power, the E-DCIS ECCS SSLC can automatically initiate a reactor depressurization (using both SRVs and DPVs) and then automatically drain the contents of the GDCS pools into the vessel. This will keep the core covered throughout the initial stages of the accident and later the E-DCIS can drain (“equalize”) the suppression pool water into the reactor vessel for long term cooling. The ICs, depressurization and GDCS can also be initiated manually.

- The DPS provides diverse coolant system inventory control by its ability to automatically initiate the ICs, SLCS, the Automatic depressurization system and the GDCS. This nonsafety-related system uses sensors, processors and actuators that are diverse from those in E-DCIS. Specifically the triply redundant processors of DPS make 2/4 sensor trip decisions and when two of the three processors agree, the various systems are initiated. The IC and SRV initiation is provided by opening nonsafety-related solenoids located “in parallel” to the existing safety-related solenoids. The explosive (squib) valves: the DPVs, GDCS and SLCS valves are fired by fiber-isolated inputs “in parallel” to the E-DCIS inputs to those same valves. Note that the suppression pool equalizing function is not provided by the DPS because it is not required for approximately 30 minutes and manual actuation is deemed acceptable. The DPS also provides for manual initiations of these various systems diverse from the E-DCIS manual initiations. Several accident scenarios are further discussed in Section 5.8 of this report.

## 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 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 injection systems discussed in Section 5.4.

- During normal and accident plant operation, core decay heat removal is accomplished with the bypass valves or main turbine and the main condenser from startup to rated power operation to shutdown under the control of the SB&PC System and Turbine Generator Control System (TGCS). These control systems are a triply redundant design using triplicated 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 offsite power is available and can be operated manually.
- During normal and accident 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. Each half of the RWCU/SDC systems is controlled by the PIP A and PIP B NE-DCIS respectively and each half can be operated independently.

- During accident situations when neither offsite power nor the diesel generators are available, the four safety-related ICs are automatically initiated by E-DCIS ECCS SSLC. These systems will 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 will cause the E-DCIS ECCS SSLC to automatically initiate a reactor depressurization (using both SRVs and DPVs) and then automatically drain the contents of the GDCS pools, and eventually the suppression pools, into the vessel. This will keep the core covered and decay heat 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, depressurization 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 E-DCIS, specifically ICs, the reactor depressurization system and the GDCS. This nonsafety-related system uses sensors, processors and actuators that are diverse from those in E-DCIS. Specifically the triply redundant processors of DPS make 2/4 sensor trip decisions and when two of the three processors agree, the various systems are initiated. The IC and SRV initiation is provided by opening nonsafety-related solenoids located “in parallel” to the existing safety-related solenoids. The explosive valves on the DPVs and GDCS are fired by fiber-isolated inputs “in parallel” to the E-DCIS inputs to those same valves. The DPS also provides for manual initiations of these various systems diverse from the E-DCIS manual initiations. As mentioned in Section 5.4, manual action is required to drain (“equalize”) the suppression pool water into the reactor vessel. Several accident scenarios are further discussed in Section 5.8 of this report.

## 5.6 CONTAINMENT COOLING

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

- In normal or accident operation with offsite power or diesel generator power available, drywell cooling is provided by the PIP A and PIP B drywell cooling system. The fans of the drywell coolers as well as the supporting chilled water, and the RCCW and PSW systems can maintain the drywell within its design temperatures. Each half of the drywell cooling system is controlled by the PIP A and PIP B NE-DCIS respectively and each half can be operated independently.
- In normal or accident operation without offsite or diesel generator power available, the passive containment cooling system will maintain containment cooling. This system is completely passive with no active components and does

not need to be “initiated”. 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 will automatically remove more heat that is ultimately dissipated in pool temperature increase and boiling to the atmosphere. Since this system has no active components and is permanently “on”, neither E-DCIS nor DPS is required to initiate it.

## 5.7 CONTAINMENT ISOLATION

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

- In normal operation many containment isolation valves are open and are automatically closed by the E-DCIS; depending on the system different signals used to initiate automatic closure. Manual isolation is also provided by the E-DCIS.
- The MSIVs and certain streamline drain valves are controlled by the RPS SSLC portion of E-DCIS; the ESF/ECCS SSLC portion of E-DCIS controls other isolation valves. The actuation logic typically uses a combination of low reactor level, high area temperatures, high system flows or high differential flows to automatically close the various valves. The logic is described in chapter 7 of the DCD.
- The DPS does not provide automatic isolation of all ESBWR containment isolation valves but rather only those thought to represent a large leakage path to the plant environs. The choice of valves, which will be validated by later studies on accidents and radiation release assuming a digital protection system CMF, includes the MSIVs, the IC isolation valves and the RWCU/SDC isolation valves. The MSIVs will be closed by DPS on low reactor level or high steamline flow; the actuators will be switches in the 120 VAC MSIV solenoid return current. The IC isolation valves will be closed by high flow; the actuators will be nonsafety-related solenoids “in parallel” with the existing safety-related solenoids controlled by E-DCIS. The RWCU/SDC isolation valves will be closed by high differential flow; the actuators will be nonsafety-related solenoids “in parallel” with the existing safety-related solenoids controlled by E-DCIS. The DPS also provides for manual isolation of these valves.

## 5.8 EVENT SCENARIOS

Appendix A provides a discussion of the DCD Chapter 15 accidents and transients evaluated to determine the effectiveness and scope of the DPS. Appendix B provides a summary table of the Chapter 15 evaluation. Confirmatory analyses will finalize the design of sensors and logic necessary for DPS to be compliant with BTP HICB-19 (Reference 2). The following sections of transients/accidents provide a qualitative

evaluation of DPS response to the same events used to evaluate ATWS/SLCS, which has a similar (partial) function.

### **5.8.1 MSIV closure**

This accident is effectively mitigated by the DPS. The DPS will SCRAM the reactor directly on MSIV closure and initiate the ICs on either low reactor level or MSIV closure when needed to provide core cooling when isolated. Additionally the feedwater system and main condenser will remain available with offsite power. The CRD, FAPCS and RWCU/SDC systems will remain available to provide inventory and heat removal with diesel generator power – none of which is affected by an E-DCIS failure.

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

This accident is effectively mitigated by the DPS. The main turbine will trip on high condenser vacuum (otherwise insufficient vacuum), as will the bypass valves – both controlled by triply redundant NE-DCIS control systems unaffected by the loss of E-DCIS. With the reactor effectively isolated, the DPS will SCRAM the reactor directly on the resulting high pressure and initiate the ICs needed to provide core cooling when isolated. Additionally the CRD, FAPCS and RWCU/SDC systems will remain available to provide inventory and heat removal with diesel generator power – none of which is affected by an E-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. In the worst case the reactor will remain in a steady state overpower condition with the potential for fuel damage; since the NE-DCIS remains operational the situation will be alarmed to the operator and control rods automatically inserted by the FWC logic. Even assuming the unlikely failure of the E-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 will be concentrated in the power plant rather than offsite. Although DPS had no part in the transient, there should be little or no offsite consequences.

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

This accident is effectively mitigated by the DPS. The DPS will SCRAM the reactor directly on either low reactor water level from loss of feedflow or the high reactor pressure resulting from the turbine trip and bypass valve closure. Both the bypass valves and turbine are controlled by triply redundant NE-DCIS control systems unaffected by the loss of E-DCIS. The DPS will initiate the ICs on low reactor level when needed to provide core cooling when isolated. Additionally the CRD, FAPCS and RWCU/SDC

systems will remain available to provide inventory and heat removal with diesel generator power – none of which is affected by a postulated E-DCIS failure.

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

This accident is effectively mitigated by the DPS. The DPS will SCRAM the reactor directly on low reactor water level from loss of feedflow; what separates this transient from the one above is that the main condenser and bypass valve pressure control remains available. The turbine will eventually be tripped either manually or on reverse power; both the bypass valves and turbine are controlled by triply redundant NE-DCIS control systems unaffected by the loss of E-DCIS. The DPS will initiate the ICs on low reactor level when needed to provide core cooling if level falls below IC initiation level. Additionally the CRD, FAPCS and RWCU/SDC systems will remain available to provide inventory and heat removal with offsite or diesel generator power – none of which is affected by an E-DCIS failure.

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

This accident is effectively mitigated by the DPS. The accident scenario is different depending on whether the E-DCIS failure either SCRAMs or doesn't SCRAM the reactor (the SCRAM is automatically bypassed if the bypass valves open). The single bypass system failure will not affect the SB&PC triply redundant control system nor the high pressure EHC oil system (a standby pump will automatically start) so the failure is that one of the twelve bypass valves will fail to open. If the E-DCIS SCRAMs the plant the remaining bypass valves, main condenser and feedwater will allow/maintain normal reactor level and pressure and a normal shutdown. If the E-DCIS does not SCRAM the plant but the resulting steam flow is within the capacity of eleven remaining bypass valves, then the above scenario repeats. If the remaining bypass capacity is insufficient the DPS will SCRAM the plant on the resulting high reactor pressure.

Note that the load rejection may have been caused by a grid related condition so the E-DCIS SCRAM or SCRAM failure will determine whether the turbine is supplying house load and “offsite power” remains available. If the turbine remains on line (no SCRAM) the plant operator will reduce power to approximately 20 – 30% and will manually (DPS) SCRAM the plant when offsite power is restored (to repair the E-DCIS).

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

### 5.8.7 Inadvertent Isolation Condenser Initiation

This transient does not require mitigation by DPS since the result of the inadvertent actuation should only result in 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 E-DCIS failure. In any case, the IC pools will begin heating and eventually the ICs should be isolated if the normal initiation valves cannot be closed. If the E-DCIS failure results in the inability to isolate, the isolation can be done manually by the DPS. Since feedwater and the normal heat sinks remain available, the plant can be manually scrammed (from DPS if necessary) and shut down normally. If offsite power were lost, the CRD, FAPCS and RWCU/SDC systems will remain available to provide inventory and heat removal with diesel generator power – none of which is affected by an E-DCIS failure.

### 5.8.8 Turbine Trip with Full Bypass

This accident is effectively mitigated by the DPS. The accident scenario is different depending on whether the E-DCIS failure either SCRAMs or doesn't SCRAM the reactor (the SCRAM is automatically bypassed if the bypass valves open). If the E-DCIS scrams the plant the bypass valves, normal heat sink and feedwater flow will allow/maintain normal reactor level and pressure and a normal shutdown. If the E-DCIS does not SCRAM the plant but the resulting steam flow is still within the capacity of the bypass system, then the above scenario repeats.

Since the turbine is offline but offsite power remains available, the plant operator will reduce power to hot standby to minimize condenser duty and will manually (DPS) SCRAM the plant (to repair the E-DCIS).

If there is a simultaneous loss of offsite power, the DPS will SCRAM the reactor directly on low reactor water level from loss of feedflow or high reactor pressure resulting from the turbine and bypass valve trip (these control systems are unaffected by the E-DCIS failure). The DPS will initiate the ICs on low reactor level when needed to provide core cooling if level falls below IC initiation level. Additionally the CRD, FAPCS and RWCU/SDC systems will remain available to provide inventory and heat removal with offsite or diesel generator power – none of which is affected by an E-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 an E-DCIS failure will not affect the triply redundant turbine control or SB&PC systems. The SB&PC and turbine control systems will close a turbine control valve(s) to match the open bypass valve steam flow; no level or pressure changes should result.

If the transient involves an opening turbine control valve or the turbine or bypass valve opening is too sudden for proper pressure control, then a decreasing reactor pressure

transient should result. This could eventually cause a low pressure MSIV isolation but the assumed E-DCIS failure would prevent that. If the DPS system 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 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 will allow/maintain normal reactor level and pressure and a normal shutdown. The DPS will initiate the ICs on low reactor level when needed to provide core cooling if level falls below IC initiation level. Additionally the CRD, FAPCS and RWCU/SDC systems will remain available to provide inventory and heat removal with offsite or diesel generator power – none of which is affected by an E-DCIS failure.

## 6 REFERENCES

1. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection systems," October 21, 1994.
2. Branch Technical Position HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," Rev. 4 - June 1997
3. 26A6641 (Tier 1, Rev. 1, March 2006), 26A6642 (Tier 2 Rev. 1, January 2006), "ESBWR Design Control Document",
4. NEDO-33230, LTP "ESBWR I&C Software Safety Plan," January 2006.
5. NEDO-33227, LTP "ESBWR I&C Software Configuration Management Plan", February 2006
6. NEDO-33228, LTP "ESBWR I&C Software Verification and Validation Plan", January 2006
7. NEDO-33226, LTP "ESBWR I&C Software Management Plan", January 2006
8. IEEE 384-1981, "IEEE Criteria for Independence of Class 1E Equipment and Circuits."
9. NEDO-33201, "ESBWR Certification Probabilistic Risk Assessment" (not yet issued)
10. NUREG-0493, "A Defense-in-Depth & Diversity Assessment of the RESAR-414 Integrated Protection System," March 1979
11. IEEE 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"
12. IEEE 379-2000, "IEEE Standard Application of the Single-failure Criterion to Nuclear Power Generating Station Safety Systems – Description"
13. R.G. 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," May 1973
14. General Design Criteria 24, Separation of Protection and Control Systems

## **APPENDIX A - ESBWR Instrumentation & Control Defense-in-Depth and Diversity (D3) Evaluation of Chapter 15 Events Assuming Common Mode Failure of a Digital Protection System**

### **INTRODUCTION**

This evaluation determines the effect of common-cause/common mode failures on the events documented in Design Control Document Chapter 15, Safety Analyses, as required by Branch Technical Position HICB-19 (Reference No. 1).

As a point of reference, Branch Technical Position (BTP) HICB-19 provides acceptance criteria for two sets of events (Abnormal Operating Occurrences and Design Basis Accidents). Some events are bounded and this conclusion is documented as part of the evaluation.

This evaluation needs to be updated when design details are finalized (e.g., hardware platforms and details of the hardware components are determined, and failure modes and effects are better known or evaluated).

Additionally, this evaluation needs to be updated when future analyses are completed to support the evaluation. The table that follows identifies those events which either require further analyses to support the conclusions, are recommended, or require an assessment positioning the conclusions provided.

Conclusions:

The following DPS system attributes are confirmed:

Diverse reactor trip on the following signals:

- High reactor pressure,
- High drywell pressure,
- High suppression pool temperature,
- High reactor water level (L8)
- Low reactor water level (L3)

Diverse ECCS actuation on the following signals:

- Low reactor water level (L1)

DPS scope expansion (to be confirmed by analysis):

- *Diverse MSIV closure reactor trip*
- *Diverse containment/break isolation of RWCU/SDC on differential flow or temperature or radiation (to limit radiation release)*
- *Diverse containment/break isolation of Isolation condenser system on differential flow, or radiation (to limit radiation release)*
- *Diverse containment/break isolation of Main Steam Lines via MSIV on high steam flow/or low steamline pressure (to limit radiation release).*
- *Possible diverse containment isolation on Low reactor water level (L1) (to limit radiation release).*

**Table - Summary of Events That Require Supporting Analyses or Confirmatory Assessment.**

The following ESBWR DCD Tier 2 Chapter 15 events may require further analysis to verify that the acceptance criteria (2.5 REM for AOOs and 25 REM for DBAs) can be met.

Subsection	Event	Issue
15.2.2.7	Closure of all MSIVs:	Determine the amount of fuel failure.
15.2.1.1	Loss of Feedwater Heating:	Cycle specific analysis may be required to verify evaluation assumptions are valid.
15.3.4	Pressure Regulator Failure – Closure of All Turbine and Bypass Valves:	Fuel failure more likely to occur in this event assuming a CMF of RPS. Verify radiological acceptance criteria satisfied.
15.3.5	Generator Load rejection with Total Turbine Bypass Failure:	Fuel failure more likely to occur in this event assuming a CMF of RPS. Verify radiological acceptance criteria satisfied.
15.3.6	Turbine Trip With Total Turbine Bypass failure:	Fuel failure more likely to occur in this event assuming a CMF of RPS. Verify radiological acceptance criteria satisfied.
15.4.2	LOCA Inside containment:	Worst-case dose may challenge 10 CFR 100 guidelines without implementation of containment isolation. Analysis is required to confirm the results.
15.4.5	Main Steamline Break Outside Containment:	Level 3 should occur quickly to provide trip. Confirmation required that isolation on L1 is acceptable or if MSIV closure is required to limit radiation release.
15.4.9	RWCU/SDC System Line Failure Outside Containment:	Analysis required to verify radiological acceptance criteria satisfied; if break size not sufficient to reduce level to L1 containment isolation does not occur. Determine acceptability of radiological release.

**References:**

1. Branch Technical Position HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in digital Computer-Based Instrumentation and control systems"
2. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, " December 1994?"
3. Staff Requirements Memorandum to SECY-93-087, Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs, " July, 21 1993.

**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 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>1</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.*

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.*

---

<sup>1</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 CMF, 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 CMFs 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.

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

**ESBWR DCD Tier 2, Chapter 15 Event Analysis**

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

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

Systems required (DCD Table 15.1-5: System Event Matrix): SCRRRI

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

Event Diagram: 15.1-2

Event Analysis: Non-limiting event. No SCRAM assumed for this event (slow power increase occurs). RC&IS/SCRRRI 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 associated with this event.

**15.2.2 Increase in Reactor Pressure**

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

Systems 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 acts to open remaining TCVs and some TBVs and plant stabilizes at new steady state. No barrier breaches occur. Overpressure protection is available but not challenged.

Conclusion: No radiological consequences associated with this event.

**15.2.2.2 Generator Load Rejection With The Turbine Bypass System (AOO)**

Systems required (DCD Table 15.1-5: System Event Matrix): TBV Initiation – TCV Fast Closure; TCV Fast Closure – Load rejection; SCRRRI

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 acts to open remaining TCVs and some TBVs and plant stabilizes at new steady state. RC&IS/SCRRRI assumed to function. Neutron flux may reach SCRAM setpoint (but CMF failure precludes trip). There is a possibility of SCRAM on high reactor pressure from DPS. SB&PC acts to mitigate event.

No barrier breaches occur.

Conclusion: No radiological consequences associated with this event. Overpressure protection available.

**15.2.2.3 Generator Load Rejection With A Single Failure In The Turbine Bypass System (AOO)**

Systems required (DCD Table 15.1-5: System Event Matrix): ICS and MSIV closure – RPV Low Water Level (L2 + 30 sec delay); TBV Initiation – TCV Fast Closure;

TCV Fast Closure – Load rejection; CRD Makeup Water – RPV Low Water Level (L2)

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

Event Diagram: 15.1-5

Event Analysis: 50% of the BPVs assumed available; pressurization is less severe than MSIV closure event. Event bounded by MSIV closure event.

Conclusion: No radiological consequences associated with this event. Overpressure protection available from SRVs.

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

Systems required (DCD Table 15.1-5: System Event Matrix): TBV Initiation – TSV Closure; SCRR

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

Event Diagram: 15.1-6

Event Analysis: Bounded by Turbine trip with a Single Failure in the Turbine Bypass system.

Conclusion: No radiological consequences associated with this event. Overpressure protection available from SRVs.

#### 15.2.2.5 Turbine Trip With A Single Failure In The Turbine Bypass System (AOO)

Systems required (DCD Table 15.1-5: System Event Matrix): ICS and MSIV closure – RPV Low Water Level (L2 + 30 sec delay); TBV Initiation – TSV Closure; CRD Makeup Water – RPV Low Water Level (L2)

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

Event Diagram: 15.1-7

Event Analysis: Event bounded by MSIV closure event. In this event the single failure assumed results in the worst case scenario of 50% of the bypass valves failing. The pressurization resulting from this event is less severe than all MSIV closure event.

Conclusion: No radiological consequences associated with this event. Overpressure protection available from SRVs.

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

Systems required (DCD Table 15.1-5: System Event Matrix): ICS – MSIV position; MSIV Closure – High Steamline Flow; CRD Makeup Water – RPV Low Water Level (L2)

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

Event Diagram: 15.1-8

Event Analysis: Event bounded by closure of all MSIVs.

Conclusion: No radiological consequences associated with this event. Overpressure protection available from SRVs.

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

Systems required (DCD Table 15.1-5: System Event Matrix): ICS – MSIV position; CRD Makeup Water – RPV Low Water Level (L2)

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

Event Diagram: 15.1-9

Event Analysis: In worst-case analysis, MSIV position trip (which is the primary trip) is not credited, and high neutron flux trip is credited. Safety valves function to protect the reactor coolant pressure boundary (RCPB). In this event, assume RPS does not function. The DPS high reactor pressure trip reached within seconds to limit the pressure transient. Some fuel failure may occur. Pressure transient is bounded by the ATWS scenario. High neutron flux, vessel pressure and suppression pool temperature are anticipated for this event.

Conclusion: No radiological consequences associated with this event. Some fuel failure may occur if the DPS high pressure SCRAM is credited. [Worst case, dose less than D3 acceptance criteria (2.5 REM TEDE for AOOs).] Pressure response bounded by ATWS analysis. Implementation of an MSIV closure trip in DPS will provide margin.

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

Systems required (DCD Table 15.1-5: System Event Matrix): ICS – MSIV position; TBV Closure – Low Low Condenser Vacuum; TSV Closure – Low Condenser Vacuum; MSIV Closure – Low Condenser Vacuum; CRD Makeup Water – RPV Low Water Level (L2)

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

Event Diagram: 15.1-10

Event Analysis: If RPS CMF is assumed, vessel pressurization and peak cladding temperature may approach MSIV closure event which is bounding. Overpressure protection available (with peak pressure controlled by the SRVs). Assume RPS CMF as the worst case for this event. With RPS CMF, it may be possible that ATWS may fail to function due to unavailability of the NMS neutron flux permissive (same platform for RPS and NMS). DPS high reactor pressure trip functions to provide negative reactivity insertion within seconds. The DPS high reactor pressure trip will also attenuate the pressure transient. As an additional layer of defense, manual initiation of ATWS mitigation would be available to provide initiation of ARI, SLC injection and feedwater runback. Manual scram from RPS or DPS would be available to mitigate this event. (ATWS sensor indication and DPS sensor indication are available for operator to assess and determine an ATWS event has occurred and manual initiation is required.)

Conclusion: No radiological consequences associated with this event. Overpressure protection available from SRVs.

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

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

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.)

Conclusion: No radiological consequences associated with this event.

**15.2.3 Reactor and Power Distribution Anomalies (Event Category)**

(No events identified for ESBWR)

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

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

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

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

Event Diagram: 15.1-12

Event Analysis: Not a significant or limiting event, plant systems respond to mitigate this event.

Conclusion: No radiological consequences associated with this event.

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

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

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

Event Diagram: 15.1-13

Event Analysis: Feedwater control system acts to reduce flow from other pumps to maintain desired water level. With failure of RPS, DPS would be available to produce a high water level L8 reactor trip as a worst case scenario. Not a significant or limiting event.

Conclusion: No radiological consequences associated with this event.

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

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

Systems 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.

Conclusion: No radiological consequences associated with this event.

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

Systems required (DCD Table 15.1-5: System Event Matrix): ICS – MSIV Position; ICS and MSIV closure – RPV Low Water Level (L2 + 30 sec delay); TBV Closure – Low Low Condenser Vacuum; TBV Initiation – TCV Fast Closure; TCV Fast Closure – Load rejection; MSIV Closure – Low Condenser Vacuum; CRD Makeup Water – RPV Low Water Level (L2

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

Event Diagram: 15.1-15

Event Analysis: 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

lost due to circulating water pump trips. Brief operation of bypass valves is assumed until vacuum decays. Assume RPS fails to process trip signals.  
 DPS (L3) SCRAM used to quickly provide negative reactivity.  
Conclusion: No radiological consequences associated with this event.

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

Systems required (DCD Table 15.1-5: System Event Matrix): ICS – MSIV position; CRD Makeup Water – RPV Low Water Level (L2)

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

Event Diagram: 15.1-16

Event Analysis: (Event similar to loss of power generation bus, which trips power to all feedwater pump motors.) If CMF of RPS assumed, DPS provides trip at L3. Not a limiting event.

Conclusion: No radiological consequences associated with this event.

**15.2.6 AOO Analysis Summary (Event Category)**

**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 (Infrequent Event)**

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

Automatic Trip (from DCD Table 15.1-6): None (APRM High Simulated Thermal Power-not credited)

Event Diagram: 15.1-17

Event Analysis: APRM High simulated thermal power SCRAM available for this event, but not credited. Failure of both SCRRI and RPS simultaneously is of extremely low probability. (In the unlikely scenario of both SCRRI failure and RPS CMF, a percentage of fuel may fail.)

Conclusion: Worst case, dose within 10% of 10 CFR 100 guidelines. Analysis conservatively assumes a loss of 55.6°C FW heating, while 39°C is realistic. Assumption of 1000 rods failed is conservative. Using realistic assumptions, acceptance criteria met, without crediting DPS action.

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

Systems required (DCD Table 15.1-5: System Event Matrix): ICS and MSIV closure – RPV Low Water Level (L2 + 30 sec delay); TBV Initiation – TSV Closure; TSV Closure – RPV high water Level (L8); Feedwater Pump Runback – L8; CRD Makeup Water – RPV Low Water Level (L2)

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. 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. SCRAM on

L8 occurs early enough to limit neutron flux peak and fuel thermal transient so that no fuel damage occurs.

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

Systems required (DCD Table 15.1-5: System Event Matrix): ICS – MSIV Position; MSIV Closure – Low Turbine Inlet Pressure; CRD Makeup Water – RPV Low Water Level (L2)

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 L3 SCRAM to mitigate the event.

If ESF/ECCS CMF assumed, RPS SCRAMs on MSIV closure from low turbine inlet pressure. If level drops to L1, diverse ESF (ECCS) initiation occurs.

Conclusion: No radiological consequences associated with this event.

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

Systems required (DCD Table 15.1-5: System Event Matrix): ICS – RPV High Dome Pressure; ICS and MSIV Closure - RPV Low Water Level (L2 + 30 Sec delay); CRD Makeup Water – RPV Low Water Level (L2)

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 not assumed. Reactor power and pressure controlled by SB&PC. Event bounded by closure of all MSIVs for over pressure. RCPB: Reactor pressure is maintained below ASME Service Level C limit (<120% of design pressure). Assume failure of RPS to SCRAM.

DPS SCRAMs on high pressure. Overpressure protection available from SRVs.

Conclusion: No radiological consequences associated with this event. With failure of the flux SCRAM fuel failure more likely to occur. Dose within acceptance criteria of 2.5 REM.

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

Systems required (DCD Table 15.1-5: System Event Matrix): ICS – RPV High Dome Pressure; ICS and MSIV Closure - RPV Low Water Level (L2 + 30 Sec delay); TCV Fast closure – Load Rejection; CRD Makeup Water – RPV Low Water Level (L2)

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 CMF failure assumed, DPS provides high-pressure trip. ICS and HP-CRD still available to stabilize the plant. If ESF/ECCS CMF assumed, RPS high neutron flux SCRAM signal and high RPV pressure SCRAMs still available.

Conclusion: There is a fuel failure analysis in DCD 15.3.1.5 for this event. With failure of the TCV/flux SCRAM fuel failure would be more severe. Overpressure protection still available.

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

Systems required (DCD Table 15.1-5: System Event Matrix): ICS – RPV High Dome Pressure; ICS and MSIV Closure - RPV Low Water Level (L2 + 30 Sec delay); CRD Makeup Water – RPV Low Water Level (L2)

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 not assumed. IF RPS CMF assumed, DPS provides high-pressure trip. If ESF/ECCS CMF failure assumed, RPS available for high-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 TCV/flux SCRAM fuel failure would be more severe. This event is assumed to be bounded by the load rejection with no bypass.

Overpressure protection available from SRVs to protect RCPB.

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

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

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

Event Diagram: 15.1-23

Event Analysis: Not a credible event.

Conclusion: Not analyzed.

**15.3.8 Control Rod Withdrawal Error During Startup (Infrequent Event)**

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

Trip/Protection (from DCD Table 15.1-6): SRNM Period; Rod Block – SRNM Period or ATLM Parameter Exceeded

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.

Conclusion: No radiological consequences associated with this event.

**15.3.9 Control Rod Withdrawal Error During Power Operations (Infrequent Event)**

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

Automatic Trip (from DCD Table 15.1-6): SRNM Period: SRNM trips are not in operation during power operation (RUN Mode); Rod Block – SRNM Period or ATLM Parameter Exceeded

Event Diagram: 15.1-25

Event Analysis: Simultaneous failure of RC&IS and RPS/NMS extremely low. Event not analyzed.

Conclusion: Event not analyzed.

**15.3.10 Fuel Assembly Loading Error, Mis-located Bundle (Infrequent Event)**

Systems 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 radiological consequences associated with this event.

**15.3.11 Fuel Assembly Loading error, Mis-oriented Bundle (Infrequent Event)**

Systems 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 radiological consequences associated with this event.

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

Systems 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 CMF assumed, SB&PC 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 associated with this event.

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

Systems required (DCD Table 15.1-5: System Event Matrix): FAPCS – High Suppression Pool Temperature

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 SCRAM, after which time the pressure will decrease. If RPS CMF 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 associated with this event.

**15.3.14 Inadvertent Opening of a DPV (Infrequent Event)**

Systems required (DCD Table 15.1-5: System Event Matrix): FAPCS – High Suppression Pool Temperature.

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

Event Diagram: 15.1-30

Event Analysis: SB&PC available to stabilize pressure prior to occurrence of SCRAM after which time the pressure will decrease. If RPS CMF 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 available and may be required if conditions degrade (No DPS high drywell pressure trip available).

Conclusion: No fuel damage anticipated for this event, only coolant activity is a concern. Worst case dose within 10% of 10 CFR 100 guidelines. Radiation monitoring and isolation can be credited.

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

Systems required (DCD Table 15.1-5: System Event Matrix): ICS – MSIV Position; MSIV Closure – Low Turbine Inlet Pressure; CRD Makeup Water – RPV Low Water Level (L2); FAPCS – High Suppression Pool Temperature

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

Event Diagram: 15.1-31

Event Analysis: If RPS CMF assumed DPS SCRAMs on high suppression pool temperature. FAPCS provides suppression pool cooling.

IF ESF/ECCS CMF assumed, RPS provides SCRAM on high suppression pool temperature.

Conclusion: No fuel failure occurs in this event, only coolant activity is a concern. Worst case dose within 10% of 10 CFR 100 guidelines. Radiation monitoring and isolation can be credited.

**15.3.16 Liquid Containing Tank Failure (Infrequent Event) [COL Applicant Scope]**

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

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 or DPS.

Conclusion: No adverse consequences assumed.

**15.3.17 COL Information - Not Applicable**

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

**15.4.1 Fuel Handling Accident (Accident)**

Systems 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 or DPS.

Conclusion: Worst case dose within 10 CFR 100 guidelines.

**15.4.2 LOCA Inside Containment (Containment Analysis) (Accident)**

Systems required (DCD Table 15.1-5: System Event Matrix): SRV – Power Actuated Mode (ADS); DPV – Actuation; ICS and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS and MSIV Closure– RPV Low Water Level (L1.5); SLCS - DPV Open; SLCS – RPV Low Water Level L2 – APRM not Downscale; GDCS; GDCS Equalizing Lines; High Radiation MCR recirculation; CRD Makeup Water – RPV Low Water Level (L2)

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

Event Diagram: 15.1-34

Event Analysis: If RPS CMF 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. ESF/ECCS initiation occurs to mitigate the event. Non-MSIV LD&IS isolation occurs. . If ESF/ECCS CMF assumed, diverse ESF initiation (at L1) is required to mitigate the event.

Conclusion: Worst-case dose may challenge 10 CFR 100 guidelines. Diverse ECCS initiation available to mitigate the event. Diverse containment isolation may be required to mitigate the event.

**15.4.3 LOCA Inside Containment (Performance Analysis) (Accident)**

Systems required (DCD Table 15.1-5: System Event Matrix): SRV – Power Actuated Mode (ADS); DPV – Actuation; ICS and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS and MSIV Closure– RPV Low Water Level (L1.5); SLCS - DPV Open; SLCS – RPV Low Water Level L2 – APRM not Downscale; GDCS; GDCS Equalizing Lines; High Radiation MCR recirculation; CRD Makeup Water – RPV Low Water Level (L2)

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

Event Diagram: 15.1-34

Event Analysis: Refer to 15.4.2

Conclusion: Refer to 15.4.2

**15.4.4 LOCA Inside Containment (Radiological Analysis) (Accident)**

Systems required (DCD Table 15.1-5: System Event Matrix): SRV – Power Actuated Mode (ADS); DPV – Actuation; ICS and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS and MSIV Closure– RPV Low Water Level (L1.5); SLCS - DPV Open; SLCS – RPV Low Water Level L2 – APRM not Downscale; GDCS; GDCS Equalizing Lines; High Radiation MCR recirculation; CRD Makeup Water – RPV Low Water Level (L2)

Automatic Trip (from DCD Table 15.1-6): RPV Low Water Level (L3); Loss of Power Generation Bus; 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 Outside Containment (Accident)**

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

Low Water Level (L2 + 30 sec delay); ICS and MSIV Closure– RPV Low Water Level (L1.5); MSIV Closure – Low Turbine Inlet Pressure; MSIV Closure – High Steamline Flow; SLCS - DPV Open; SLCS – RPV Low Water Level L2 – APRM not Downscale; GDCS; GDCS Equalizing Lines; High Radiation MCR recirculation; CRD Makeup Water – RPV Low Water Level (L2)

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

Event Diagram: 15.1-35

Event Analysis: If RPS CMF assumed, DPS provides SCRAM on low water level (L3). LD&IS (MSIV) isolation failure is assumed because of the same platform as RPS. ESF/ECCS initiation occurs. Diverse ESF may be required for MSIV isolation (L1) (on low turbine inlet pressure or low flow) to isolate any radiation release quickly. If ESF/ECCS CMF assumed, diverse ESF initiation (at L1) is required to mitigate the event.

Conclusion: Worst-case dose may challenge 10 CFR 100 guidelines. Diverse ECCS initiation available to mitigate the event. Diverse containment/MSIV isolation may be required to mitigate the event.

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

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

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

Event Diagram: 15.1-36

Event Analysis: Not a credible event.

Conclusion: Not analyzed.

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

Systems required (DCD Table 15.1-5: System Event Matrix): SRV – Power Actuated Mode (ADS); DPV – Actuation; ICS – MSIV Position; ICS and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS and MSIV Closure– RPV Low Water Level (L1.5); ICS – RPV High Dome Pressure; SLCS - DPV Open; SLCS – RPV Low Water Level L2 – APRM not Downscale; GDCS; GDCS Equalizing Lines; High Radiation MCR recirculation; CRD Makeup Water – RPV Low Water Level (L2)

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

Event Diagram: 15.1-37

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

Conclusion: No fuel failure assumed for this event. Worst-case dose will not challenge 10 CFR 100 guidelines.

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

Systems required (DCD Table 15.1-5: System Event Matrix): SRV – Power Actuated Mode (ADS); DPV – Actuation; ICS – MSIV Position; ICS and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS and MSIV Closure– RPV Low Water Level (L1.5); ICS – RPV High Dome Pressure; SLCS - DPV Open; SLCS – RPV

Low Water Level L2 – APRM not Downscale; GDCS; GDCS Equalizing Lines; High Radiation MCR recirculation; CRD Makeup Water – RPV Low Water Level (L2)  
Automatic Trip (from DCD Table 15.1-6): RPV Low Water Level (L3); MSIV Position; Loss of Power Generation Bus

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 CMF assumed, manual SCRAM would still be available. DPS provides manual backup SCRAM. Manually controlled orderly shutdown 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 bounded by larger breaks. Using realistic assumptions, excess flow check valves should limit release of coolant. Dose within 10 CFR 100 guidelines.

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

Systems required (DCD Table 15.1-5: System Event Matrix): SRV – Power Actuated Mode (ADS); DPV – Actuation; ICS – MSIV Position; ICS and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS and MSIV Closure– RPV Low Water Level (L1.5); ICS – RPV High Dome Pressure; SLCS - DPV Open; SLCS – RPV Low Water Level L2 – APRM not Downscale; GDCS; GDCS Equalizing Lines; High Radiation Main Control Room recirculation; CRD Makeup Water – RPV Low Water Level (L2)

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

Event Diagram: 15.1-39

Event Analysis: If RPS CMF assumed, DPS available to SCRAM on L3. If level continues to drop, Diverse ESF initiation occurs at L1. Differential flow sensors may isolate line to terminate event. CMF failure of LD&IS would extend the duration of the event until leak identified and isolated. Manual remote isolation should be available to the operator. High radiation Main Control Room Recirculation actuation signal should alert the operator of a possible line break. Additional mitigation measure may be required if dose consequences are unacceptable. [If time permits (radiation release is not excessive for ~30 minutes), consider differential flow indication to DPS for remote manual operator isolation, or diverse automatic isolation of break.]

Conclusion: Worst case dose may challenge 10 CFR 100 guidelines with CMF failure of LD&IS. Diverse isolation may be required to mitigate. If exposure does not challenge 10 CFR 100 guidelines, no additional DPS scope required.

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

Systems 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 assumed to be available. This event does not involve the RPV or containment and requires no actions from RPS and 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.

**APPENDIX B – Summary Table of DCD Chapter 15 Accidents Evaluated for D3**

Assume the worst case scenario is a CMF of a digital protection platform; no cross platform CMFs are assumed. Therefore, the analysis assumes that RPS/RTIF and LD&IS-MSIV isolation or ESF/ECCS platform will fail.

Sect	Description	Event Class	Diverse I&C system (Event Category)	Comments
15.2.1	Decrease in Core/Coolant Temperature			
15.2.1.1	Loss of Feedwater Heating	AOO	No SCRAM assumed	Diverse Protection System (DPS) has no action. Worst case failure is failure of RC&IS/SCRRRI. No radiological consequences associated with this event.
15.2.2	Increase in Reactor Pressure (Event Category)			
15.2.2.1	Closure of One Turbine Control Valve	AOO	No significant pressure increase assumed. No Diverse Protection System (DPS) challenge	Bounded by load reject. Common mode failure of any protection system presents no challenge. Since the closure of one TCV will automatically result in the opening of a sufficient number of Turbine Bypass Valves (TBVs) to offset the loss in steam flow to the turbine, nothing will happen other than a reduction of generator output and an alarm. DPS has no action. No radiological consequences associated with this event.
15.2.2.2	Generator Load rejection With Turbine Bypass	AOO	No challenge to SCRAM setpoints.	DPS has no action. Event bounded by load rejection with turbine bypass system failure.
15.2.2.3	Generator Load Rejection With a Single Failure in the Turbine Bypass System	AOO	No DPS SCRAM assumed.	A 50% reduction in bypass capacity is conservatively assumed. It is possible this will result in reaching a RPS SCRAM (flux) SCRAM setpoint (but no DPS SCRAM). There should not be a pressure increase to the DPS SCRAM setpoint, so no DPS action. This should look like a turbine trip with good level and pressure control. Event bounded by MSIV closure event.
15.2.2.4	Turbine Trip With Turbine Bypass	AOO	Bypass capability not affected. No challenge to DPS.	Event bounded by turbine trip with a single failure in the turbine bypass system.

Sect	Description	Event Class	Diverse I&C system	Comments
15.2.2.5	Turbine Trip With a Single Failure in the Turbine Bypass System	AOO	No significant pressure increase. No challenge to DPS.	A 50% reduction in bypass capacity is conservatively assumed. Event bounded by MSIV closure event.
15.2.2.6	Closure of One Main Steamline Isolation Valve (MSIV)	AOO	High reactor pressure SCRAM	DPS will SCRAM at approximately the same pressure as RPS. Event bounded by MSIV closure event.
15.2.2.7	Closure of All Main Steamline Isolation Valves	AOO	High reactor pressure SCRAM. (Possibly add MSIV closure SCRAM in DPS)	DPS will not SCRAM on MSIV closure but should SCRAM on resulting reactor pressure – effect is an MSIV closure with a slightly delayed SCRAM. ATWS event bounds this event. Some fuel failure may occur if DPS is credited. Worst case dose less than 2.5 REM.
15.2.2.8	Loss of Condenser Vacuum	AOO	High reactor pressure SCRAM	This event is essentially a turbine trip without bypass or a Main Steam Isolation Valve (MSIV) closure – DPS will SCRAM on pressure if RPS does not SCRAM on vacuum.
15.2.2.9	Loss of Shutdown Cooling Function of RWCU/SDC	AOO	No DPS action.	1 train still assumed to function. No challenge to DPS
<b>15.2.3 Reactor and Power Distribution Anomalies (Event Category)</b>				
(No events identified for ESBWR)				
<b>15.2.4 Increase in Reactor Coolant Inventory (Event Category)</b>				
15.2.4.1	Inadvertent Isolation Condenser Initiation	AOO	No significant impact.	No DPS action. No challenge to DPS.
15.2.4.2	Runout of One Feedwater Pump	AOO	No SCRAM occurs. DPS L8 SCRAM is worst case.	A feedwater (FW) pump run out results in a slowdown of the other FW pump speeds and therefore there is no level change (failure of the TMR feedwater controller (FWC) is incredible). Either DPS has no action or (like RPS) worst case will require DPS SCRAM at level L8.
<b>15.2.5 Decrease in Reactor Coolant Inventory (Event Category)</b>				
15.2.5.1	Opening of One Turbine Control or Bypass Valve	AOO	No SCRAM assumed.	Non-event since SB&PC will automatically reduce other control valve positions. If level does get to L3, then DPS will SCRAM

Sect	Description	Event Class	Diverse I&C system	Comments
15.2.5.2	Loss of Non-Emergency AC Power to Station Auxiliaries	AOO	L3 SCRAM. DPS is still available (battery power) high reactor pressure SCRAM worst case.	RPS will normally SCRAM on loss of power to plant 13.8 kV busses – DPS will not. However if RPS fails to SCRAM, then DPS will SCRAM on L3.
15.2.5.3	Loss of All Feedwater Flow	AOO	L3 SCRAM	DPS will SCRAM on L3
15.2.6	AOO Analysis of Infrequent Events Summary (Event Category)			
15.2.7	COL Information			
	Not Applicable			
15.3	Analysis of Infrequent Events (Event Category)			
15.3.1	Loss of Feedwater Heating With Failure of Selected Control Rod Run-In	Infrequent Event	SCRAM not credited. NO DPS SCRAM	Failure of both SCRRI and RPS unlikely, If both fail, percentage of fuel may fail. Doses within 10% of 10 CFR 100 guidelines (2.5 REM).
15.3.2	Feedwater Controller Failure – Maximum Demand	Infrequent Event	L8 SCRAM	Incredible event but DPS will SCRAM on L8
15.3.3	Pressure Regulator Failure – Opening of All Turbine Control and Bypass Valves	Infrequent Event	L3 SCRAM	Level swells initially but delayed SCRAM on low level from DPS (L3).
15.3.4	Pressure Regulator Failure – Closure of All Turbine Control and Bypass Valves	Infrequent Event	High reactor pressure SCRAM	Incredible event but DPS will SCRAM on high pressure
15.3.5	Generator Load Rejection With Total Turbine Bypass Failure	Infrequent Event	High reactor pressure SCRAM	Incredible event but DPS will SCRAM on high pressure
15.3.6	Turbine Trip With Total Turbine Bypass Failure	Infrequent Event	High reactor pressure SCRAM	Incredible event but DPS will SCRAM on high pressure

Sect	Description	Event Class	Diverse I&C system	Comments
15.3.7	Control Rod Withdrawal Error During Power Refueling	Infrequent Event	No Diverse I&C required	No DPS action
15.3.8	Control Rod Withdrawal Error During Power Startup	Infrequent Event	No Diverse I&C required	No DPS action
15.3.9	Control Rod Withdrawal Error During Power Operation	Infrequent Event	No Diverse I&C required:	No DPS action
15.3.10	Fuel Assembly Loading Error, Mislocated Bundle	Infrequent Event	No Diverse I&C required	No DPS action
15.3.11	Fuel Assembly Loading Error, Misoriented Bundle	Infrequent Event	No Diverse I&C required	No DPS action
15.3.12	Inadvertent SDC Function Operation	Infrequent Event	No significant impact.	SB&PC available to mitigate. Slow moving event most likely terminated by operator (for tightly controlled startup scenario).
15.3.13	Inadvertent Opening of a Safety-Relief Valve	Infrequent Event	High suppression pool temperature SCRAM	DPS will also SCRAM on high suppression pool temperature
15.3.14	Inadvertent Opening of a Depressurization Valve	Infrequent Event	High drywell press SCRAM	DPS will also SCRAM on high drywell pressure
15.3.15	Stuck Open Safety-Relief Valve	Infrequent Event	Suppression pool temperature SCRAM	DPS will also SCRAM on high suppression pool temperature
15.3.16	Liquid Containing Tank Failure (COL applicant scope)	Infrequent Event	No diverse I&C required	No DPS action
15.3.17	COL Information			Not Applicable
15.4	Analysis of Accidents (Event Category)			
15.4.1	Fuel Handling Accident	Accident	No diverse I&C required	No DPS action

Sect	Description	Event Class	Diverse I&C system	Comments
15.4.2	Loss-of-Coolant Accident Containment Analysis	Accident	L3 SCRAM/Hi drywell pressure SCRAM Diverse ESF/ECCS actuation	DPS will SCRAM on reactor level, drywell pressure and initiate (ECCS) Automatic Depressurization System (ADS)/Gravity Driven Cooling System (GDCCS), SLCS, etc. Worst case dose may challenge 10 CFR 100 guidelines. Need confirmatory analysis. Diverse containment isolation may be required.
15.4.3	Loss-of-Coolant Accident ECCS Performance Analysis	Accident	L3 SCRAM Diverse ESF/ECCS actuation	Refer to 15.4.2.
15.4.4	Loss-of-Coolant Accident Inside Containment Radiological Analysis	Accident	L3 SCRAM Diverse ESF/ECCS actuation	Refer to 15.4.2.
15.4.5	Main Steamline Break Accident Outside Containment	Accident	L3 SCRAM Diverse ESF/ECCS actuation	DPS SCRAMs on low level (L3). Diverse containment/MSIV closure may be required to limit radiological consequences. Release may challenge 10 CFR 100 guidelines. Confirmatory analysis required. MSIV closure on flow may be required.
15.4.6	Control Rod Drop Accident	Accident	No diverse I&C required	No DPS action
15.4.7	Feedwater Line Break Outside Containment	Accident	L3 SCRAM Diverse ESF/ECCS actuation	DPS will SCRAM on reactor level Worst case dose will not challenge 10 CFR 100 guidelines.
15.4.8	Failure of Small Line Carrying Primary Coolant Outside Containment	Accident	L3 SCRAM Diverse ESF/ECCS actuation	No DPS action unless level gets to L3. If level gets really low (L1) then DPS will operate diverse ECCS. Diverse containment. Line break bounded by larger breaks. Manual containment isolation available. Aberrant indication (radiation available to alert the operator). Excess flow check valves should limit release of coolant. Dose within 10 CFR 100 guidelines.

Sect	Description	Event Class	Diverse I&C system	Comments
15.4.9	RWCU/SDC System Line Failure Outside Containment	Accident	L3 SCRAM Diverse ESF/ECCS actuation Possible operator action required.	No DPS action unless level gets to L3. If level gets really low then DPS will operate diverse ESF. May require operator action to remotely isolate or locally isolate based on conditions. Worst case dose may challenge 10 CFR 100 guidelines. (Possible inclusion of differential flow sensor for DPS leak isolation function)
15.4.10	Spent Fuel Cask Drop Accident	Accident	No diverse I&C required	No DPS action
15.4.11	COL Information			Not Applicable
Category 15.5 Special Event Evaluations - (Event Category) - Events not evaluated				