GE-Hitachi Nuclear Energy Americas LLC

James C. Kinsey
Project Manager, ESBWR Licensing

PO Box 780 M/C A-55
Wilmington, NC 28402-0780
USA

T 910 675 5057
F 910 362 5057
jim.kinsey@ge.com

MFN 07-475

Docket No. 52-010

August 31, 2007

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

Subject: **Topical Report NEDO-33251, Revision 1, ESBWR I&C Diversity and Defense-In-Depth Report, August 2007**

The purpose of this letter is to provide the GE-Hitachi (GEH) Licensing Topical Report (LTR) NEDO-33251, "ESBWR I&C Diversity and Defense-In-Depth Report," Revision 1. Enclosure 1 contains NEDO-33251, which describes the type of diversity that exists among the four echelons of defense-in-depth for the ESBWR and identifies dependencies among the echelons. Revision 1 includes a discussion of the QNX operating system associated with the safety-related Video Display Units (VDUs) and the non-safety-related Mark VIe controllers. The discussion concludes that there are no common cause failure concerns associated with this operating system.

Enclosure 2 contains the ESBWR DCD Tier 2 markups associated with this LTR. These markups will be included in ESBWR DCD Revision 5.

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

Sincerely,

Kathy Sedney for

James C. Kinsey
Project Manager, ESBWR Licensing

D068
NRO

Enclosures:

1. Licensing Topical Report (LTR) NEDO-33251, "ESBWR I&C Diversity and Defense-In-Depth Report," Revision 1
2. ESBWR DCD Tier 2 markups

cc: AE Cubbage USNRC (with enclosures)
RE Brown GEH/Wilmington (with enclosures)
GB Stramback GEH/San Jose (with enclosures)
eDRF 0000-0073-2894

MFN 07-475

Enclosure 1

Licensing Topical Report (LTR) NEDO-33251,
"ESBWR I&C Diversity and Defense-In-Depth Report"
Revision 1

GE-Hitachi
Nuclear
Energy

NEDO-33251
Revision 1
Class I
eDRF# 0000-0073-2894
August 2007

LICENSING TOPICAL REPORT

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

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

Table Of Contents

List of Tables

List of Figures

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
AMS	Alarm Management System
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
CMS	Containment Monitoring System
COL	Combined Operating License
CRD	Control Rod Drive
CRHS	Control Room Habitability System
DAS	Data Acquisition System
DATALINK	A communication path between two systems – almost always by fiber-optic cable.
DC	Direct Current
DCD	Design Control Document
DCIS	Distributed Control and Information System
DPS	Diverse Protection System
DPV	Depressurization Valve
DS	Deluge System
ECCS	Emergency Core Cooling System
EQV	Equalizing Valve
EMI/RFI	Electromagnetic Interference/Radio Frequency Interference
EOF	Emergency Offsite Facility
EPA	Electric Protection Assembly
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Feature (ESF) Actuation System
FAPCS	Fuel and Auxiliary Pools Cooling System
FB	Fuel Building
FMCRD	Fine Motion Control Rod Drive
FOAKE	First-of-a-Kind Engineering

FW	Feedwater
FWCS	Feedwater Control System
GATEWAY	A device representing a "translator" between two datalinked systems.
GDC	General Design 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	Local Power Range Monitor
Mark*VIe	General Electric Dual or Triply redundant controller
MCC	Main Control Console
MCR	Main Control Room
MRBM	Multi-Channel Rod Block Monitor
MSIV	Main Steam Isolation Valve
N-DCIS	Nonsafety-related Distributed Control and Information System
NDL	Nuclear Data Link
NI	Nuclear Island
NMS	Neutron Monitoring System
NRC	Nuclear Regulatory Commission
NUMAC	Nuclear Measurement Analysis and Control
PAS	Plant Automation System
PCCS	Passive Containment Cooling System
PCF	Plant Computer Function(s) (Sub-system of N-DCIS)
PIP	Plant Investment Protection
PLC	Programmable Logic Controller
PRA	Probabilistic Risk Assessment
PRHR	Passive Residual Heat Removal
PSWS	Plant Service Water System
Q-DCIS	Safety-related Distributed Control and Information 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
RPV	Reactor Pressure Vessel
RSS	Remote Shutdown System
RTIF	Reactor Trip and Isolation Function
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
SPDS	Safety Parameter Display System (Sub-system of N-DCIS)
SRI	Select Rod Insert
SRNM	Source Range Neutron Monitor
SRV	Safety-Relief Valve
SSC	Shift Supervisor Console
SSLC	Safety System Logic and Control
TBV	Turbine Bypass Valve
TCCW	Turbine Component Cooling Water
TGCS	Turbine Generator Control System
TMI	Three Mile Island
TMR	Triple Modular Redundant
TSC	Technical Support Center
VDU	Video Display Unit (in this document the VDUs are assumed to be touch screen but further HFE analysis may dictate other operator pointing devices)
WDP	Wide Display Panel

* Trademark of General Electric Company

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 the understanding of the report text, instrumentation and control architecture, and conformance to guidelines. The definitions and clarifications may vary from corresponding definitions in Reference 1 because of development and evolution of the ESBWR I&C architecture. *Definitions verbatim from Reference 1 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 Design Control Document (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 a significant amount of radioactive material." (Standard Format, Section 15, "Accident Analysis," NRC Reg. Guide 1.70).

Section 15 of the Reference 3. provides the definition and discussion of Accidents.

Block

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

detailed examination of internal failure mechanisms while examining system behavior under reasonable assumptions of failure containment.

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

Channel

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

Common-Mode (or -Cause) Failure

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

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

Defense-in-Depth

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

Diversity

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

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

Echelons of Defense

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

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

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

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

2. Reactor Trip or SCRAM System [Reactor Protection System (RPS)]

   "The reactor trip echelon is that safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion. It consists of instrumentation for detecting potential or actual excursions, means for rapidly and completely inserting the reactor control rods, and may also include certain chemical neutron moderation systems (e.g., boron injection)."

   The automatic reactor trip functions performed by the reactor trip echelon of defense are included in the safety-related control systems (Q-DCIS); specifically the RPS. As will be later described, the nonsafety-related Diverse Protection System (DPS) also provides automatic and manual reactor trip capabilities.

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

   "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 Safety System Logic and Control (SSLC)/ESF echelon of defense are included in the Q-DCIS. The nonsafety-related DPS also provides automatic actuation capability for a subset of Emergency Core Cooling System (ECCS) component actuations. The ESBWR is a passive plant and does not require emergency generators, motors, or pumps to perform its ECCS functions.

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

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

   Monitoring and indication functions are provided by both the N-DCIS and Q-DCIS. The safety-related manual reactor trip and manual ESF actuation functions performed by the monitoring and indication echelon of defense are included in the Q-DCIS. The nonsafety-related DPS also provides manual reactor trip and a subset of manual ESF actuation capabilities.

Instrumentation System

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

In this report, the instrumentation system includes the following systems in the I&C architecture:

- N-DCIS or cabinets including:
  - Plant Investment Protection A,
  - Plant Investment Protection B,
  - DPS Severe Accident (deluge) Control System,
  - Balance of Plant Control, and
  - Plant Computer Functions (Sub-system of N-DCIS).

- Q-DCIS or cabinets including:
  - Reactor Trip and Isolation Function (RTIF), (the RTIF cabinet includes the RPS and the Main Steam Isolation Valve (MSIV), Leak Detection and Isolation System (LD&IS.)
  - Anticipated Transients Without Scram/Standby Liquid Control System - (ATWS/SLCS) (also includes some nonsafety-related functions, the safety-related functions of ATWS/SLCS are physically located in the RTIF cabinet.)
  - SSLC/ESF [includes ECCS (Isolation Condensers, Automatic - Depressurization System, Gravity-Driven Cooling System and Standby - Liquid Control System), control room habitability system, Non-MSIV - LD&IS and the safety-related functions of the Containment Monitoring System (CMS.)

1 INTRODUCTION

1.1 PREFACE

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

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

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

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

In December 1994, the Nuclear Regulatory Commission (NRC) published Reference 1, which describes a deterministic method of analyzing computer-based nuclear reactor protection systems that identifies and evaluates design vulnerabilities to CMF. The ESBWR I&C system functions follow the SBWR instrumentation and control systems and the ABWR hardware and software applications, which were designed and analyzed before Reference 1 was published. As with the SBWR design, PRA methods are used for the analysis of systems used to provide diversity and defense-in-depth for ESBWR, rather than the deterministic methods described in Reference 1. These PRA methods are consistent with Reference 1 and allow the designers to concentrate on situations that are the largest potential contributors to the predicted core melt frequency.

1.2 ARCHITECTURE OVERVIEW

The Q-DCIS is a safety-related I&C system that is included in the ESBWR distributed control and information systems architecture to address the anticipated operational occurrences and accidents outlined and described in Chapter 15 of the ESBWR Design Control Document (DCD) (Reference 3). The Q-DCIS design complies with NEDO-33245P – Software Quality Assurance Plan (Reference 4) and specifically meets plant licensing requirements by including design features such as:

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

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

The DPS is a nonsafety-related I&C system whose functions augment those of the Anticipated Transients without SCRAM/Standby Liquid Control (ATWS/SLC) system included in the ESBWR and the ABWR. The DPS enables the ESBWR DCIS to meet reliability goals, when the Q-DCIS is assumed to fail as a result of postulated failures beyond design basis, such as a software CMF.

1.3 SCOPE

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

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

Reference 1 defines echelons of defense as:

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

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

1.4 SUMMARY AND CONCLUSIONS

1.4.1 Compliance with NUREG-0493

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

1.4.2 Compliance with NUREG/CR-6303

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

1.4.3 Meeting Probabilistic Safety-Related Goals

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

2 ESBWR INSTRUMENTATION AND CONTROL ARCHITECTURE / SYSTEMS DESCRIPTION

2.1 ARCHITECTURE DESCRIPTION

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

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

Almost all communication to/from the field Remote Multiplexing Units (RMUs) is by fiber and all communication from the DCIS rooms to the main control room (MCR) safety-related and nonsafety-related Video Display Units (VDUs) are via fiber. The few hard-wired exceptions are for signals like main turbine trip or reactor SCRAM signals. These MCR considerations are important because the communications protocol is such that a failure of a fiber will not cause erroneous operation nor affect the continued operation of all automatic safety-related or nonsafety-related systems. Likewise, touch screen operation of the VDUs 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 Measurement Analysis and Control (NUMAC) derived functions (four divisions)
  - Reactor Protection System (RPS),
  - Main steam isolation valve (MSIV),
  - Leak Detection and Isolation System (LD&IS), and
- Neutron Monitoring System (NMS).

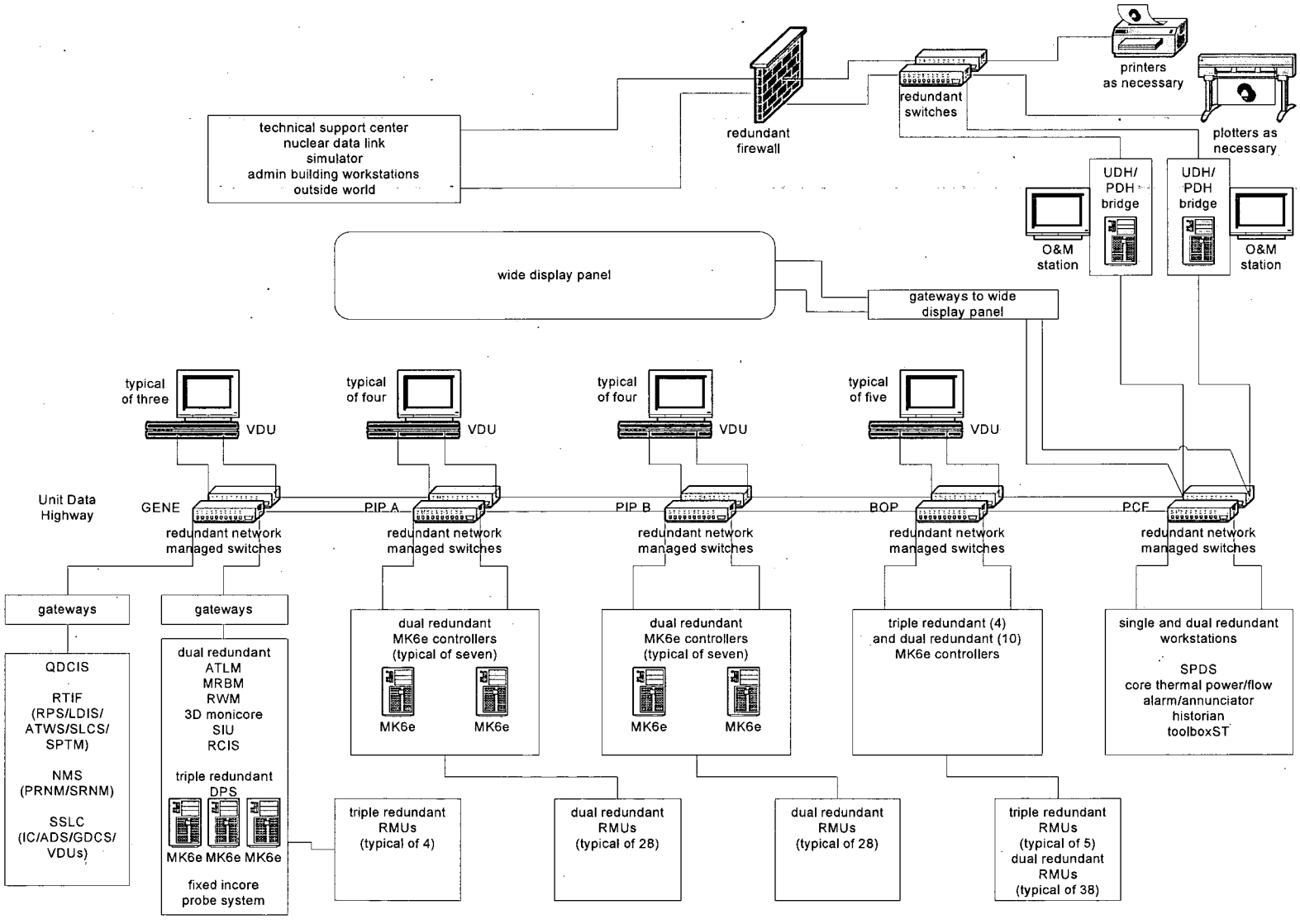
(Non-microprocessor based ATWS/SLCS – this logic may include simple microprocessors but they will not be user programmable nor use the same hardware/software platform as NUMAC.)

- Safety System Logic and Control (SSLC)/ESF Emergency Core Cooling System (ECCS) functions (four divisions):
  - Isolation Condenser System (ICS),
  - Safety Relief Valve (SRV),
  - Automatic Depressurization System (ADS),
  - Gravity-Driven Cooling System (GDCS), and
  - Standby Liquid Control (SLC) System, and the isolation function performed by the LD&IS (non-MSIV).

Nuclear functions [3D-Monicore, Automatic Thermal Limit Monitor (ATLM), Rod Block Monitor (RBM), Rod Worth Minimizer (RWM), Automatic Fixed in Core Probe (AFIP), Rod Control and Information System (RC&IS)]

- PIP A functions,
- PIP B functions,
- Balance of Plant (BOP) functions,
- Plant Computer Functions (PCF) [Safety Parameter Display System (SPDS), Alarm Management System, Historian, etc.], and
- 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-33226P – Software 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 N-DCIS,
- The alarm management of safety-related systems on the N-DCIS (through isolated data links from the four divisions (control of Q-DCIS from N-DCIS is not possible through the data links),
- Dual and triple redundancy for all important PCF and for control of power generation systems,
- Segmented PIP systems, and
- A high quality nonsafety-related DPS that can perform a subset of reactor scrams, isolations, and ESF actuations without affecting or interfering with its safety-related counterparts.

The ESBWR DCIS use all the methodologies mandated 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:

- Q-DCIS cabinets including:
  - Reactor Trip and Isolation System (RTIF) cabinet [includes RPS and (MSIV), LD&IS].
  - NMS [including APRMs, LPRMs and Source Range Neutron Monitor (SRNMs)].
  - ATWS/SLCS (also includes some nonsafety-related functions) (this function is physically located in the RTIF cabinets).
  - ESF/ECCS [(includes ICS, ADS, GDCS, SLCS, Non MSIV, LD&IS, Control Room Habitability System (CRHS) and Containment Monitoring System (CMS).]

- N-DCIS cabinets including:
  - PIP A,
  - PIP B,
  - DPS,
  - Severe Accident (deluge) Control System,
  - BOP Control, and
  - PCF (Subsystem of N-DCIS).

As indicated in Figure 2, within the Q-DCIS, the RPS, LD&IS (MSIV) and NMS use hardware and software different from the SSLC/ESF processors. In turn both the RPS and SSLC/ESF DCIS systems use hardware and software different from the N-DCIS systems, specifically

including the DPS, which provides a completely diverse backup design to most protection functions in the Q-DCIS. The severe accident deluge system is also diverse from both Q-DCIS and N-DCIS.

On the N-DCIS side, the important nuclear instrumentation and control systems, such as DPS, use triply redundant 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 I&C systems.

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

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

The operator interface functions of the DCIS define the arrangement of the MCR, the layout of the DCIS equipment on the main bench boards (and Remote System Shutdown (RSS) panels) and dictate 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 defined in the appropriate I&C sections of the ESBWR Design Control Document (Reference 3).

Figure 4 is a functional representation of the MCR panels. The design is contingent upon final HFE analyses. There are three main control room panels – the wide display panel (WDP) 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 WDP houses the plant mimic, large variable display, various nonsafety-related VDUs, synchronizing equipment for the main and diesel generators and fire protection system indicators and alarms. The WDP also houses the plant annunciators, generally one per system, which are part of the AMS.

The Main Control Console (MCC) is the primary operator interface, and also houses compartmentalized (one per division) sections housing VDUs and manual switches for ECCS equipment and ECCS/RPS bypass and initiation. The remainder of the MCC houses the nonsafety-related VDUs and hard controls [for example, main turbine trip, control rod insert/withdraw (in manual mode)] that are used for normal plant operation. Although the nonsafety-related displays are segmented in that they are driven by the PIP A, PIP B and BOP

portions of the N-DCIS, in normal operation they appear "seamless" to the operator and all displays can control and monitor all nonsafety-related equipment that the operator selects. The segmentation of the nonsafety-related DCIS allows operation of each segment independently should another segment be lost (the "uplinks" between the segmented network switches are by fiber).

Both the WDP and MCC have four divisional VDUs from which safety-related systems can be both monitored and controlled. The safety-related VDUs, although using touch screen technology and having the same operator "look and feel", use technology diverse from that of the nonsafety-related VDUs, and are completely isolated from the N-DCIS.

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

The bench boards also contain the hard control and bypass switches that 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 ESBWR raceways, conduits and duct banks fully support the divisional and non-divisional separation criteria. The four divisions of RPS and NMS cabling are always in four separated raceways/conduits and the very low level signals on LPRM and SRNM cables are further segregated from all other wiring. The signals representing the Hydraulic Control Unit (HCU) solenoid currents in division 1 and 2 are also further subdivided into four "SCRAM" groups (per division) and segregated from each other and all other plant wiring.

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

Figure 2 Hardware/Software (Platform) Diversity

Safety	**Safety-Related**		**Nonsafety-Related**				
Category	**Q-DCIS**		**N-DCIS**				
System Families	**RPS NMS**	**SSLC/ ESF**	**DPS**	**Nuclear Control Systems**	**Other N-DCIS Systems**	**PCF**	**Severe Accident**
Architecture	**NUMAC**	**TRICON**	**MK6e (TMR)****	**MK6e (TMR)****	**MK6e (dual redundant)**	**workstations**	**PLCs**
Systems/ Subsystems	RPS LD&IS (MSIV) NMS ATWS/ SLCS*	ICS ADS GDCS SLCS LD&IS (non MSIV)	RPS SSLC/ ESF LD&IS backup	FWC, SB&PC, T/G Control, PAS (automation)	PIP A, PIP B, Balance of Plant (power generation)	HMI (VDUs), Alarm Management SPDS, Historian, 3D Monicore	Deluge System (GDCS subsystem)
Diversity Strategy	* non programmable diverse from RPS hardware/software		** triple modular redundant				
Within Safety-Related Controls							
Safety-Related vs DPS							
Safety-Related vs Nonsafety-Related							

Figure 3 ESBWR Sensors and Power Diversity

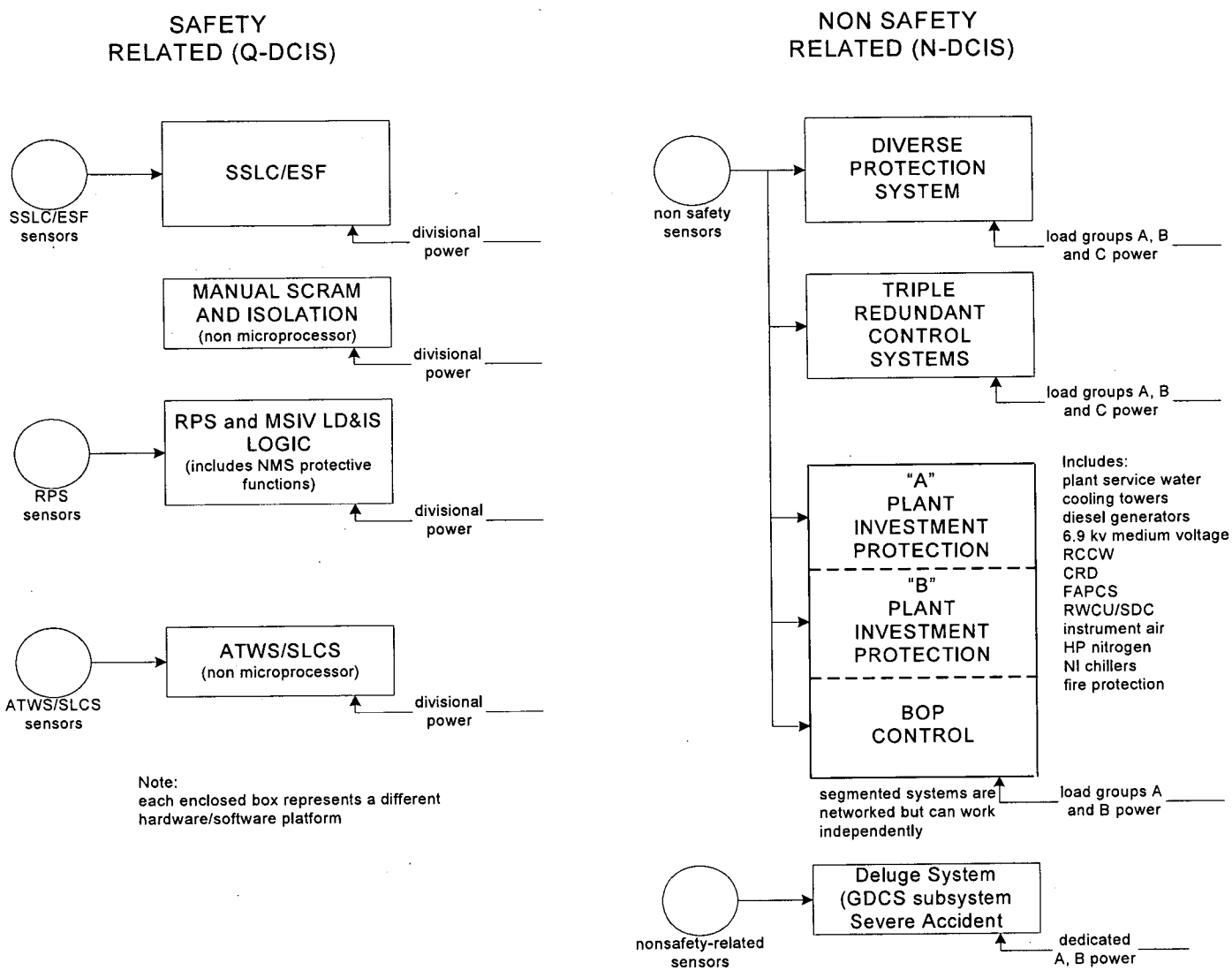

SAFETY
RELATED (Q-DCIS)
SSLC/ESF
sensors
SSLC/ESF
divisional
power
MANUAL SCRAM
AND ISOLATION
(non microprocessor)
divisional
power
RPS
sensors
RPS and MSIV LD&IS
LOGIC
(includes NMS protective
functions)
divisional
power
ATWS/SLCS
sensors
ATWS/SLCS
(non microprocessor)
divisional
power
Note:
each enclosed box represents a different
hardware/software platform
NON SAFETY
RELATED (N-DCIS)
non safety
sensors
DIVERSE
PROTECTION
SYSTEM
load groups A, B
and C power
TRIPLE
REDUNDANT
CONTROL
SYSTEMS
load groups A, B
and C power
"A"
PLANT
INVESTMENT
PROTECTION
"B"
PLANT
INVESTMENT
PROTECTION
BOP
CONTROL
Includes:
plant service water
cooling towers
diesel generators
6.9 kv medium voltage
RCCW
CRD
FAPCS
RWCU/SDC
instrument air
HP nitrogen
NI chillers
fire protection
segmented systems are
networked but can work
independently
load groups A
and B power
nonsafety-related
sensors
Deluge System
(GDCS subsystem
Severe Accident
dedicated
A, B power

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

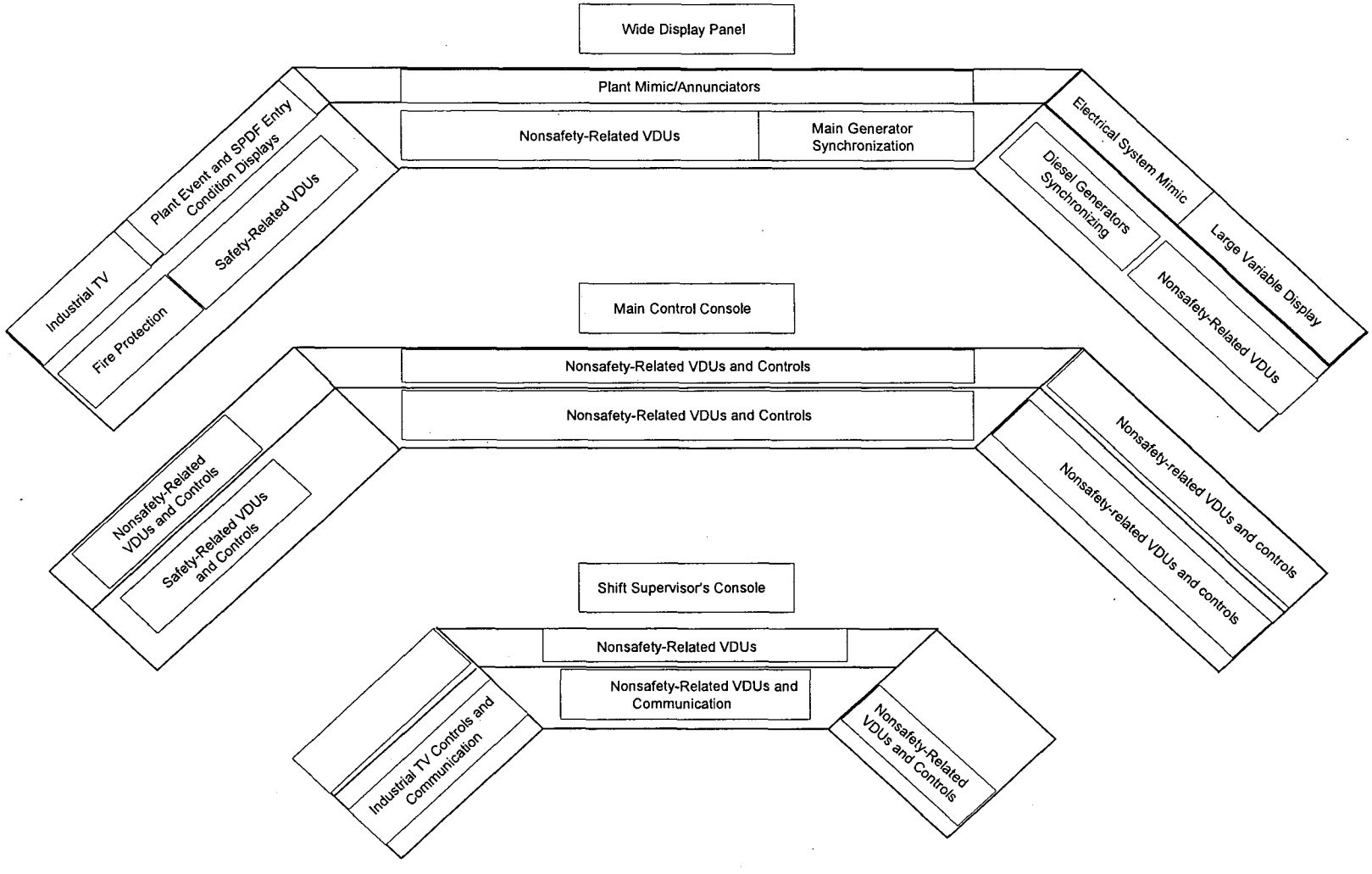
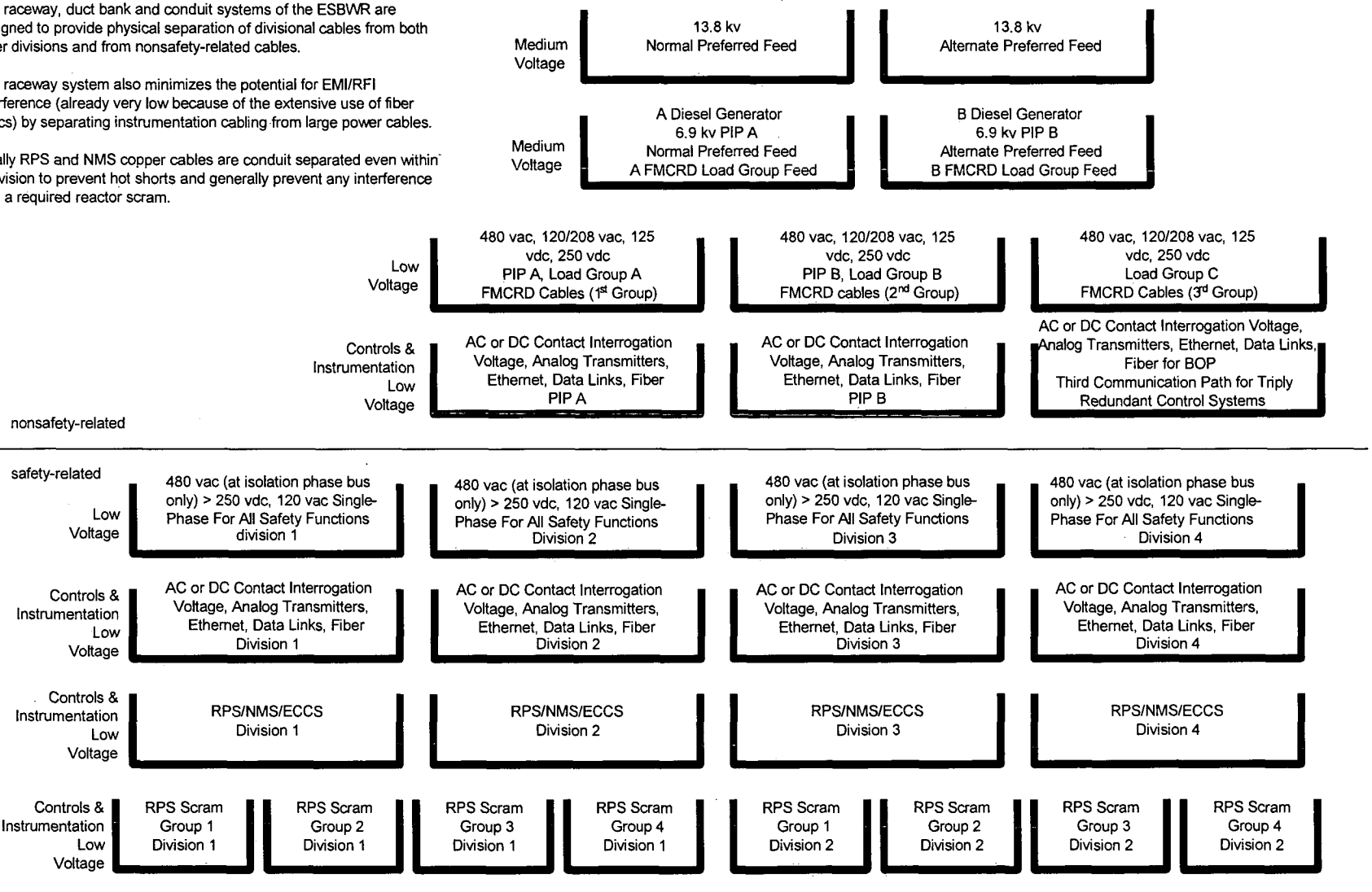


Figure 5 ESBWR DCIS and POWER Separation

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-RELATED DISTRIBUTED CONTROL AND INFORMATION SYSTEM OVERVIEW

The Q-DCIS consists of the RPS (including MSIV isolation), the NMS and the SSLC/ESF. 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 (Reference 13). The two-out-of-four logic associated with the RPS, LD&IS, NMS and SSLC/ESF, and the simplified ECCS systems of the ESBWR allow the plant to be designed as "N-2"; specifically any two divisions can accomplish the safety-related trip and ECCS functions. N-2 is a significant element of the defense in depth design of the ESBWR DCIS.

The RPS and NMS systems are implemented on a NUMAC hardware/software platform and are sub functions of the Q-DCIS; the general relationship is shown in Figure 6. (There are also nonsafety-related portions of NMS not implemented on NUMAC platforms.) The RPS controllers/logic are located in the RTIF cabinet (one per division in separate Q-DCIS rooms) that combines the RPS, LD&IS (for MSIVs and drains only) and ATWS/SLCS functions. Although all equipment located in the RTIF cabinet is appropriate to the division and everything in the cabinet is powered by the appropriate divisional uninterruptible and battery power, the 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 other Boiling Water Reactor (BWR) SCRAM logic and hardware (although many of these features were included in the ABWR design); these include:

- Per parameter trip (specifically there must be (for example) two un-bypassed level trips to SCRAM, a pressure trip and a level trip will not cause a SCRAM).

- No operator manipulation of the division of sensors and/or division of logic bypass, nor any operation of the RPS back panel inoperable switches can reduce SCRAM logic redundancy to less than "any two un-bypassed same parameters in trip will cause a SCRAM". Only one division at a time can be physically bypassed. The RPS (and MSIV LD&IS) is N-2 to SCRAM/isolate.

- Communication with the nonsafety-related DCIS is one-way (Q-DCIS to N-DCIS) through fiber; the loss of this communication does not affect RPS functionality.

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

- All signals are actively transported such that "fail safe" is not a "1" or a "0" but rather "trip on loss of communication". As a result, loss of communication from another division is interpreted as a trip signal (unless that division is bypassed) and loss of communication with a bypass joystick switch is interpreted as "no bypass".

- RPS (and Q-DCIS) logic is powered by divisional redundant (uninterruptible AC 120V) power supplies that are backed by redundant batteries; additionally the systems are backed up by offsite power and either of the two diesel generators.

- The Hydraulic Control Unit (HCU) solenoid power is local to the Reactor Building (RB) and switched by fiber driven two-out-of-four logic from the RPS (RTIF) cabinet in the Control Building (CB). This avoids the long distance voltage drops to the solenoids in the older BWR designs and eliminates (along with using monitored, safety-related inverters for solenoid power) the need for Electric Protection Assemblies (EPAs). Loss of communication from the CB RTIF cabinets is interpreted as a trip.

- The hardware, software and solenoid switching for the RPS is both diverse and separate from the DPS.

The SSLC/ESF DCIS is implemented on a TRICON hardware/software platform that is a sub function of the Q-DCIS. For diversity, the SSLC/ESF ECCS and non-MSIV LD&IS logics use different sensors and are implemented on a hardware/software platform different from that of RPS/(MSIV) LD&IS and the DPS. Since it is highly desirable to avoid the consequences of inadvertent actuation of ECCS (specifically automatic depressurization) and also important to reliably actuate ECCS when required, the SSLC/ESF ECCS logic is implemented on a triply redundant hardware/software platform per division. The SSLC/ESF ECCS functions are described in more detail in ESBWR Design Control Document (Reference 3), but include the following systems controlled by the SSLC/ESF DCIS:

- ADS (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 bring the reactor pressure to a low enough value for the GDCS to work.

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

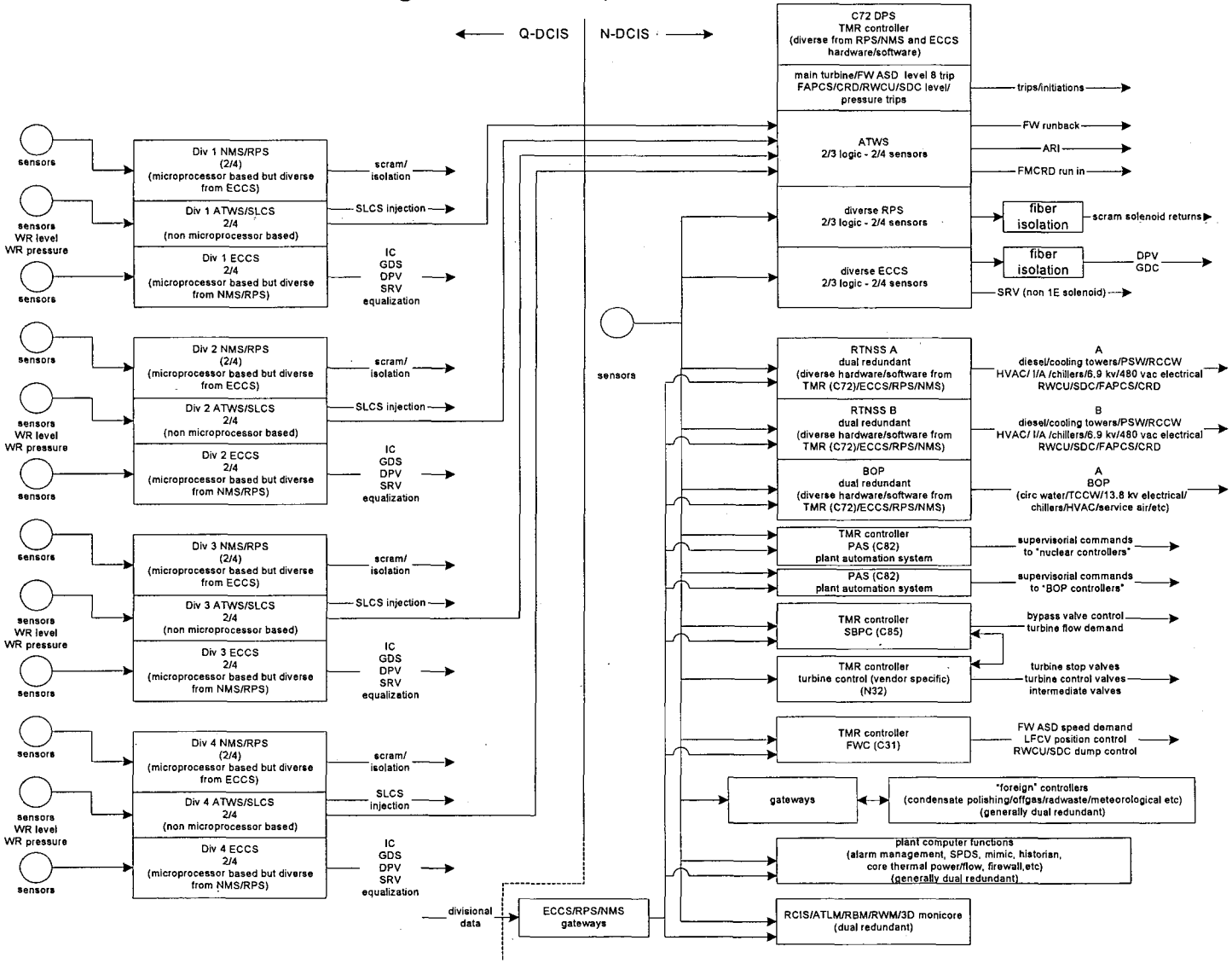
- Suppression Pool Subsystem of GDCS (also Squib-Actuated Valves) - These equalizing valves allow the water stored in the suppression pool to drain into the depressurized RPV well after a postulated accident event to compensate for long term reactor coolant boil-off.

- SLC (also Squib Actuated Valves) – These valves allow soluble boron to be injected into the RPV from two accumulator tanks to provide additional coolant inventory.

- ICS - The four isolation condensers are passive heat exchangers with Isolation Condenser/Passive Containment Cooling System (IC/PCCS) pool water on one side and reactor steam on the other. Each IC, once initiated by either of two valves that open a condensate return path to the reactor, condenses reactor steam and returns it to the RPV. The system operates at high reactor pressures and provides cooling and depressurization without reactor coolant inventory loss.

- LD&IS - The ESF/ECCS processors perform the inboard and outboard isolation function for all isolation valves other than the MSIVs and selected steam line drain valves.

Figure 6 NMS/RPS, SSLC/ESF and DPS



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

Per division, a two-out-of-three 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 two-out-of-three logic and two-out-of-four agreement) can operate the actuator; however the actuator cannot be operated by a single failure within the division.

2.3 NONSAFETY-RELATED DISTRIBUTED CONTROL AND INFORMATION SYSTEM OVERVIEW

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

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

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

- Diesel Generators,
- 6.9 KV PIP Busses,
- Plant Service Water System (PSWS),
- Reactor Closed Cooling Water (RCCW),
- Reactor Building (RB) 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, and
- RB, Fuel Building (FB), Control Building (CB), Switchgear Building Heating Ventilation and Air Conditioning (HVAC).

The PIP systems are organized mechanically into two trains (i.e., pump "A" and pump "B") with each train powered by a different diesel generator and 6.9 KV bus. The two trains are controlled by a deliberately segmented N-DCIS, so that the RMUs, control processors and displays that

operate PIP A systems are separate from those operating PIP B systems. The segmentation is implemented using managed network switches; approximately one third of the nonsafety-related control room displays are assigned to the PIP A and the PIP B switches. Normally any control room nonsafety-related display can control/monitor any PIP or BOP system but the loss of either PIP system DCIS or the BOP DCIS will not affect the operation of the remaining PIP system or its displays.

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

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

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

The N-DCIS supports the severe accident deluge 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 underneath the RPV should all other core cooling and shutdown systems fail. The valves are actuated by sensed containment floor high temperatures attributable to the postulated core and vessel melt.

2.4 DIVERSE PROTECTION SYSTEM OVERVIEW

The DPS is a 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 SSLC/ESF. Specifically, the DPS uses hardware, software and power that are different (diverse) from those used by the safety-related systems. The DPS is described further in Chapter 7 of Reference 3.

The DPS system performs several major/minor functions:

- It SCRAMs the plant using a subset of the safety-related RPS parameters.
- It closes the MSIVs on receipt of a high steam flow signal, low RPV water level and low reactor pressure.

- It initiates Select Rod Insert (SRI) for turbine trips and load rejections to rapidly reduce power.
- It initiates selected ECCS.
- It transmits ATWS/SLCS logic signals to cause the Feedwater Control System (FWCS) to run back feedwater flow and is diversely able to activate SLCS.
- It trips the feedwater pumps on RPV water level 9 (after they have been run back to zero flow on RPV water level 8).

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

- Detection of high or low RPV water level,
- Detection of high reactor pressure,
- Detection of high drywell pressure,
- Detection of high suppression pool temperature, and
- 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 two-out-of-three SCRAM decision of the triply redundant processors is sent via three isolated fibers to the SCRAM timing panel where they are two-out-of-three voted to open all the solenoid return power switches. The operator also has the ability to initiate a manual DPS SCRAM from either hard switches or the DPS touch screen display.

The DPS is also able to initiate:

- The isolation condensers on low RPV water level or MSIV closure,
- The ADS (SRVs and DPVs) on low RPV water level,
- The GDCS squib valves on low RPV water level, and
- The SLC System squib valves on low RPV water level.

The two-out-of-four sensor logic and the two-out-of-three processing logic is similar to the SCRAM logic and the operator also has the ability to initiate the above actions from the DPS touch screen display. The ECCS subsystems that use three or four divisional solenoids to initiate flow (SRVs and ICs), also have a fourth or fifth nonsafety-related solenoid to also cause initiation from the DPS (after a two-out-of-three vote). The ECCS systems, which use squibs, also use a DPS actuated squib initiator that is electrically isolated from the safety-related initiators on the same valve. Although the DPS does not provide input to all squib divisions, all squib valves can be opened by the DPS logic.

The DPS also provides the following major isolations:

- Closure of the MSIVs on detection of high steam flow, low reactor pressure or low RPV water level,
- Closure of the IC isolation valves on high steam flow or high condensate flow,
- Closure of the RWCU/SDC isolation valves on high differential flow using two-out-of-four sensor logic and 2/3 processing logic, and

- Closure of the feedwater isolation valves on high drywell pressure and high feedwater line differential pressure.

The DPS does not violate the general rule of avoiding communication between nonsafety-related systems and safety-related systems. The DPS has its own "actuators" (SRV and IC solenoids or 120 VAC HCU solenoid return switches). The DPS does not interface with the RPS or ECCS logic or processors. For both RPS and ECCS functions, the failure of the DPS cannot prevent the Q-DCIS from performing its safety-related functions and the communication path from Q-DCIS to N-DCIS is always by fiber.

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

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

2.5 PCF (PLANT COMPUTER FUNCTIONS) OVERVIEW

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

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

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

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

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

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

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

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

Table 1 ESBWR Instrumentation and Control Echelons of Defense

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

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

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/ESF, ATWS/SLCS	2/4 voting logic, Load Drivers, HCU SCRAM Solenoids, Backup SCRAM Solenoids, SSLC/ESF 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/ESF (all Diverse from Reactor Trip Functions)	2/3 Logic per Division, 2/4 Divisional Voting Logic, Load Drivers, Solenoids, Squib Valves	Manual Switches through SSLC/ESF Logic, some Hardwired Switches
	Diverse	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 SLC System, 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/ESF	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 I&C architecture that provide redundant design, fail-safe design, and self-diagnostics/failure detection and repair. Section 5 discusses design diversity.

3.2 DEFINITION OF COMMON-MODE FAILURES

For the purpose of this report, Common-Mode Failures (CMFs) are considered to be sets of causally related failures that occur within a limited time, and fall outside of system design capabilities for detection or mitigation of those failures; the limited time is because simultaneous failures of diverse platforms 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 I&C architecture that redundant design is ineffective in enabling the system to tolerate them.
- The failures are such that fail-safe design is ineffective in enabling the system to tolerate them.
- The failures are undetectable, or they occur within a sufficiently short time that neither automatic nor manual responses are possible to enable the system to tolerate them.
- The failures occur simultaneously in only related hardware/software platforms.

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

- Diverse design exists 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 there is an automatic or manual response to the failure (most safety-related and nonsafety-related DCIS).

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

3.3 OVERALL INSTRUMENTATION AND CONTROL FAULT TOLERANT DESIGN FEATURES

The I&C architecture contains design features which enhance plant reliability and availability. However, these features also provide a degree of protection against CMFs, and, as a result,

decrease the probability that a CMF causes any portion of the ESBWR I&C architecture to be unable to respond to a transient, accident or plant fault. Among the design features that protect against failures, including CMF, are:

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

- Fail Safe/Fault Tolerant Design - Fail safe design features in the I&C 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 restore the plant to a safe condition following a single failure. Some 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 or manually restore the plant to a safe condition.

- Redundancy – Redundant design alone does not prevent CMFs, but the use of redundant subsystems can enable the plant to detect and respond to failures, including CMFs when sufficient time exists between occurrences of the individual failures. For example the four divisions of SSLC/ESF are not time synchronized nor dependent on other divisions for correct operation, which 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. When failures, including CMFs, occur, but sufficient time between them exists for detection and repair, modular design enables the redundant or diverse subsystems to be made available in response. The redundant components of the N-DCIS can be changed on line without affecting plant control, and divisional systems can be made inoperable and their chassis replaced on line without affecting plant operation.

- Use of Distributed Processing Architecture - I&C 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. When functional diversity exists in the I&C architecture, complete system failure may not occur as a result of CMF. For example. RPV water level and reactor pressure control are implemented in different cabinets with each cabinet using triply redundant processors. It is very unlikely that both functions would be lost simultaneously. The reactor pressure control function is implemented on the Q-DCIS by the SRVs and the isolation condensers (SSLC/ESF) and on the N-DCIS by the triply redundant Steam Bypass and Pressure Control (SB&PC) System; given the diversity of these systems it is highly unlikely that both reactor pressure control functions could be completely or simultaneously lost.

- Alarm Management System - The ESBWR AMS is capable of alerting the operator to not only process failures, but also DCIS failures including multiple failures, in other parts of

the I&C system. The main ESBWR AMS is part of the PCF of N-DCIS, which uses hardware and software different from the Q-DCIS.

- Continuous Self-Diagnostics - In the ESBWR I&C architecture, the subsystems continuously execute self-diagnostic software routines. Other self-diagnostic features, such as read-backs and watchdog timers continuously monitor the operation of critical subsystems. These self-diagnostic features are designed to detect and report hardware failures, enabling the operator to respond appropriately. For example, the Q-DCIS and most of the N-DCIS use redundant power supplies; a detected power supply failure allows diagnosis and replacement before the second power supply fails. An additional example is the adjustable speed drives in the feedwater system that continuously report back the received speed demand to the FWCS. When the FWCS senses a difference between transmitted and received demand, the adjustable speed drive is "locked up" (held at constant speed) until another drive can be brought on line.

- Test Subsystem - The test subsystem rapidly and consistently verifies system operation. The use of the test subsystem enhances the timely detection of all failures, including CMFs. The test subsystem also enhances the ability of plant personnel to quickly diagnose and repair detected failures.

- Circuit Isolation - Circuit isolation is used to electrically isolate segments of the I&C architecture and to prevent propagation of electrical faults caused by failures, including CMFs. For example all interdivisional communication (for two-out-of-four trip decisions) is via isolated fiber, similarly all safety-related to nonsafety-related communication is also via fiber; the fiber communication is monitored to implement both fail safe and self- diagnostic schemes. Both the safety-related and nonsafety-related DCIS communicate with their remote multiplexing (data acquisition) units using redundant fibers to prevent circulating ground currents that could adversely (and commonly) affect all DCIS in an area.

- Control of Setpoint and Tuning Adjustments - The I&C architecture has physical and administrative controls and multiple levels of security for access to setpoint and tuning adjustments. This helps to prevent CMF due to incorrect constants entered as a result of a maintenance error. For example access to nonsafety-related setpoints requires a higher level of security than simply operating a system. A safety-related example is the requirement to make NMS, RPS, or SSLC/ESF divisions inoperable before setpoints can be changed; the rendering of a division inoperable generates a plant alarm as required by RG 1.47 (Reference 11).

- Use of Engineering Units for Setpoints and Tuning Constants - Setpoints and tuning constants in the I&C architecture are entered in engineering units rather than as scaled values. This prevents a potential common-mode error by eliminating scaling calculations.

- Signal Selection Algorithms in the DCIS - All of the signals used for nonsafety-related plant control and power generation (for example hotwell level, feedwater heater level and reactor pressure) are used only after a validation process that combines the signals from multiple sensors. No single sensor (or its power supply) failure causes a transient or loss

of power generation; the failures are alarmed to allow timely repair. On the safety-related side, all four divisions use sensor trip data from all of the other divisions; unless one of the divisions is bypassed, the loss of any two divisions of like sensors causes an RPS trip. The loss of any single divisional sensor does not prevent two-out-of-four trip logic from occurring in any division – even the division with the failed sensor. Sensor data from the four divisions are continuously (not just for surveillance tests) compared and discrepancies are alarmed to the operator. The alarm warns the operator to repair the failed sensor in a timely manner.

- Physical Separation - Physical separation is provided between the four redundant Q-DCIS divisions of equipment. Likewise, the four divisions are separated from nonsafety-related systems and the DPS. There are four safety-related DCIS equipment rooms in the CB that provide physical, fire and electrical separation of the four divisions. Physical separation meets the requirements of IEEE-384 (Reference 6). The PIP A and PIP B N-DCIS systems are located in two physically separate N-DCIS rooms to provide the same physical, fire and electrical separation. The DPS controller is physically separated from PIP A, PIP B, and Q-DCIS. This physical separation provides protection from CMF induced by physical phenomena.

- Equipment Qualification - Equipment in the I&C architecture is qualified to environmental requirements, including temperature, humidity, radiation, vibration/seismic, electro-magnetic interference/radio frequency interference (EMI/RFI), Electrostatic Discharge (ESD) and surge withstand criteria commensurate with its safety-related classification and intended usage; specifically the safety-related DCIS components are qualified with the understanding that the passive nature of the ESBWR does not take credit for any active heat removal for 72 hours. The environmental qualification program provides assurance that physical phenomena do not introduce CMF unless design requirements are exceeded.

- Power - The Q-DCIS components are always powered with two power supplies and two separate power feeds appropriate to the division; the two feeds are two separate inverters. The component power supplies act as an "isolator" such that most power source problems are not propagated into the component and the redundancy allows the component to both continue operation and generate alarms should one power supply or power feed be lost. The N-DCIS components are also powered with two or three inverter (uninterruptible) power sources and are provided with the same protection. The inverter or regulating transformers prevent a single divisional or non-divisional power problem from causing the loss of safety-related functions or nonsafety-related control or power generation.

- Other Features - The I&C architecture also contains other design features such as ac power line protection and filtering, EMI/RFI design, and surge withstand networks at signal conditioning board inputs, which prevent failures from specific causes. These features assure that the causes of multiple failures exceed design and qualification test limits.

4 EVALUATION OF NUREG/CR-6303 GUIDELINES

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

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

4.1 IDENTIFYING SYSTEM BLOCKS - GUIDELINES 1 AND 5

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

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

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

4.2 DETERMINING DIVERSITY- GUIDELINE 2

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

1. Design Diversity
   In the nonsafety-related DPS, energize to trip or actuate logic is used. In the Q-DCIS, de-energize to trip or actuate logic is used for the RPS and NMS and energize to trip logic is used for the SSLC/ESF.

2. Equipment Diversity
   For the DPS, the hardware and software used to provide the automatic actions and sensor monitoring is diverse from the equipment used for safety-related functions in the Q-DCIS. For example, the DPS and RPS monitor different sensors and provide a reactor trip by operating the switches in the HCU SCRAM solenoid 120 VAC returns. This DPS action is diverse from the RPS load drivers used in the RPS NUMACs for reactor SCRAM.

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

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

5. Signal Diversity
   Signal diversity for specific events is provided within the safety-related level of the reactor trip and SSLC/ESF actuation echelons. The signals used to produce reactor trips and SSLC/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 Q-DCIS.

4.3 SYSTEM FAILURE TYPES - GUIDELINE 3

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

4.3.1 Type 1 Failure

Type 1 failures are those postulated in one echelon that result in a plant transient that requires a protection function to mitigate it. Generally, the postulated failure is assumed to occur in the control system echelon such that a plant transient occurs that results in an automatic reactor trip

or SSLC/ESF actuation. However, there are also postulated failures in the SSLC/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 a plant control or protection system and result in a plant transient requiring protective action. A substantial defense against these failures is provided by requiring that the control system echelon be single-failure proof and self-diagnosing such that only (postulated) common cause failures (CCF) are "credible".

4.3.2 Type 2 Failure

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

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

4.3.3 Type 3 Failure

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

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

4.4 ECHELONS OF DEFENSE - GUIDELINE 4

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

The DPS and the Q-DCIS provide the reactor trip echelon. The plant protection subsystems, the voting logic, dedicated data links, load drivers and HCU solenoids provide the reactor trip

function in the Q-DCIS. The backup SCRAM solenoids in the HCU solenoid air header and safety-related ATWS/SLC System 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 N-DCIS redundant control systems enable the plant to avoid the need to trip (including a 100% load rejection) by maintaining it within acceptable limits.

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

4.5 POSTULATED COMMON-MODE FAILURE OF BLOCKS – GUIDELINE 6

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

4.6 USE OF IDENTICAL HARDWARE AND SOFTWARE MODULES – GUIDELINE 7

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

4.7 EFFECT OF OTHER BLOCKS - GUIDELINE 8

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

4.8 OUTPUT SIGNALS - GUIDELINE 9

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

contains features to minimize the occurrence of this failure mode, such as auto-calibration, A/D conversion and application software checksum diagnostics and parameter validation.)

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

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

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

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

4.10 DIVERSITY AMONG ECHELONS OF DEFENSE - GUIDELINE 12

4.10.1 Control/Reactor Trip

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

Additionally, both the Q-DCIS and DPS provide a manual means of tripping the reactor. To support manual reactor trip, both the Q-DCIS and the DPS provide plant information to the operator. The Q-DCIS provides the safety-related measurements of the parameters that SCRAM the reactor while the DPS provides similar nonsafety-related diverse indications.

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

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

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

4.10.3 Reactor Trip/ESFAS

Generally isolated, independent interconnections exist between the reactor trip and ESF actuation functions for safety-related display purposes. Since the RPS and ECCS functions use separate sensors and hardware/software, failure of the reactor trip function does not prevent the ESF actuation function from responding to other inputs. Likewise, failure of the ESF actuation function does not prevent the reactor trip function from responding to other inputs.

4.11 PLANT MONITORING - GUIDELINE 13

Indications to support manual actions to maintain the plant within operating limits, trip the reactor, and actuate ESF functions are provided within the three layers of the I&C architecture. The N-DCIS provides nonsafety-related operator displays and alarms. Plant data for the nonsafety-related displays and alarms are obtained from the I&C architecture by means of the real-time data network. The SSLC/ESF within the Q-DCIS provides safety-related operator displays (safety-related information is also available on nonsafety-related displays through isolated gateways). In addition, the DPS provides nonsafety-related, diverse operator indications. No sensors are shared between the RPS/SSLC/ESF and the DPS. Diverse and independent signal conditioning and data acquisition functions are performed in the RPS/SSLC/ESF and DPS such that a postulated software CMF in one platform does not degrade the signal conditioning and data acquisition functions in the other platform.

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

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

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

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

4.12 MANUAL OPERATOR ACTION – GUIDELINE 14

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

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

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

5 EVALUATION OF DIVERSITY WITHIN THE ESBWR INSTRUMENTATION AND CONTROL ARCHITECTURE

5.1 INTRODUCTION

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

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

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

5.2 DIVERSITY OVERVIEW OF THE ESBWR INSTRUMENTATION AND CONTROL ARCHITECTURE

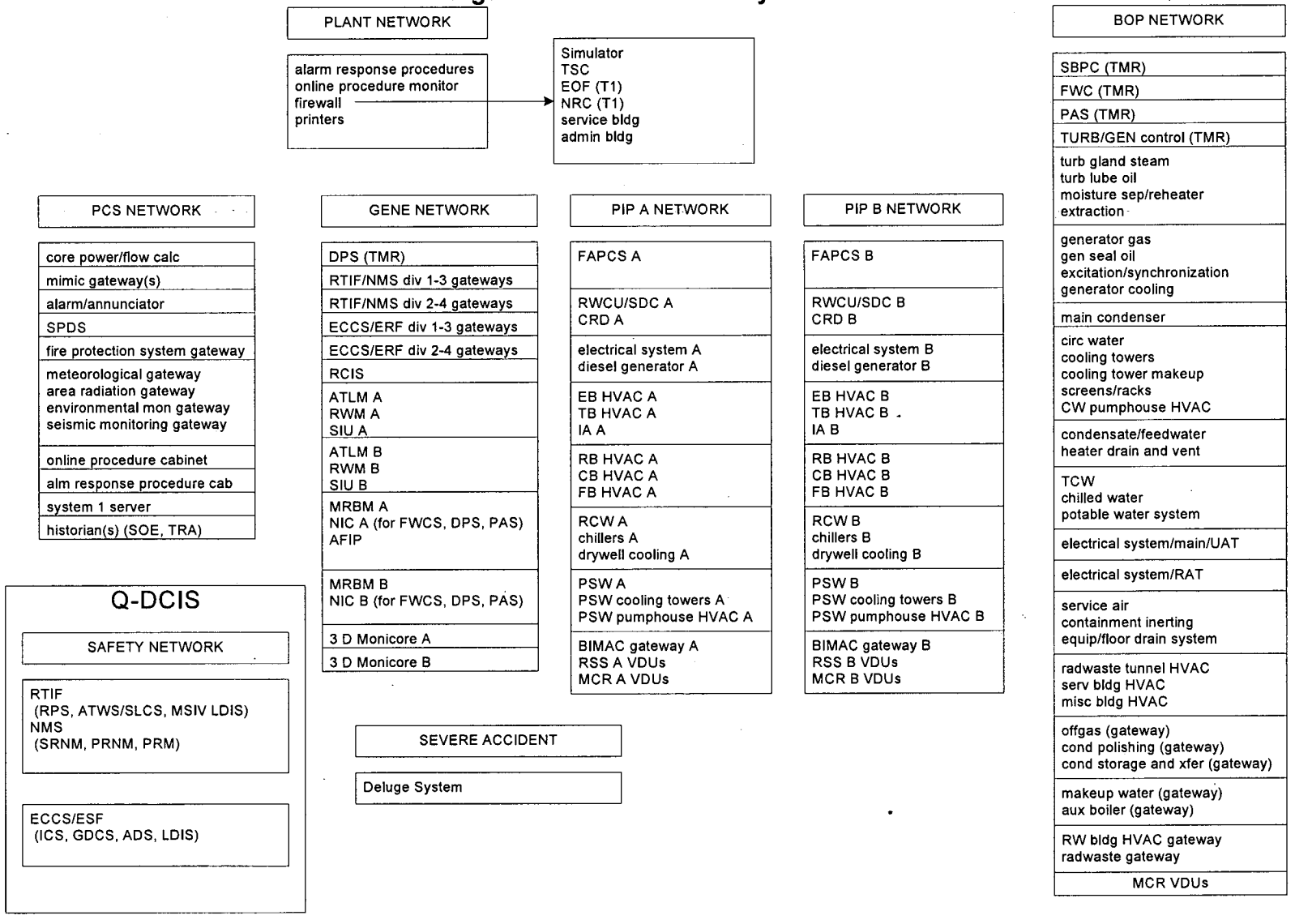
5.2.1 ESBWR DCIS Hierarchy

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

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

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

Figure 7 N-DCIS Control Systems



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

The third layer contains the DPS that provides nonsafety-related reactor trip functions, actuation of engineered safety features, and operator displays. In the DPS, both automatic and manual means are provided to trip the reactor and actuate selected engineered safety features; automatic actuation uses two-out-of-four sensor trip information and 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 that used in the Q-DCIS.

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

5.2.2 ESBWR DCIS Use of QNX

The safety-related and nonsafety-related DCIS (Q-DCIS and N-DCIS) hardware and software platforms are diverse from each other, with the exception that some hardware platforms use the QNX real-time operating system (RTOS) to control certain processes within the platform. The TRICON SSLC/ESF platform uses the QNX-based highly modular graphical user interface (GUI) windowing system to control the safety-related VDUs and a non-QNX proprietary TRICON RTOS, TSX, to control the triple-modular redundant (TMR) processor core of the TRICON programmable logic controller (PLC). Like the TRICON PLC, the GE Mark VIe (Mark VIe) is a TMR architecture PLC system; however, it uses QNX as the RTOS for the processor core and the non-QNX Cimplicity Display System running on a Windows NT operating system (OS) platform for its GUI. Thus, there is a diverse application of QNX across the two platforms.

This diversity in application does not result in a point of common cause failure (CCF). The presence of QNX across the different ESBWR control system platforms, by itself, is not considered a point of CMF because the QNX RTOS receives different stimuli from the same event from the two platforms. The TRICON VDU QNX RTOS by its nature processes an event differently from the Mark VIe QNX RTOS. The TRICON QNX processes stimuli external to the processor environment and the Mark VIe QNX processes stimuli internal to the processor environment. The output of the TRICON QNX is further processed by the TRICON TSX RTOS. The Cimplicity Display System and Windows NT OS would have processed the input received by the Mark VIe QNX RTOS. It is postulated that the same external stimulus cannot reach the processors in each platform and cause an irrecoverable fault or failure in each platform as a result of that stimulus because of these other factors that reside outside of the use of QNX.

Despite the above "diversity" of QNX application and however unlikely, a common cause failure, both the safety-related displays and the Mark VIe (including resulting DPS) would fail. The Mark VIe is a nonsafety-related platform; thus, its failure does not lead to a loss of reactor coolant pressure boundary or an event that could potentially result in radiation exposures

exceeding regulated limits. The RPS and NMS do not use QNX and are not assumed to fail as result of the event that causes QNX to fail; the RPS automatically trips the reactor if 2-out-of-4 divisions sense a trip condition. Likewise, failure of the safety-related TRICON VDU does not affect the automatic SSLC/ESF actuation and monitoring functions of the TRICON because the TRICON determines whether or not incoming VDU data is both valid and timely. If the data is not evaluated as both valid and timely, the TRICON ignores the incoming VDU input and relies on the input from its safety-related sensors. The emergency core cooling systems ECCS are still automatically actuated if the TRICON senses an upset condition in 2-out-of-4 divisions.

During this assumed event, the MCR operators still receive safety-related information through the nonsafety-related VDUs because the intervening gateways and display controllers do not use QNX. The CMF that causes QNX to fail does not cause a simultaneous loss of the nonsafety-related VDUs. The ESBWR operates after an accident for 72 hours without any operator intervention. After 72 hours, manual pool refills (from the fire protection system) are required to maintain adequate core cooling. Monitoring of the pools can be performed through the nonsafety-related VDUs. Thus, even in the highly unlikely event that both the safety-related TRICON VDU and Mark VIe platforms failed as a result of a CMF in QNX, the plant's safety-related automatic controls and nonsafety-related monitoring systems are diverse enough that they remain functional.

In addition, the QNX microkernel architecture provides further assurance against CMF. The microkernel provides a minimal set of primitives, or system calls, to implement the basic necessities of an operating system. These basic necessities typically include address-space management, thread management, and interprocess communication. All other services normally provided by traditional, or monolithic, kernels are implemented in user space as individual processes or programs. Further, the use of a microkernel allows users (developers) to turn off any functionality they do not require without having to change the operating system itself; instead, those servers are simply not run.

By virtue of its small, comprehensible size, a microkernel is less prone to errors, provides a superior security platform, and allows for easier validation of implementation than conventional operating system kernels. Also, because system services (networking, device drivers, file systems) are implemented outside of the kernel as separate, user-space processes, a failure in any service won't impact the performance of the kernel or of other running processes. This modular approach also provides for both flexibility and ease of extensibility.

Unlike most software qualified for safety-related applications, there is a good track record with the QNX operating system. It is widely used in the Automotive industry and has been designed into over 180 different automobile models with 100's of thousands of installations. None of these applications has experienced a common cause QNX failure.

In the ESBWR, the QA of the applications running under QNX in the MARK VIe and the safety-related VDU is different and separate. The features of QNX used in Mark VIe specifically exclude all graphical user interface functionality, so the probability of a CMF that affects the part of QNX used by the non-safety control is low.

5.3 REACTOR SHUTDOWN

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

- The control rods can be hydraulically scrammed into the core using stored nitrogen pressure initiated by the RPS function of Q-DCIS. The safety-related NUMAC processors evaluate two-out-of-four sensor trip decisions and separately provide two-out-of-four SCRAM decisions; the SCRAM is initiated by using load drivers to interrupt the 120 VAC power to the SCRAM solenoids on the HCUs. A backup SCRAM circuit is simultaneously energized that picks up the solenoids that blow down the air headers common to all the HCUs and eventually causes a SCRAM should the load drivers fail to open. The Q-DCIS also provides controls for manual insertion of the control rods by using contactors to directly interrupt the HCU solenoid current without any microprocessor involvement. The non-microprocessor based ATWS/SSLC logic automatically injects soluble boron and can independently shut down the reactor; the manual SCRAM and ATWS/SLCS system represent diversity within the Q-DCIS. Figure 8 illustrates the RPS function of the Q-DCIS.

Figure 8 RPS Function of Q-DCIS

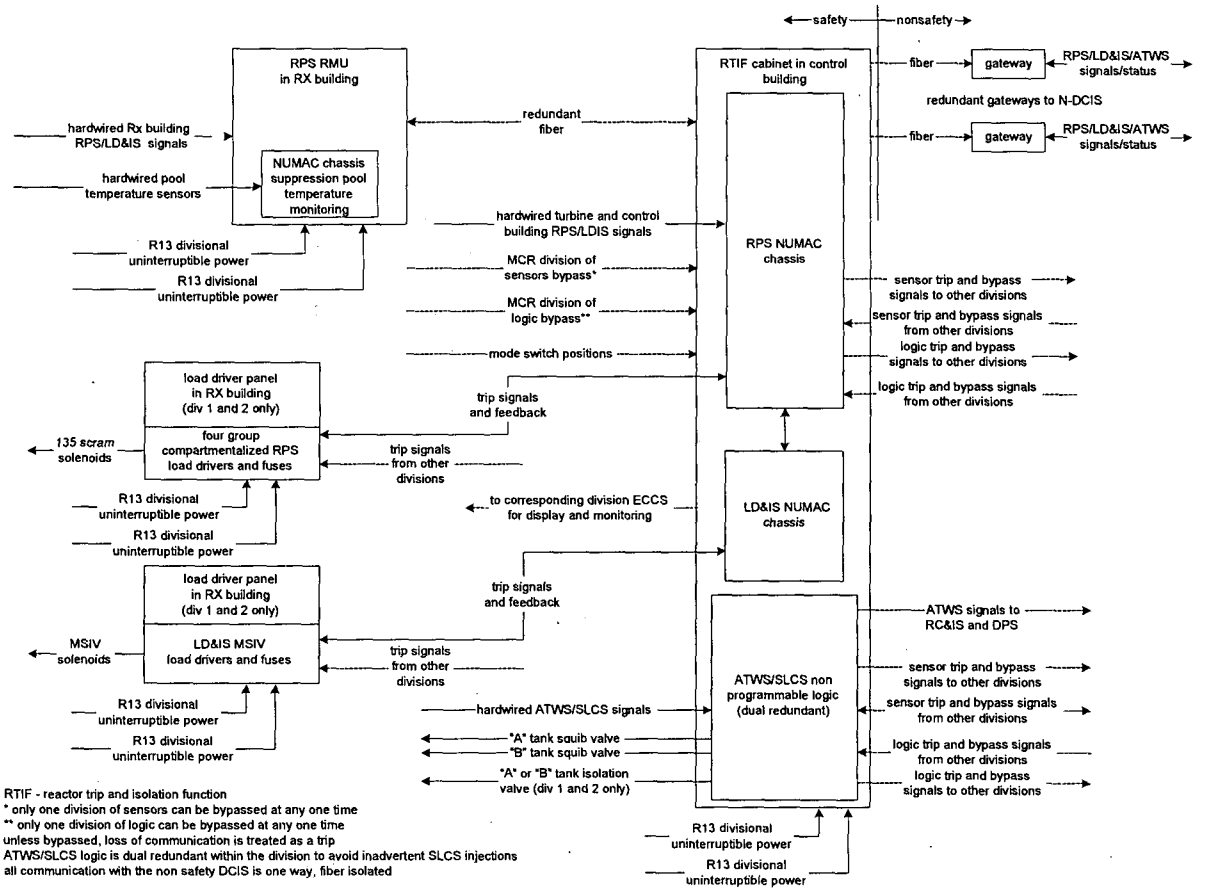
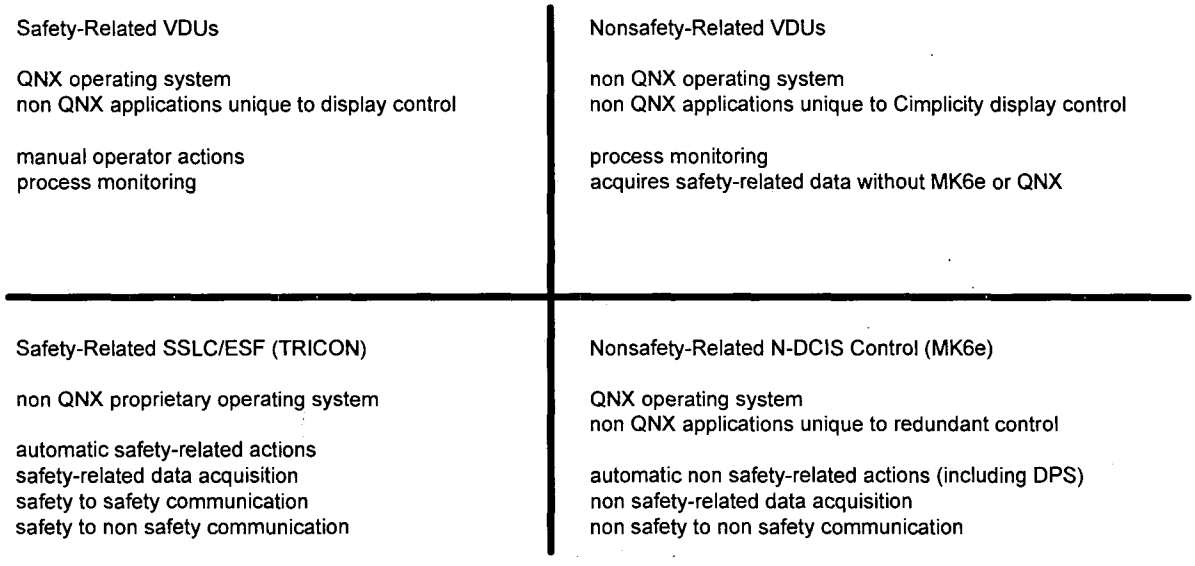


Figure 9 ESBWR QNX/Common Cause Failure Arrangement



- 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/SLC System logic through the DPS.

- The DPS provides automatic reactor shutdown by also hydraulically scramming the control rods. This nonsafety-related system uses sensors, processors and actuators that are diverse from those in Q-DCIS. Specifically the triply redundant processors of DPS make two-out-of-four sensor trip decisions and when two of the inputs to the three processors agree, the reactor is scrammed. The SCRAM is initiated by interrupting the current from the 120 VAC return of the HCU SCRAM solenoids. The DPS also provides for a manual SCRAM diverse from the Q-DCIS manual SCRAM. The DPS uses only a subset of Q-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.

5.4 REACTOR COOLANT SYSTEM INVENTORY CONTROL

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

- During normal and accident plant operation, RPV water level is automatically maintained from startup to rated power operation to shutdown by the FWCS. This control system and the mechanical Feedwater System is a 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 that 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. Half of these systems are controlled by the PIP A N-DCIS segment and the other half by the PIP B N-DCIS segment, and each half can be operated independently.

- During accident situations when neither offsite power nor the diesel generators are available, the Q-DCIS SSLC/ESF can automatically initiate the four isolation condensers; although the ICs do not add inventory, they do not lose inventory as they provide cooling at any but the lowest reactor pressures. At lower reactor power levels without offsite or diesel power, the Q-DCIS SSLC/ESF can automatically initiate an RPV depressurization (using both SRVs and DPVs) and

then automatically drain the contents of the GDCS pools into the RPV. This keeps the core covered throughout the initial stages of the accident; later, the Q-DCIS can drain ("equalize") the suppression pool water into the RPV for long term cooling. The ICs, RPV depressurization and GDCS can also be initiated manually.

- The DPS provides diverse coolant system inventory control by automatically initiating the ICs, SLC System, the ADS and the GDCS. The DPS uses sensors, processors and actuators that are diverse from those in Q-DCIS. Specifically the triply redundant processors of the DPS make two-out-of-four sensor trip decisions and when two of the three inputs to the processors agree, the required systems are initiated. The IC and SRV initiation is provided by opening nonsafety-related solenoids located "in parallel" with the existing safety-related solenoids. The explosive (squib) valves; the DPVs, GDCS and SLC System valves are fired by separate squib initiators "in parallel with" but isolated from the Q-DCIS squib initiators on those same valves. The suppression pool equalizing function is not provided by the DPS because it is not required for approximately 30 minutes, and manual actuation is acceptable. The DPS also provides for manual initiations of these various systems diverse from the Q-DCIS manual initiations. Several accident scenarios are further discussed in Section 5.8.

5.5 CORE DECAY HEAT REMOVAL

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

- During normal plant operation from startup to rated power operation to shutdown, core decay heat removal is accomplished with the bypass valves, the main turbine control valves, and the main condenser under the control of the SB&PC System and Turbine Generator Control System (TGCS); if offsite power is available, these systems also function during plant accidents. These control system designs are triply redundant using three of four sensors and an N-1 (at least) bypass valve and condenser shell arrangement that is single failure proof for power generation. The system has a capacity of at least 110% reactor steam flow and can easily accommodate any level of post SCRAM decay heat without requiring the use of the other safety-related and nonsafety-related systems. The system is available at all times that offsite power is available and can be operated manually.

- During normal and 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. Half of the RWCU/SDC systems are controlled by the PIP A N-DCIS segment and the other half by the PIP B N-DCIS segment 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 the Q-DCIS SSLC/ESF. These systems passively remove core decay heat without inventory loss by transferring the heat to the IC/PCCS pools and, through pool boiling, to the atmosphere that represents the ESBWR ultimate heat sink. If the ICs fail or are otherwise inadequate, the resulting lower reactor water levels cause the Q-DCIS SSLC/ESF to automatically initiate an RPV depressurization (using both SRVs and DPVs) and then automatically drain the contents of the GDCS pools, and eventually the suppression pools, into the RPV. This keeps the core covered and decay heat is removed by sensible heat addition to the added water and later boiling. The GDCS pools and suppression pool are designed to supply long-term heat removal. The ICs, RPV depressurization and GDCS systems can also be initiated manually.

- The DPS provides diverse core decay heat removal by its ability to automatically initiate the same systems as the Q-DCIS, specifically ICs, the RPV depressurization system and the GDCS. The IC and SRV initiation is provided by initiating nonsafety-related solenoids located "in parallel with" the existing safety-related solenoids. The explosive valves on the DPVs and GDCS are fired by separate squib initiators "in parallel with" but isolated from the Q-DCIS inputs to the squib initiators on those same valves. The DPS also provides for manual initiations of these various systems diverse from the Q-DCIS manual initiations. Manual action is required to drain ("equalize") the suppression pool water into the RPV. Several accident scenarios are further discussed in Section 5.8.

5.6 CONTAINMENT COOLING

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

- In normal or accident operation with offsite power or diesel generator power available, drywell cooling is provided by the PIP A and PIP B drywell cooling systems. The fans of the drywell coolers, the supporting chilled water, and the RCCW and PSW systems can maintain the drywell within its design temperature. Half of the drywell cooling system is controlled by the PIP A N-DCIS segment and the other half by the PIP B N-DCIS segment and each half can be operated independently.

- During normal or accident operation without offsite or diesel generator power available, the passive containment cooling system maintains containment cooling. There is a permanently open connection between the containment and the PCCS heat exchangers in the IC/PCCS pools above the containment. As containment temperatures increase the PCCS automatically removes more heat that is ultimately dissipated in pool temperature increase and boiling to the atmosphere. Since this system has no active components and is always "on", neither the Q-DCIS nor the DPS is required to initiate it or operate 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 potential release of radioactivity from the containment, following an accident.

- During normal operation many containment isolation valves are open and can be automatically closed by the Q-DCIS; depending on the system different signals are used to initiate automatic closure. Manual isolation is also provided by the Q-DCIS.

- The MSIVs and certain steam line drain valves are controlled by the RPS NUMAC portion of Q-DCIS; the SSLC/ESF portion of Q-DCIS controls other isolation valves. The actuation logic typically uses a combination of low RPV water level, high area temperatures, high system flows or high differential flows to automatically close the affected valves. The logic is described in Chapter 7 Reference 3.

- The DPS does not provide automatic isolation of all ESBWR containment isolation valves but those that present a potentially 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 are closed by the DPS on low RPV water level or high steam line flow; the actuators are switches in the 120 VAC MSIV solenoid return current. The IC isolation valves are closed by high flow; the actuators are nonsafety-related solenoids "in parallel with" the existing safety-related solenoids controlled by the Q-DCIS. The RWCU/SDC isolation valves are closed by high differential flow; the actuators are nonsafety-related solenoids "in parallel with" the existing safety-related solenoids controlled by Q-DCIS. The DPS also provides for manual isolation of these valves.

5.8 EVENT SCENARIOS

Appendix A provides a discussion of the Reference 3, 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 Reference 2. The following sections of transients/accidents provide a qualitative evaluation of DPS response to the same events used to evaluate the ATWS/SLC System, which has a similar (partial) function.

5.8.1 MSIV closure

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

5.8.2 Loss of Condenser Vacuum

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

5.8.3 Loss of Feedwater Heating

Since there is no DPS flux SCRAM, this event is controlled by the amount of feedwater heating lost/reactor power increase. In the worst case the reactor remains in a steady state overpower condition with the potential for fuel damage; since the N-DCIS remains operational the situation is alarmed to the operator and control rods automatically inserted by the DPS and FWC logic. Even assuming the unlikely failure of the Q-DCIS manual SCRAM, the reactor can be manually scrammed by the DPS. Since there is no coincident breach of piping or main condenser, the radiation consequences of fuel damage are concentrated in the power plant rather than offsite. Although the DPS played only a small 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 SCRAMs the reactor directly on either low RPV water level from loss of feedwater flow or the high RPV pressure resulting from the turbine trip and bypass valve closure. Both the bypass valves and turbine are controlled by triply redundant N-DCIS control systems unaffected by the loss of Q-DCIS. The DPS initiates the ICs on low reactor level when needed to provide core cooling. Additionally, the CRD, FAPCS and RWCU/SDC systems remain available to provide inventory and heat removal with diesel generator power – none of which are affected by a postulated Q-DCIS failure.

5.8.5 Loss of Feedwater Flow

This accident is effectively mitigated by the DPS. The DPS SCRAMs the reactor directly on low RPV water level from loss of feedwater flow; unlike the previous transient, the main condenser and bypass valve pressure control remains available. The turbine is

eventually tripped either manually or on reverse power; both the bypass valves and turbine are controlled by triply redundant N-DCIS control systems unaffected by the loss of Q-DCIS. The DPS initiates the ICs on low RPV water level when needed to provide core cooling, if the level falls below the IC initiation set point. Additionally the CRD, FAPCS and RWCU/SDC systems remain available to provide inventory and heat removal with offsite or diesel generator power – none of which are affected by a Q-DCIS failure.

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

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

The load rejection may have been caused by a grid related condition so the Q-DCIS SCRAM or SCRAM failure determines 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 manually (DPS) SCRAMs the plant when offsite power is restored (to repair the Q-DCIS).

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

5.8.7 Inadvertent Isolation Condenser Initiation

This transient does not require mitigation by DPS since the result of the inadvertent actuation is the loss of some power generation as steam is diverted from the turbine. If a level transient resulted, the DPS would SCRAM the reactor on level. The SB&PC should prevent a pressure transient since it is unaffected by the Q-DCIS failure. In any case, the IC pools begin heating and eventually the ICs should be isolated if the normal initiation valves cannot be closed. If the Q-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 the DPS if necessary) and

shut down normally. If offsite power is lost, the CRD, FAPCS and RWCU/SDC systems remain available to provide inventory and heat removal with diesel generator power – none of which are affected by a Q-DCIS failure.

5.8.8 Turbine Trip with Full Bypass

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

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

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

5.8.9 Opening of One Control or Turbine Bypass Valve

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

If the transient involves an opening turbine control valve or the turbine or bypass valve opening is too sudden for proper pressure control, a decreasing reactor pressure transient should result. This could eventually cause a low pressure MSIV isolation but the assumed Q-DCIS failure would prevent that. If the DPS 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 allow/maintain normal RPV water level, reactor pressure and a normal shutdown. The DPS initiates the ICs on low reactor level when needed to provide core cooling if the level falls below the IC initiation level setpoint. Additionally, the CRD, FAPCS and RWCU/SDC systems remain available to provide

inventory and heat removal with offsite or diesel generator power – none of which are affected by a Q-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. 26A6641AB (Tier 1, Rev. 3, February 2007), 26A6642AW (Tier 2 Rev. 3, February 2007), "ESBWR Design Control Document."
4. NEDE-33245P LTR "ESBWR Software Quality Assurance Plan," Revision 2, July 2007.
5. NEDE-33226P, LTR "ESBWR I&C Software Management Plan," Revision 2, July 2007.
6. IEEE 384-1981, "IEEE Criteria for Independence of Class 1E Equipment and Circuits."
7. NEDO-33201, "ESBWR Certification Probabilistic Risk Assessment," Revision 1, September 2006.
8. NUREG-0493, "A Defense-in-Depth & Diversity Assessment of the RESAR-414 Integrated Protection System," March 1979.
9. IEEE 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
10. IEEE 379-2000, "IEEE Standard Application of the Single-failure Criterion to Nuclear Power Generating Station Safety Systems – Description."
11. RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," May 1973
12. General Design Criterion 24, Separation of Protection and Control Systems
13. RG 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident."

APPENDIX A - ESBWR Instrumentation &Control Defense-in-Depth and Diversity (D3) Evaluation of Reference 3, 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 (Reference 1), as required by Branch Technical Position HICB-19 (Reference 2).

Reference 2 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 it. Table A1 identifies those events which either require further analyses to support the conclusions, are recommended, or require an assessment dispositioning 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), and
- MSIV closure.

Diverse ECCS actuation on the following signals:

- Low reactor water level (L1), and
- MSIV closure (ICs).

Diverse IC operation - reactor pressure control on the following signal:
MSIV closure.

Diverse reactor isolation on the following signals:

- Low reactor water level,
- High reactor steam flow, and
- Low steamline pressure.

Diverse containment isolation on the following signals:

- Low reactor water level,
- High process flows,
- High process differential flows, and
- High drywell pressure.

DPS scope expansion (to be confirmed by analysis):

- Possible diverse containment isolation on low reactor water level (L1) (to limit radiation release).
- Possible initiation of feedwater line isolation on high drywell pressure and high feedwater line differential pressure.
- Possible initiation of SRI and or SCRRI on loss of feedwater heating.
- Possible initiation of emergency control room HVAC.

Table A1 - Summary of Events That Require Supporting Analyses or Confirmatory Assessment

The following Reference 3, 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 Steam line 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 RPV L1 containment isolation does not occur. Determine acceptability of radiological release.

1. 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).* [1]

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*

[1] 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.

limiting conditions of operation, the analysis should demonstrate that such operator-induced transients will be compensated by protection system function.

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

Reference 1, 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): SCRRI
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). SCRRI/SRI 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 Turbine System (AOO)

Systems required (DCD Table 15.1-5: System Event Matrix): TBV Initiation – TCV Fast Closure; SCRRI/SRI
Automatic Trip (from DCD Table 15.1-6): None
Event Diagram: 15.1-4
Event Analysis: Event bounded by load rejection with a single failure in the Turbine Bypass. SB&PC acts to open remaining TCVs and some TBVs and plant stabilizes at new steady state. SCRRI/SRI 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 from SRVs.

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 initiation – MSIV position ICS – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV closure – RPV Low Water Level (L2 + 30 sec delay); TBV Initiation – TCV Fast

Closure; Automatic Trip (from DCD Table 15.1-6): TCV Fast Closure (with insufficient bypass available)
Event Diagram: 15.1-5
Event Analysis: 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; SCRRI/SRI
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 initiation– MSIV Position; ICS – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV closure – RPV Low Water Level (L2 + 30 sec delay); MSIV closure – Low Turbine Inlet/Main Steamline Pressure; TBV Initiation –TSV Closure; Automatic Trip (from DCD Table 15.1-6): TSV Closure (with insufficient bypass available)
Event Diagram: 15.1-7
Event Analysis: 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 initiation – MSIV position; MSIV Closure – High Steamline Flow Automatic Trip (from DCD Table 15.1-6): MSIV Position
Event Diagram: 15.1-8
Event Analysis: 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 initiation – MSIV position 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 (i.e., with 10% of 10 CFR 100 guidelines.] Pressure response bounded by ATWS analysis. Implementation of an MSIV closure trip in DPS provides margin.

15.2.2.8 Loss of Condenser Vacuum (AOO)

Systems required (DCD Table 15.1-5: System Event Matrix): ICS initiation – MSIV position; TBV Closure – Low Low Condenser Vacuum; TSV Closure – Low Condenser Vacuum; MSIV Closure – Low Condenser Vacuum Automatic Trip (from DCD Table 15.1-6): Low Condenser Vacuum
Event Diagram: 15.1-10
Event Analysis: If RPS 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 also attenuates the pressure transient. As an additional layer of defense, manual initiation of ATWS mitigation is available to provide initiation of ARI, SLC injection and feedwater runback. Manual scram from RPS or DPS is 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): ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation – RPV Low Water Level (L2 + 30 sec delay); GDCS
Automatic Trip (from DCD Table 15.1-6): None
Event Diagram: 15.1-11
Event Analysis: Not a significant event or limiting event. Operating systems function to mitigate this event. (One train of SDC still assumed to function.)
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 is 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): TBV Closure – Low Low Condenser Vacuum; ICS initiation – Loss of Power Generation Buss (Loss of Feedwater Flow); and MSIV closure – RPV Low Water Level (L2 + 30 sec delay); TBV Initiation – TCV Fast Closure; TCV Fast Closure – Load rejection; MSIV Closure – Low Condenser Vacuum;
Automatic Trip (from DCD Table 15.1-6): Loss of Power on Power Generation Busses - Loss of Feedwater Flow
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 initiation –Loss of Power Generation Buss (Loss of Feedwater Flow); MSIV closure – RPV Low Water Level (L2 + 30 sec delay)
Automatic Trip (from DCD Table 15.1-6): Loss of Power on Power Generation Busses- Loss of Feedwater Flow
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. DPS also starts ICS on delayed L2 signal. 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 initiation – MSIV Position; ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV closure – RPV Low Water Level (L2 + 30 sec delay); TBV Initiation – TSV Closure; TSV Closure – RPV high water Level (L8); MSIV Closure – Low Turbine Inlet/Main Steamline Pressure Automatic Trip (from DCD Table 15.1-6): RPV High Water Level (L8)
Event Diagram: 15.1-18
Event Analysis: Assume RPS failure: for this event, DPS provides SCRAM on L8 to mitigate this event. FW runback occurs. 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 SSLC/ESF 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 Control and Bypass Valves (Infrequent Event)

Systems required (DCD Table 15.1-5: System Event Matrix): ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV Closure - RPV Low Water Level (L2 + 30 Sec delay); MSIV closure – Low Turbine Inlet/Main Steamline Pressure Automatic Trip (from DCD Table 15.1-6): APRM High Neutron Flux
Event Diagram: 15.1-20
Event Analysis: Using realistic assumptions, a complete failure of the SB&PC 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 (10% of 10 CFR 100 guidelines).

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

Systems required (DCD Table 15.1-5: System Event Matrix): ICS initiation – MSIV Position; ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV Closure - RPV Low Water Level (L2 + 30 Sec delay); TCV Fast closure – Load Rejection; MSIV closure – Low Turbine Inlet/Main Steamline PressureAutomatic 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 SSLC/ESF 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 initiation – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV Closure - RPV Low Water Level (L2 + 30 Sec delay); MSIV closure – Low Turbine Inlet/Main Steamline PressureAutomatic 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 SSLC/ESF 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 is 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): 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): None Automatic Trip (from DCD Table 15.1-6): High Suppression Pool Temperature
Event Diagram: 15.1-29
Event Analysis: SB&PC available to stabilize pressure prior to occurrence of 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): SRV – Power Actuated Mode (ADS); DPV – Actuation; GDCS; Passive Containment Cooling (PCCS).
Automatic Trip (from DCD Table 15.1-6): High Drywell Pressure
Event Diagram: 15.1-30
Event Analysis: SB&PC available to stabilize pressure prior to occurrence of SCRAM after which time the pressure decreases. 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
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): SRV – Power Actuated Mode (ADS); DPV – Actuation; ICS initiation – MSIV Position; MSIV Closure – Low Turbine Inlet /Main Steamline Pressure; GDCS; PCCS
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 SSLC/ESF 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 initiation – MSIV position; ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L1); ICS initiation – Loss of Power Generation Buss (Loss of Feedwater Flow); SLC System - DPV Open; GDCS; GDCS Equalizing Lines; PCCS;

High Radiation MCR recirculation Automatic Trip (from DCD Table 15.1-6): RPV Low Water Level (L3); Loss of Power Generation Bus- Loss of Feedwater Flow; High Drywell Pressure
Event Diagram: 15.1-34
Event Analysis: If RPS 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. SSLC/ESF initiation occurs to mitigate the event. Non-MSIV LD&IS isolation occurs. If SSLC/ESF 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 or feedwater system 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 initiation – MSIV Position; ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L1); ICS initiation – Loss of Power Generation Buss (Loss of Feedwater Flow); SLC System - DPV Open;; GDCS; GDCS Equalizing Lines; High Radiation MCR recirculation PCCS
Automatic Trip (from DCD Table 15.1-6): RPV Low Water Level (L3); Loss of Power Generation Bus-Loss of Feedwater Flow; High Drywell Pressure
Event Diagram: 15.1-34
Event Analysis: Refer to 15.4.2
Conclusion: Refer to 15.4.2

15.4.4 LOCA Inside Containment (Radiological Analysis) (Accident)

Systems required (DCD Table 15.1-5: System Event Matrix): SRV – Power Actuated Mode (ADS); DPV – Actuation; ICS initiation – MSIV Position; ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L1); ICS initiation – Loss of Power Generation Buss (Loss of Feedwater Flow); SLC System - DPV Open; GDCS; GDCS Equalizing Lines; High Radiation MCR recirculation; PCCS
Automatic Trip (from DCD Table 15.1-6): RPV Low Water Level (L3); Loss of Power Generation Bus-Loss of Feedwater Flow; High Drywell Pressure
Event Diagram: 15.1-34
Event Analysis: Refer to 15.4.2
Conclusion: Refer 15.4.2

15.4.5 Main Steamline Break Outside Containment (Accident)

Systems required (DCD Table 15.1-5: System Event Matrix): SRV – Power Actuated Mode (ADS); DPV – Actuation; ICS initiation – MSIV Position; ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L1); ICS initiation – Loss of Power Generation Buss (Loss of Feedwater Flow); MSIV Closure – Low Turbine Inlet/Main Steamline Pressure;

MSIV Closure – High Steamline Flow; SLC System - DPV Open; SLC System – RPV Low Water Level L2 – APRM not Downscale; GDCS; GDCS Equalizing Lines
Automatic Trip (from DCD Table 15.1-6): RPV Low Water Level (L3); MSIV Position; Loss of Power Generation Bus-Loss of Feedwater Flow
Event Diagram: 15.1-35
Event Analysis: If RPS CMF assumed, DPS provides SCRAM on low water level (L3). LD&IS (MSIV) isolation failure is assumed because of the same platform as RPS. SSLC/ESF 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 SSLC/ESF 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 initiation – MSIV Position; ICS initiation and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L1); ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation – Loss of Power Generation Buss (Loss of Feedwater Flow); SLC System - DPV Open; GDCS; GDCS Equalizing Lines; PCCS
Automatic Trip (from DCD Table 15.1-6): RPV Low Water Level (L3); MSIV Position; Loss of Power Generation Bus-Loss of Feedwater Flow
Event Diagram: 15.1-37
Event Analysis: If RPS CMF assumed, DPS provides SCRAM on low water level (L3). SSLC/ESF initiation occurs. If SSLC/ESF CMF assumed, diverse ESF initiation (at L1) is required to mitigate the event.
Conclusion: No fuel failure assumed for this event. Worst-case dose does 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 initiation – MSIV Position; ICS initiation and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L1); ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation – Loss of Power Generation Buss (Loss of Feedwater Flow); SLC System - DPV Open; GDCS; GDCS Equalizing Lines; PCCS
Automatic Trip (from DCD Table 15.1-6): RPV Low Water Level (L3); MSIV Position; Loss of Power Generation Bus-Loss of Feedwater Flow

Event Diagram: 15.1-38
Event Analysis: Leak detection by aberrant indication (radiation, temperature, humidity or noise) alerts operator to perform an orderly shutdown. If RPS CMF assumed, manual SCRAM is still 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 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 initiation – MSIV Position; ICS initiation and MSIV Closure– RPV Low Water Level (L2 + 30 sec delay); ICS initiation and MSIV Closure– RPV Low Water Level (L1); ICS initiation – RPV High Dome Pressure (10 sec delay); ICS initiation – Loss of Power Generation Buss (Loss of Feedwater Flow); SLC System - DPV Open; GDCS; GDCS Equalizing LinesPCCS
Automatic Trip (from DCD Table 15.1-6): RPV Low Water Level (L3); MSIV Position; Loss of Power Generation Bus-Loss of Feedwater Flow
Event Diagram: 15.1-39
Event Analysis: If RPS 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 extends the duration of the event until leak is identified and isolated. Manual remote isolation is available to the operator. High radiation Main Control Room Recirculation actuation signal alerts the operator to 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 SSLC/ESF platform fails.

Sect	Description	Event Class	Diverse I&C system	Comments
15.2.1	Decrease in Core Coolant Temperature	(Event Category)		
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/SCRRI. 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 happens 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 results 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.	DPS SCRAMs on MSIV closure or SCRAMs 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 SCRAMs 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
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	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 requires DPS SCRAM at level L8.
15.2.5	Decrease in Reactor Coolant Inventory (Event Category)			
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 normally SCRAMs on loss of power to plant 13.8 kV busses – DPS does not. However if RPS fails to SCRAM, then DPS SCRAMs on L3.
15.2.5.3	Loss of All Feedwater Flow	AOO	L3 SCRAM	DPS SCRAMs 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 SCRAMs 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 SCRAMs on high pressure
15.3.5	Generator Load Rejection With Total Turbine Bypass Failure	Infrequent Event	High reactor pressure SCRAM	Incredible event but DPS SCRAMs on high pressure
15.3.6	Turbine Trip With Total Turbine Bypass Failure	Infrequent Event	High reactor pressure SCRAM	Incredible event but DPS SCRAMs on high pressure

Sect	Description	Event Class	Diverse I&C system	Comments
15.3.7	Control Rod Withdrawal Error During Refueling	Infrequent Event	No Diverse I&C required	No DPS action
15.3.8	Control Rod Withdrawal Error During 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 also SCRAMs on high suppression pool temperature
15.3.14	Inadvertent Opening of a Depressurization Valve	Infrequent Event	High drywell press SCRAM	DPS also SCRAMs on high drywell pressure
15.3.15	Stuck Open Safety-Relief Valve	Infrequent Event	Suppression pool temperature SCRAM	DPS also SCRAMs 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 SCRAMs on reactor level, drywell pressure and initiate (ECCS) Automatic Depressurization System (ADS)/Gravity Driven Cooling System (GDCS), SLC System, 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 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 SCRAMs on low RPV water level. Worst case dose does 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 reaches L3. If level reaches (L1), DPS operates diverse ECCS. 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 reaches L3. If level reaches L1, the DPS actuates the 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.				

MFN 07-475

Enclosure 2

ESBWR DCD Tier 2 Markups

generators or off-site power. This allows for operation of the Q-DCIS when one power supply is in maintenance bypass. Further discussion of the safety-related power supplies is provided in Chapter 8.

7.1.6.6.1.28 Cyber Security (IEEE Std. 7-4.3.2)

The security requirements included in RG 1.152 are evaluated and incorporated in the Q-DCIS design and include both plant hardware and software security measures. The software development process plans will be developed with the security requirements incorporated for actual detailed design implementation.

The comprehensive cyber security program plan identifies security risks and outlines appropriate procedures to ensure that hardware, controls, and data networks comprising the control network cannot be disrupted, interrupted or negatively impacted by unauthorized users or external systems. It also documents the design commitments meeting the applicable requirements of RG 1.152, Section C.2, and Positions 2.1 through 2.9.

Inspections, tests, analyses, and acceptance criteria (ITAAC) associated with the cyber-security program plan are provided in ESBWR DCD, Tier 1 together with the software development plan.

7.1.7 COL Information

None.

7.1.8 References

7.1-1 USNRC, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," NUREG-0800.

7.1-2 General Electric Company, "General Electric Environmental Qualification Program," NEDE-24326-1-P, Revision 1, Class III (proprietary), January 1983.

7.1-3 Electric Power Research Institute (EPRI) TR-102323 (TR-1003697), "Guidelines for Electromagnetic Interference Testing of Power Plant Equipment", Revision 3.

7.1-4 ~~GE Energy~~ Licensing Topical Report (LTR) entitled, "ESBWR I&C Defense-In-Depth and Diversity Report." NEDO-33251, Class I (Non-proprietary), ~~Revision 0, July 2006.~~

7.1-5 GE Energy, "ESBWR Safety Criteria for Instrumentation & Control Systems." NEDO-33294, Class I (Non-proprietary), Revision 0.

7.1-6 GE Energy, "Application of Nuclear Measurement Analysis and Control for a new BWR (NUMAC Platform Architecture.)" NEDC-33288P, Class III (Proprietary), Revision 0

7.1-7 GE Energy, "SSLC/ESF Licensing Topical Report (Platform Architecture.)" Class III (Proprietary), Revision 0

- BTP HICB-18 - Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems
- BTP HICB-19 - Evaluation of Defense in Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems
  - Licensing Topical Report NEDO-33251, "ESBWR I&C Defense-In-Depth and Diversity Report," details the echelons of defense used in the ESBWR design. This document also discusses the basis for selection of the DPS functions used as backups for the RPS and SSLC/ESF. A failure modes and effects analysis based on the Guidance in NUREG/CR-6303 is performed to ensure the radiation limits derived from 10 CFR 100 are not exceeded in the event of a common mode failure of the RPS or SSLC/ESF software platform, during the design basis events discussed in the Safety Analyses.
- BTP HICB-21 - Guidance on Digital System Real-Time Performance

7.8.4 COL Information

None

7.8.5 References

7.8-1 ~~GE~~ GE-Hitachi Nuclear Energy, ESBWR I&C Defense-In-Depth and Diversity Report, NEDO-33251, Class I (Non-proprietary), ~~Revision 0, July 2006.~~ Revision 1, August 2007.

7.8-2 NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection systems, December 1994