ENCLOSURE 1

MFN 05-118

Revised DCD section 7.1, "Introduction"

(Instrumentation and Control Systems)

Conditional Release – pending closure of design verifications

7. INSTRUMENTATION AND CONTROL SYSTEMS

7.1 INTRODUCTION

This chapter presents the specific detailed design and performance information relative to the instrumentation and control (I&C) aspects of safety-related and nonsafety-related systems important to safety utilized throughout the plant. Many of the systems have other design aspects relative to mechanical, radiological, and other items that are described in other chapters.

7.1.1 Identification of I&C Systems

7.1.1.1 General

Instrumentation and control systems are designated as either nonsafety-related systems or safety-related systems, depending on their functions. Some portions of a system may have a safety function, while other portions of the same system may be classified as nonsafety-related. A description of the system of classification can be found in Section 3.2.

Because many of the ESBWR safety functions (engineered safety features) do not rely on diesel backed electrical energy or active systems by design, the necessary safety-related instruments and controls are considerably reduced and simplified compared to previous BWR plant designs. The systems presented in Chapter 7 are arranged consistent with the Nuclear Regulatory Commission (NRC) Standard Review Plan (SRP), Reference 7.1-1, with slight variations in some section titles to accommodate ESBWR design philosophy, i.e., Introduction, Reactor Trip System, Engineered Safety Feature (ESF) Systems, Shutdown Systems, Safety-Related and Nonsafety-related Information Systems, Interlock Systems, Control Systems, Diverse Instrumentation and Controls, and Data Communication Systems. Table 7.1-1 shows the application of the regulatory requirements specified in the SRP to the various systems.

Each individual safety-related system utilizes redundant channels of safety-related instruments for initiating safety action. The automatic decision-making and trip logic functions associated with the safety actions of the safety-related reactor trip system and engineered safety feature systems are accomplished by a four-division, separated protection logic system framework called the Safety System Logic and Control (SSLC). The SSLC provides the hardware and software platforms for the logic for the safety-related protection functions, such as reactor trip, isolation, and emergency core cooling functions. The SSLC multi-divisional system includes divisionally separate panels which house the SSLC equipment for controlling the various safety functions and the actuation devices. The SSLC receives input signals from the redundant channels of safety-related instrumentation, and uses the input information to perform logic functions in making decisions for safety actions. The ESBWR systems, which have logic implemented in the SSLC, include the Reactor Protection (Trip) System, the Suppression Pool Temperature Monitoring function of the Containment Monitoring System, the control logic of the Automatic Depressurization System of the Nuclear Boiler System, the control logic of the Gravity-Driven Cooling System, the Leak Detection and Isolation System, and the control logic of the Isolation Condenser System. Divisional separation is also applied to the Essential Distributed Control and

Information System (E-DCIS), which provides data highways for the sensor input to the logic units and for the logic output to the system actuators (actuated devices such as valves or squibs). These and other SSLC interfaces are identified in the following subsections, and discussed in detail in the appropriate sections of this chapter. A simplified block diagram showing the major ESBWR I&C systems and main control room interfaces is shown in Figure 7.1-1.

Note that the ESBWR instrumentation and control (I&C) systems provide many levels of diversity. In general the RPS and MSIV isolation use separate sensors, hardware and software than the ESF I&C. Furthermore, ATWS/SLCS is implemented in non-microprocessor based hardware and uses separate level transmitters than RPS. A diverse protection system, which includes both diverse RPS and diverse ESF actuation functions using different sensors, hardware and software platforms than either of the safety related I&C systems is also provided. Finally the nonsafety related I&C systems which operate both plant investment protection (PIP) systems and BOP systems are also different hardware and software platforms than the safety I&C systems. Figure 7.1-2 presents a block diagram identifying the diverse hardware and software platforms of the ESBWR I&C systems.

7.1.1.2 The ESBWR Instrumentation and Control Architecture

The ESBWR instrumentation and control (I&C) systems consist of both safety-related and nonsafety-related control systems. The primary safety-related systems, such as the reactor protection system, lead detection and isolation system, and the engineering safety features initiation logics, are encompassed by the Safety System Logic and Control (SSLC) framework. The SSLC and safety-related systems are supported by the safety-related data communication network, the Essential Distributed Control and Information System (E-DCIS). The nonsafety-related (control) systems include all other plant I&C systems, which are supported by the nonsafety-related data communication network, the Non-Essential Distributed Control and Information System (NE-DCIS). A simplified block diagram of the ESBWR I&C architecture is shown in Figure 7.1-1.

7.1.1.2.1 The Safety System Logic and Control (SSLC) Architecture

The safety-related I&C systems consists of the SSLC and other individual monitoring systems such as the Neutron Monitoring System and the Process Radiation Monitoring System, etc. The SSLC is a four-division, separate and redundant protection logic system framework that provides automatic decision-making and trip logic functions to implement the safety actions of the safety-related reactor trip system and engineered safety feature systems within the framework. The SSLC multi-divisional system includes divisionally separate panels which house the SSLC equipment for controlling the various safety functions and the actuation devices. Figure 7.3-5 provides an overview of the structure of the SSLC, which mainly consists of the Reactor Trip and Isolation Function (RTIF) part of the framework and the Engineering Safety Features (ESF) part of the framework. The RTIF includes the logics of the Reactor Protection System (RPS) for reactor scram and the isolation logics of main steam-line isolation valves (MSIV). The ESF logics include all ECCS initiation logics for the opening of Automatic Depressurization System (ADS) Safety Relief Valves (SRV), Depressurization Valves (DPV), Gravity-Driven Cooling System (GDCS) squib valves, and Isolation Condenser (IC) valves. It also includes the leak

detection and isolation function logics and the Standby Liquid Control System liquid boron injection initiation logic for the Anticipated Transient Without Scram (ATWS) function.

SSLC/RTIF

The basic system architecture of the RTIF, i.e., the RPS and MSIV Isolation part of SSLC, employs four independent trip logic systems in four separate divisions of safety protection equipment, as shown in Figure 7.2-1. The four redundant RPS divisions are identical in design and independent in operation. There are four instrument channels provided for each process variable being monitored, one for each RPS division. Four sensors, one per division, are provided for each variable. The logic in each division does not depend on time-of-day and is asynchronous to the other divisions; no division depends on the correct operation of another division nor on interdivisional communication links. As shown in Figure 7.2-1, each division has the Remote Multiplexing Unit (RMU) function, the Digital Trip Module (DTM) function, the Trip Logic Unit (TLU) function, the Output Logic Unit (OLU) function, and the Communication Interface Module (CIM) function. The RMU receives input from the sensors device and performs analog-to-digital conversion and signal processing function. The digitized signal is then sent to the DTM. Some signals are directly sent to the DTM such as those from the turbine stop valves and control valves positions. The DTM generates the trip signal to the TLU based on setpoint comparison. The DTM and the TLU reside in separate and independent processors. Each TLU receives the trip status from the DTMs in all four divisions and perform 2 out of 4 logic to determine the trip status for each system. Some trip signals are sent to the TLU directly from other inputs such as the NMS trip signals and operator manual inputs. The DTM receives division of sensor bypass signal to activate divisional trip bypass. The trip signal from the TLU is then sent to the OLU in this division and output to the load drivers in the scram circuitry. The CIM serves as the communication interface for data communication between the RTIF division and the nonsafety systems. The RPS logic and system design arrangement and architecture are described in more detail in Section 7.2.1.2.4. Like the ABWR, the ESBWR RPS logic will always scram the plant when any two or more same parameters (in two or more divisions) exceed their trip value, under any single failure and any division of sensors/logic bypass.

For the actual hardware and software design platform descriptions of the RTIF, detailed information of the platform concept is included in the referenced documents. Reference 7.1-2 provides a sample description of the platform performance of various functional components in RTIF applied in ABWR. The ESBWR employs the same functional components and platform structure. Reference 7.1-3 provides a sample detailed hardware and software functional description and specification of the RTIF applied in ABWR. Such RTIF hardware and software platform structure concept is identical to that of ESBWR. To provide as an example of a key RTIF component, Reference 7.1-4 provides the sample software design description and specification of the Digital Trip Module (DTM) of the RTIF applied in ABWR. Such RTIF DTM component structure concept is identical to that of ESBWR. In addition, Reference 7.1-5 and Reference 7.1-6 also provide the typical safety-related NMS system component units platform concepts (PRNM and SRNM) that are identical to that used in ESBWR NMS. Other than detailed specific parameters application and logic hardware/software designs, the ESBWR SSLC/RTIF architecture concept is identical to that of the ABWR. The ABWR SSLC/RTIF architecture concept has been reviewed and approved per the ABWR Certification.

SSLC/ESF

The ESF part of SSLC also follows a four-division architecture and platform. The basic system architecture of the ESF logics employs four independent trip logic systems in four separate divisions of safety protection equipment, as shown in Figure 7.3-4. The four redundant ESF logic divisions are identical in design and independent in operation. There are four instrument channels for each ESF logic division. Four sensors, one per division, are provided for each variable monitored. The logic data in each division does not depend on time-of-day and is asynchronous to the other divisions; no division depends on the correct operation of another division nor on interdivisional communication links. The ESF logic design arrangement and architecture are described in more details in Section 7.3.4.2. SSLC/ESF input data (process variables) are multiplexed via the Essential DCIS System (E-DCIS) in four physically and electrically isolated redundant divisions. Each of the four independent and separated E-DCIS channels feeds separate and independent channel of SSLC/ESF equipment.

As shown in Figure 7.3-4, each division of ESF logic has the Remote Multiplexing Unit (RMU), the Digital Trip Module (DTM) function, the Voter Logic Unit (VLU) function, the Network Interface Module (NIM) function and Communication Interface Module (CIM) function, and the Bridge Transfer Module (BTM) function. It also contains the safety-related visual display unit (VDU) for operator interface. Either directly or via data link, all the units within the network are connected by redundant fiber optic ring type network. The RMU is the input/output device and used either for sensor input function or for signal output function to actuators. The DTM generates the trip signal to the VLU based on setpoint comparison. The VLU and the DTM reside in separate and independent processors. The VLU is a dual logic function unit that processes two independent logic paths. Each VLU receives the trip status from the DTMs in all four divisions and perform 2-out-of-4 logic, in both logic paths independently, to determine the trip status for each system. The CIM serves as the communication interface for data communication between different ESF divisions and between the ESF division and other safety-related signal inputs from RPS and NMS. The BTM is used as the interface and isolation device to transfer data from the ESF division to nonsafety network through a gateway. Data is received at the input module of the RMU and processed in the RMU. It is then sent to the DTM for setpoint comparison. The resulted signal from this division and other three divisions are then processed by the VLU for 2-out-of-4 trip decision. The trip signal is then sent to the output RMU in all four divisions. The data is then sent by hardwire from the RMU to equipment for actuation. The safety-related VDU provides the operator with display and control interfaces. Specific descriptions of the SSLC/ESF logic function is presented in Section 7.3.4.2. Other than detailed specific parameters application and logic hardware/software designs, the ESBWR SSLC/ESF architecture concept is identical to that of the ABWR. The ABWR SSLC/ESF architecture concept has been reviewed and approved per the ABWR Certification.

7.1.1.3 Reactor Trip System

Reactor Protection System (RPS)

The safety-related RPS I&C initiates an automatic reactor shutdown by rapid insertion of control rods (scram) if monitored system variables exceed pre-established limits. This action prevents fuel damage, limits system pressure and thus restricts the release of radioactive material.

Neutron Monitoring System (NMS)

The safety-related NMS monitors the core neutron flux from the startup source range to beyond rated power. The NMS provides logic signals to the RPS to automatically shut down the reactor when a condition necessitating a reactor scram is detected. The NMS is composed of four subsystems:

- Startup range neutron monitor (SRNM);
- Power range neutron monitor (PRNM), a subsystem that includes the local power range monitor (LPRM), the average power range monitor (APRM), and the oscillation power range monitor (OPRM) functions;
- Automatic fixed in-core probe (AFIP) (nonsafety-related; refer to Subsection 7.1.1.7.); and
- Multi-Channel Rod Block Monitor (MRBM) (nonsafety-related; refer to Subsection 7.1.1.7.).

Suppression Pool Temperature Monitoring Subsystem Function (SPTMS)

The safety-related SPTMS is provided to monitor pool temperatures under all operating and accident conditions. The system operates continuously during reactor operation. Should the suppression pool temperature exceed established limits, the SPTMS provides input for both a reactor scram and for automatic initiation of suppression pool cooling mode of FAPCS. The SPTMS is part of the Containment Monitoring System (CMS).

7.1.1.4 Engineered Safety Features (ESF) Systems

Emergency Core Cooling Systems (ECCS)

Safety-related I&C provides automatic initiation and control of the Isolation condensers, Automatic Depressurization System (ADS) and the Gravity-Driven Cooling System (GDCS) to cool the fuel cladding in event of a design basis accident. The Standby Liquid Control (SLC) System also has an ECCS function discussed in Section 7.4.

Isolation Condenser System (ICS)

Safety-related ICS I&C automatically limit reactor pressure and temperature within an acceptable range so that safety relief valves will not lift and emergency reactor depressurization action will not occur when the reactor becomes isolated during power operations. Over longer durations, the ICS also removes excess sensible and core decay heat from the reactor without the need for an external power supply, and with minimal loss of coolant inventory from the reactor when the normal heat removal system is unavailable.

Passive Containment Cooling System (PCCS)

The safety-related PCCS functions to cool the containment following a rise in containment pressure and temperature without requiring any component actuation.

The PCCS needs no electric power and does not have instrumentation, control logic, or power actuated valves. Therefore, PCCS is not addressed in Chapter 7. However, the PCCS is briefly described herein for completeness.

Leak Detection and Isolation System (LD&IS)

The safety-related LD&IS I&C monitors leakage sources from the reactor coolant pressure boundary, and automatically initiates closure of the appropriate isolation valves to isolate the source of the leak if monitored system variables exceed preset limits. This action limits the loss of coolant from the reactor coolant pressure boundary and the release of radioactive materials to the environment.

Safety System Logic and Control System (SSLC)

The safety-related SSLC includes the control functions of the various safety function actuation devices of the safety-related plant systems. Input signals from redundant channels of safety-related instrumentation are used to perform logic operations that result in decisions for safety action. Trip logic outputs to the actuation devices (pilot solenoid valves, squib valves, etc.) initiate the appropriate plant protection.

7.1.1.5 Safety and Non-Safety Shutdown Systems

Standby Liquid Control System (SLCS)

The safety-related SLCS I&C provides for the automatic initiation of an independent boron solution system, to shut down the reactor from rated power to shutdown conditions in the event that withdrawn control rods cannot be inserted to achieve reactor shutdown. The system is also automatically initiated with ADS to provide additional core inventory

Remote Shutdown System (RSS)

Should the main control room become uninhabitable, the RSS panel provides the ability to both monitor and operate all of the required systems within the corresponding division. Although no automatic functions are lost with the control room evacuation, manual operation of all the divisional systems is also available. Similarly each RSS panel includes the ability to operate all of the non-safety Plant Investment Protection (PIP) equipment and BOP equipment, either automatically or manually.

Reactor Water Cleanup/Shutdown Cooling System (RWCU/SDC)

Nonsafety-related RWCU/SDC I&C functions to maintain reactor water purity during operation, and to provide normal shutdown cooling by taking suction from the reactor pressure vessel, pumping the flow through heat exchangers, and returning the cooled water to the vessel through the feedwater line. The I&C system is segmented and allows the different "A/B" components to operate independently.

Fuel and Auxiliary Pools Cooling System (FAPCS)

Nonsafety-related FAPCS I&C functions to maintain the various ICS, GDCS and suppression pool temperatures and cleanliness during operation, by pumping the flow through heat

exchangers and demineralizers. The FAPCS can also provide a "Low Pressure Core Injection (LPCI)" mode to provide inventory after the reactor pressure has been reduced. The I&C is segmented and allows the different "A/B" components to operate independently.

Control Rod Drive System (CRD)

Nonsafety-related CRD I&C normally functions to maintain the HCU accumulators at the required pressure, to provide cooling water flow to the FMCRDs and to provide various high pressure purge flows. The CRD can also provide a "high pressure injection" mode capable of supplying inventory to the reactor vessel at elevated pressures. The I&C is segmented and allows the different "A/B" components to operate independently.

7.1.1.6 Safety-Related Information Systems

General I&C Conformance to Regulatory Guide 1.97

Safety-related display instrumentation provides information regarding plant conditions and equipment status in order to determine the need for manual safety action. A detailed assessment of ESBWR conformance with Regulatory Guide 1.97 is presented in Subsection 7.5.1.

Containment Monitoring System (CMS)

Safety-related CMS instrumentation measures and records radiation levels and the oxygen/hydrogen concentration levels in the primary containment under post-accident conditions. It is designed to operate continuously in normal operation and is automatically put in service upon detection of loss-of-coolant accident (LOCA) conditions.

Process Radiation Monitoring System (PRMS)

Safety-related and nonsafety-related PRMS instrumentation monitors the main steam lines, fission products in the drywell, discharges from the Isolation Condenser System, vent discharges and liquid and gaseous effluent streams that may contain radioactive materials. Main control room display, recording, and alarm capability are provided along with controls, which provide automatic trip inputs to the respective systems for isolation of further radiation release.

Area Radiation Monitoring System (ARMS)

Nonsafety-related ARMS instrumentation continuously monitors the gamma radiation levels within designated areas of the plant, and provides early warning to operating personnel when predetermined exposure rates are exceeded.

7.1.1.7 Interlock Systems

Systems Interlock Function

A reactor pressure interlock is provided to Gravity-Driven Cooling System (GDCS) to prohibit inadvertent manual initiation of the system during normal reactor operation.

Normally closed isolation valves are provided on the Fuel and Auxiliary Pools Cooling System (FAPCS) low-pressure injection (LPCI) line to protect its low pressure piping from over

pressurization during the reactor power operation. A high pressure/low pressure interlock is provided to prevent opening of the isolation valve when the reactor pressure is higher than the FAPCS design pressure.

Interlock Systems

Redundant reactor pressure instruments provide a high-pressure signal to FAPCS HP/LP interlock when the reactor pressure exceeds the setpoint determined based on the design pressure of the low pressure FAPCS piping. Upon receipt of a high reactor pressure signal, the HP/LP interlock circuit initiates a signal to close the isolation valves and prevent them from opening.

Other than the isolation valves, the ESBWR design has no interlocks that isolate safety-related from nonsafety-related piping during LOCA, because there are no piping interfaces separating safety-related and nonsafety-related portions of piping systems.

7.1.1.8 Control Systems

Nuclear Boiler System Instrumentation

Redundant safety-related instrumentation is provided to monitor reactor vessel water level and reactor vessel pressure for operator monitoring and inputs to safety systems during normal, transient, and accident conditions.

Nonsafety-related instrumentation provides indication of reactor coolant and vessel temperatures, reactor vessel water level, and reactor vessel pressure.

Rod Control and Information System

Nonsafety-related I&C provide the capability to control reactor power level by controlling the movement of the control rods in the reactor core during manual, semi-automated, and automated modes of plant operations. The automated thermal limit monitor (ATLM) subsystem automatically enforces fuel operating thermal limits minimum critical power ratio (MCPR) and maximum linear heat generation rate (MLHGR) when reactor power is above the low power setpoint (LPSP).

Feedwater Control System (FWCS)

A highly reliable and triplicate redundant nonsafety-related I&C both automatically and manually regulates the flow of feedwater into the reactor pressure vessel to maintain predetermined water level limits during minor transients and normal plant operating modes.

Plant Automation System (PAS)

Nonsafety-related I&C provides automatic startup/shutdown algorithms and controls, regulates reactivity during criticality control, provides heatup & pressurization control, regulates reactor power, and provides automatic power generation control during power operation.

Steam Bypass and Pressure Control System (SBPC)

A highly reliable and triplicate redundant nonsafety-related I&C controls reactor pressure during plant startup, power generation and shutdown modes of operation, by directly controlling the

turbine bypass and indirectly controlling turbine control valve position by sending pressure regulation demand signals to the Turbine Control System - Electro-Hydraulic Control.

Neutron Monitoring System - Nonsafety-related Subsystems

The nonsafety-related Automated Fixed In-core Probe (AFIP) provides a signal proportional to the axial neutron flux distribution at the radial core locations of the Local Power Range Monitor (LPRM) detectors. The signal facilitates fully automated, precise, reliable calibration of LPRM gains and provides axial power measurement data for three dimensional core power distribution determination. The nonsafety-related MRBM Subsystem logic issues a rod block signal that is used in the RCIS logic to enforce rod blocks that prevent fuel damage by assuring that the minimum critical power ratio (MCPR) and maximum linear heat generation rate (MLHGR) do not violate fuel thermal safety limits.

Containment Inerting System

Nonsafety-related I&C establishes and maintains an inert atmosphere within the primary containment during plant operating modes, except during plant shutdown for refueling or equipment maintenance and during limited periods of time to permit access for inspection at low reactor power.

7.1.1.9 Diverse Instrumentation and Controls

Although not required for safety, Diverse I&C is provided to address Branch Technical Position HICB-19 on Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems, in addition to the ATWS mitigation features, which provide alternate control rod insertion, boron injection, and feedwater runback. (The ATWS mitigation function using liquid boron injection is part of diverse I&C functions, which is safety-related and is included as part of SSLC.) This diverse I&C function, called Diverse Protection System (DPS), is implemented in a highly reliable triplicate redundant control system whose sensors, hardware and software are different than any of the safety-related I&C platforms.

The following diverse actuation functions are provided in this DPS:

(1) A set of protection logics that provide diverse means to scram the reactor via control rod insertion using separate and independent sensors, hardware and software from the primary RPS.

(2) A set of ESF initiation logics that provide diverse means to initiate certain ESF functions using separate and independent sensors, hardware and software from the primary ESF systems.

(3) A set of alternate rod insertion (ARI) and associated logics (e.g., control rod run in) via control rod insertion through alternate means by opening the three sets of air header dump valves of the Control Rod Drive system. This is also part of the ATWS mitigation function.

The diverse protection system provides both manual and automatic initiation of the above functions.

7.1.1.10 Data Communication Systems

The Essential Distributed Control & Information System (E-DCIS) and Non-Essential Distributed Control & Information System (NE-DCIS) provide distributed control and instrumentation data communications networks to support the monitoring and control of interfacing plant safety and non-safety systems. They provide the electrical devices and circuitry (such as multiplexing units, data transmission line and transmission controllers) between sensors, display devices, controllers and actuators. They also provide acquisition and communication software required to support the function of transmitting plant-wide data for distribution control and monitoring.

Within the NE-DCIS, the various distributed plant computers and workstations support both display, alarm, monitoring and control functions that increase the efficiency of plant performance by performing functions, calculations and nonsafety-related system controls during startup, normal, and shutdown modes of plant operation. The various plant computers additionally provide both local and permanently archived records of plant operation. The plant computer functions also drive nonsafety-related display and control equipment in the main control room and provide supervisory control of plant automation features.

7.1.2 Identification of Design Bases and Safety Criteria

7.1.2.1 General

The I&C design bases address the performance of the systems intended function while satisfying the applicable general design criteria, regulatory guides, industry standards, and other documents.

The safety design basis for a safety-related system states the unique functional design requirements that establish the limits to satisfy the safety objectives. The general functional requirement portion of the safety design basis presents those requirements that have been determined to be sufficient to ensure the adequacy and reliability of the system from a safety viewpoint.

10 CFR 50.2 Safety Design Bases

Safety-related systems provide actions necessary to assure safe plant shutdown to protect the integrity of radioactive material barriers or prevent the release of radioactive material in excess of allowable dose limits for design basis accidents. These safety-related systems consist of components, groups of components, systems, or groups of systems. A safety-related system may have a power generation design basis. The unique functional design requirements stated in the design basis establish the limits to satisfy the safety objectives

The technical design bases for the instrumentation and controls for each system are presented as specific subsections throughout Chapter 7.

Nonsafety Design Bases

Nonsafety-related (including power generation) systems are reactor support systems that are not required to protect the integrity of radioactive material barriers and do not prevent the release of radioactive material in excess of allowable dose limits. The I&C portions of these system may prevent the plant from exceeding preset limits that would otherwise initiate the action of safety-related systems.

Instrument Errors

The design considers instrument drift, testability, and repeatability in the selection of instrumentation and controls and in the determination of setpoints. Adequate margin between safety limits and instrument setpoints is provided to allow for instrument error. The safety limits and allowable values are provided in the plant Technical Specifications. The amount of instrument error is determined by test and experience. The setpoint is selected based on the known error; since almost all of the I&C is microprocessor based and almost all of the instrument loop error is in the sensor since discrete setpoints do not drift. The recommended test frequency is greater on instrumentation that demonstrates a stronger tendency to drift.

The system allowable values for setpoints are listed in the plant Technical Specifications for each safety-related system. The actual settings are determined based on operating experience and conservative analyses. The settings are high enough to preclude inadvertent initiation of the safety action but low enough to assure that significant margin is maintained between the actual setting and the limiting safety-related system settings. The margin between the limiting safety-related system settings and the actual safety limits includes consideration of the maximum credible transient in the process being measured.

The periodic test frequency for each variable is determined from historical data on setpoint drift and from quantitative reliability requirements for each system and its components.

Testing and Inspection

The testing and inspection capabilities for the instrumentation and controls for each system are presented as specific subsections in Chapter 7.

7.1.2.2 Conformance to Regulatory Requirements and Industry Standards

The applicability of the following regulatory requirements and industry standards to the instrumentation and controls for the various systems are presented in the following subsections:

- Title 10 Code of Federal Regulations, including TMI Action Plan Requirements
- NRC Regulatory Guides
- Industry codes and standards
- Branch Technical Positions

The specific regulatory acceptance criteria and guidelines requirements applicable to each of these systems important to safety identified in the Standard Review Plan are identified and tabulated in Table 7.1-1 The regulatory requirements applicability matrix of Table 7.1-1 is followed in Section 7.2 through Section 7.9 for the regulatory conformance discussions of each

specific system. The degree of applicability and conformance, along with any clarifications or justification for exceptions, are presented in the evaluation sections for each specific system. General I&C conformance is discussed in the following subsections. For those safety I&C systems that are identical or very similar in architecture design to those previously reviewed by NRC (ABWR Certification), or those where the adequacy of the system is based upon prior NRC approval, such architecture design of those systems are identified in the system description sections of each specific system in Section 7.2 to Section 7.9. Where differences in design or architecture between the ESBWR and designs in prior NRC approvals, such differences are identified with adequate basis for NRC's review.

Title 10 Code of Federal Regulations

10 CFR 50.55a (Codes and Standards):

10 CFR 50.55a(a)(1) and 50.55a(h) are applicable to the instrumentation and control equipment. 10 CFR 50.55a(h) requires the application of IEEE 279 for protection systems. However, Regulatory Guide 1.153, Section B, states: "Compliance with the provisions of IEEE Std. 603-1980, as supplemented in Section C of this guide, is considered by the NRC staff to satisfy the provisions of IEEE Std. 279-1971." Therefore, because RG 1.153 (IEEE 603) is addressed for each system, IEEE 279 is not separately addressed.

10 CFR 50.34(f) (Conformance to TMI Action Plan Requirements):

Response to TMI related matters is generally addressed in Chapter 1, Appendix 1A. TMI action plan requirements are identified relative to the C&I systems in Table 7.1-1. The applicable systems are generally designed to conform. However, because of the design features of the ESBWR, several of these requirements are not applicable. These are identified as follows:

II.K.3.13 — HPCI and RCIC Initiation Levels

II.K.3.15 — Isolation of HPCI and RCIC (Turbine Driven)

II.K.3.21 — Automatic Restart of LPCS and LPCI

II.K.3.22 — RCIC Automatic Switchover of Suction Supply

For the others, the degree of conformance, along with any clarifications or exceptions, is discussed in the safety evaluation subsections of Sections 7.2 through 7.9.

10 CFR 50.62 (ATWS):

The ESBWR is designed with ATWS mitigation functions, as described in Section 7.8.

10 CFR 52.47(a)(1)(iv) Resolution of Unresolved and Generic Safety Issues

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi) ITAAC in Design Certification Applications

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii) Interface Requirements

- Conformance: Interface material is provided in Tier 1.

10 CFR 52.47(a)(2) Level of Detail

- Conformance: The level of detail provided for the RPS within the Tier 1 and Tier 2 documents conforms to this BTP.

10 CFR 52.47(b)(2)(i) Innovative Means of Accomplishing Safety Functions

- Conformance: The ESBWR is designed with innovative means of accomplishing safety functions, as delineated in Section 1.5.

10 CFR 52.79(c), ITAAC in Combined License Applications

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 50 Appendix A, General Design Criteria (GDC):

Conformance with NRC General Design Criteria (10 CFR 50 Appendix A) is discussed in Section 3.1. The applicability of GDC to each system is presented in Table 7.1-1. Specific conformance of the I&C systems themselves is addressed in Sections 7.2 through 7.7.

Staff Requirements Memoranda (SRM)

SRM to SECY 93-087 II.Q (Defense Against Common-Mode Failures):

The ESBWR digital I&C is designed with defense-in-depth and diversity for defense against common-mode failures. Section 7.8 includes the description of the diverse instrumentation and control system that specifically addresses the requirements of this SRM.

SRM to SECY 93-087 II.T (Control Room Annunciator/Alarm Reliability)

Section II.T of SECY 93-087 applies specifically to the post-accident monitoring requirement, which is described in Section 7.5. The ESBWR alarm system meets the intent of the EPRI requirements for redundancy, independence, and separation in that the "alarm system" is considered redundant. Alarm points are sent via dual network to redundant message processors on dual power supplies. The processors are dedicated and only do alarm processing. The alarms are displayed on multiple independent VDUs (dual power supplies on each). The alarm tiles are driven by redundant data links (dual power). The alarm tile processor is redundant. Each alarm tile has at least two LEDs. The horn and voice speaker are not redundant. Test buttons are available to test the horn(s) and all the lights. There are no alarms requiring manually controlled actions for safety systems to accomplish their safety function. Thus the requirements for Class 1E equipment and circuits are not applicable.

Conformance to Regulatory Guides

A discussion of the general conformance of the I&C equipment to the Regulatory Guides is as follows. Individual system conformance, along with any clarifications or exceptions, is addressed in the Safety Evaluation subsections within Sections 7.2 through 7.9.

Regulatory Guide 1.22 - Periodic Testing of Protection System Actuation Functions — Safety-related systems have provision for periodic testing. Proper functioning of analog sensors can be verified by channel cross-comparison and is done continuously by the plant computer functions. Some actuators and digital sensors, because of their locations, cannot be fully tested during actual reactor operation. Such equipment is identified and provisions for meeting the requirements of Paragraph D.4 (per BTP HICB-8) are discussed in the Safety Evaluation subsections within Sections 7.2 through 7.9.

Regulatory Guide 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems — Bypass indications are designed to satisfy the requirement of IEEE 603, Paragraph 5.8.3, and Regulatory Guide 1.47. The design of the bypass indications allows testing during normal operation and is used to supplement administrative procedures by providing indications of safety-related systems status.

Bypass indications are designed using isolation devices that preclude the possibility of any adverse electrical effect of the bypass indication circuits on the plant safety-related system.

Regulatory Guide 1.53 - Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems — The safety-related system designs conform to the single failure criterion.

Regulatory Guide 1.62 - Manual Initiation of Protective Actions — Manual initiation of the protective action is provided at the system level for safety-related systems.

Regulatory Guide 1.75 - Physical Independence of Electric Systems — The safety-related system designs conform to the physical independence criterion.

The I&C of the safety-related systems complies with the independence and separation criteria for redundant systems in accordance with Regulatory Guide 1.75 or by implementation of the following alternates:

- Associated circuits installed in accordance with IEEE 384, Section 5.5.2(1), are subject to the requirements of Class 1E circuits for cable derating, environmental qualification, flame retardants, splicing restrictions, and raceway fill unless it is demonstrated that Class 1E circuits are not degraded below an acceptable level by the absence of such requirements.
- The method of identification used (IEEE 384, Section 6.1.2) preclude the need to frequently consult any reference material to distinguish between Class 1E and non-Class 1E circuits, between non-Class 1E circuits associated with different redundant Class 1E systems, and between redundant Class 1E systems.
- First sentence of IEEE 384, Section 6.8 is implemented as follows:
  - Redundant Class 1E sensors and their connections to the process system shall be sufficiently separated so that required functional capability of the protection system are maintained despite any single design basis event.
- Non-Class 1E instrumentation circuits are exempted from the provisions of IEEE 384, Section 5.6, provided they are not routed in the same raceway as power and control cables (unless the cables are optical fiber) or are not routed with associated cables of a redundant division.

Regulatory Guide 1.97 - Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident — Instrumentation and controls are designed to meet the requirements of Regulatory Guide 1.97. Details of design implementation are discussed in Section 7.5.

Regulatory Guide 1.105 - Instrument Setpoints for Safety-Related Systems — The instrumentation and control systems are consistent with the requirements of Regulatory Guide 1.105. The applicable trip setpoint (instrument setpoint) allowance value (technical specification limit) and the analytical or design basis limit are provided in separate documentation. These parameters are appropriately separated from each other based on instrument accuracy, calibration capability and design drift (estimated) allowance data. The setpoints are within the instrument best-accuracy range. The established setpoints provide margin to satisfy both safety requirements and plant availability objectives.

Regulatory Guide 1.118 - Periodic Testing of Electric Power and Protection Systems — The instrumentation and control systems are consistent with the requirements of Regulatory Guide 1.118, with the following clarifications of the regulatory guide requirements:

- Position C.6b — Trip of an associated protective channel or actuation of an associated Class 1E load group is required on removal of fuses or opening of a breaker only for the purpose of deactivating instrumentation or control circuits.
- Position C.2 — Insofar as is practical and safe, response time testing is performed from sensor inputs (at the sensor input connection for process instruments) to and including the actuated equipment.

Regulatory Guide 1.151 Instrument Sensing Lines — The instrument sensing lines are designed to satisfy the requirements of Regulatory Guide 1.151. Such lines are used to perform both safety-related and nonsafety-related functions. However, there are four redundant and separate sets of instrument lines, each having Class 1E instruments associated with one of the four electrical Class 1E divisions. The Reactor Protection System logic requires any two out of the four signals to scram. If a channel is bypassed, the logic is two-out-of-three. Also, emergency core cooling functions are redundant throughout the four divisions and the feedwater system is designed with fault-tolerant triplicate digital controllers using separate sensors from the safety-related sensors. Therefore, the systems are designed such that no single failure could cause an event and at the same time prevent mitigating action for the event.

Regulatory Guide 1.152 - Computer Software Used in Safety-Related Systems — Criteria and guidelines stated in ANSI/IEEE-ANS-7-4.3.2, as endorsed by Regulatory Guide 1.152 are used as a basis for design procedures established for programmable digital equipment.

DG-1130/IEEE Std. 7-4.3.2-2003 Summary

Reg Guide 1.152 is the main regulatory guide on digital computers in safety systems in nuclear power plant. Draft Reg Guide DG-1130 will become RG 1.152 Rev.2 after it is officially issued. DG-1130 endorses and refers to IEEE 7-4.3.2 – 2003 and IEEE 603-1998 for specific criteria details.

The content of DG-1130 is similar to Reg Guide 1.152 Rev.1, except in certain areas that some additional requirements are specified. One major requirement area in DG-1130 contains discussions on digital I&C equipment common mode failure issues. The concern is related to the possibility that a design error in the software in redundant channels of a safety system could lead to common-cause or common-mode failure of the safety system function. Conditions may exist under which some form of diversity may be necessary to provide additional assurance beyond that provided by the design and QA programs that incorporate software QA and V&V. The design techniques of functional diversity, design diversity, diversity in operation, and diversity within the four echelons of defense in depth can be applied as defense against common-cause failures. The justification for equipment diversity, or for the diversity of related system software such as a real-time operation system, must extend to equipment components to ensure that actual diversity exists. Claims for diversity based on different manufacturers are insufficient without consideration of the above. Other considerations such as functional and signal diversity, that lead to different software requirements form a stronger basis for diversity. DG-1130 endorses IEEE Std. 7-4.3.2 – 2003. It also refers to NUREG SRP Sec 7 BTP HICB-19 (June 1997 Rev.4) for additional guidance. DG-1130 contains extensive requirements on "Security".

The following positions are noted in IEEE Std. 7-4.3.2-2003:

- The main text portions of IEEE 7-4.3.2 is similar to its 1993 version, with more extensive requirements incorporated, i.e., software development, V&V, software configuration management, equipment qualification, self-diagnostics, independence, reliability. There is no specifics details on diverse method requirements.

- Annex B "Diversity Requirements Determination" basically the same as the 1993 version. This annex provides a methodology for determining the need for diversity. Three approaches are mentioned: functional diversity (e.g., ATWS); defense-in-depth analysis (design features diversity analysis in different echelons such as RPS, ESF, controls, etc); diverse design (combination of computer and non computer channels, separate specs/hardware/software, etc.) This annex requirements are "soft" such that in both of the first two approaches it stated that it is acceptable to use identical software. NRC DG-1130 does not endorse this Annex B.

- Annex C "Dedication of existing commercial computers": This is similar to the 1993 version. NRC does not endorse this annex.

- Annex E, "Communication Independence": This is similar to the annex in the 1993 version. NRC does not endorse this annex.Annex F, "Computer reliability": This is similar to the annex in 1993 version. NRC states that quantitative reliability goals are not the only means, and does not endorse this method as the sole means of meeting the regulations for reliability of digital computers. NRC acceptance is based on deterministic criteria.

ESBWR Safety I&C System compliance to DG-1130/IEEE Std. 7-4.3.2-2003

Reg Guide 1.152 Rev.1 has been followed in the design of ABWR safety I&C systems, and the ESBWR safety I&C, being very similar or identical in design approach and in safety design requirements, also meets the requirements of Reg Guide 1.152 Rev.1. DG-1130 includes additional requirements applicable to digital computer-based safety I&C equipment. The ESBWR compliance to these additional DG-1130 requirements are summarized as follows.

Defense against software common mode failures: GE has evaluated BTP-HICB-19 requirements including the acceptance criteria on defense-in-depth and diversity and defense against common mode failures, on the four echelons of defense against common-mode failures: control systems, reactor trip system, ESFAS, and monitoring and indicators functions. Based on GE's evaluation, to fully address the requirements of BTP HICB-19 and DG-1130 on defense-in-depth and diversity and defense against common mode failures, the Diverse Protection System (DPS) is developed to back up the primary safety I&C system protection functions. The DPS is implemented with totally separate and independent equipment from the primary Safety I&C protection systems (RPS and SSLC/ESF). The DPS is implemented in addition to the ATWS/Standby Liquid Control System function.. Detailed description of the DPS and the description of defense-in-depth and diversity and defense against common mode failure are included in Section 7.8

Software development process: The software development process of the ESBWR safety I&C systems (including systems important to safety) will follow the guidelines of BTP HICB-14. Software development process plans will be developed for ESBWR safety I&C design implementation including Software Management Plan, Software Development Plan, Software Verification and Validation Plan, Software Configuration Management plan, and Software Safety Plan, etc., as required by BTP HICB-14. Actual detailed hardware and software design implementation will follow the guidelines specified by these plans as part of the DAC process.

Equipment qualification, self-diagnostics, independence, reliability: IEEE Std. 603 specifies these requirements applicable to safety I&C system equipment, as described in Section 7.1.2.3.3. The ESBWR safety I&C systems meet the requirements of IEEE Std. 603, and above requirements in areas applicable to digital computer-based equipment.

Security: The security requirements included in DG-1130 will be evaluated and incorporated as appropriate and needed in the ESBWR safety I&C design, both on plant hardware security measures and software security measures. The software development process plans will be developed with the security requirements incorporated for actual detailed design implementation.

Regulatory Guide 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems — Safety-related systems are designed to satisfy the requirements of IEEE 603, as endorsed by Regulatory Guide 1.153. Clarifications or exceptions (if any) for any of the provisions are discussed in the individual systems safety evaluation sections.

Regulatory Guide 1.168 - Verification, Validation, Reviews, And Audits For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants.

This regulatory guide endorses IEEE Std. 1012, IEEE Standard for Software Verification and Validation Plans, and IEEE Std. 1028, IEEE Standard for Software Reviews and Audits. IEEE Std. 1012 is acceptable for providing high functional reliability and design quality in software used in safety systems. IEEE Std. 1028 is acceptable for carrying out software reviews, inspections, walkthroughs, and audits subject to certain provisions. Safety-related systems such as SSLC software development uses the guidance in these standards as discussed in Appendix

7B to develop portions of the overall software development plan and thus complies with this regulatory guide.

Regulatory Guide 1.169 - Configuration Management Plans For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants

This regulatory guide endorses IEEE Std. 828, IEEE Standard for Software Configuration Management Plans, and ANSI/IEEE Std. 1042, IEEE Guide to Software Configuration Management. These standards, with the clarifications provided in the Regulatory Position, describe acceptable methods for providing high functional reliability and design quality in software used in safety systems. Safety-related systems such as SSLC software development uses the guidance in these standards as discussed in Appendix 7B to develop portions of the overall software development plan and thus complies with this regulatory guide.

Regulatory Guide 1.170 - Software Test Documentation For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants

The requirement contained in IEEE Std. 829, IEEE Standard for Software Test Documentation, provide an acceptable approach for meeting the requirements of 10 CFR Part 50 as they apply to the test documentation of safety system software subject to the provisions in this guide. Safety-related systems such as SSLC software development uses the guidance in these standards as discussed in Appendix 7B to develop portions of the overall software development plan and thus complies with this regulatory guide.

Regulatory Guide 1.171 - Software Unit Testing For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants

This regulatory guide endorses IEEE Std. 1008, IEEE Standard for Software Unit Testing, subject to the provisions in this guide. This standard defines an acceptable method for planning, preparing for, conducting, and evaluating software unit testing. Safety-related systems such as SSLC software development uses the guidance in this standard as discussed in Appendix 7B to develop portions of the overall software development plan and thus complies with this regulatory guide.

Regulatory Guide 1.172 - Software Requirements Specifications For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants

This regulatory guide endorses IEEE Std. 830, Recommended Practice for Software Requirements Specifications, as amended in the Regulatory Position. This standard describes current practice for writing software requirements specifications for a wide variety of systems. It is not specifically aimed at safety applications; however, it does provide guidance on the development of software requirements specifications that will exhibit characteristics important for developing safety system software. This is consistent with the goal of ensuring high-integrity software in reactor safety systems. Safety-related systems such as SSLC software development uses the guidance in this standard as discussed in Appendix 7B to develop portions of the overall software development plan and thus complies with this regulatory guide.

Regulatory Guide 1.173 - Developing Software Life Cycle Processes For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants

This regulatory guide endorses IEEE Std. 1074. The standard describes, in terms of inputs, development, verification or control processes, and outputs, a set of processes and constituent activities that are commonly accepted as composing a controlled and well-coordinated software-development process. It describes inter-relationships among activities by defining the source activities that produce the inputs and the destination activities that receive the outputs. The standard specifies activities that must be performed and their inter-relationships; it does not specify complete acceptance criteria for determining whether the activities themselves are properly designed. Therefore, the standard should be used in conjunction with guidance from other appropriate regulatory guides, standards, and software engineering literature. Safety-related systems such as SSLC software development uses the guidance in this standard as discussed in Appendix 7B to develop portions of the overall software development plan and thus complies with this regulatory guide.

Conformance to Industry Standards

The safety evaluation subsections throughout Chapter 7 address the regulatory guides in accordance with the SRP. Those IEEE standards that are endorsed by regulatory guides are not addressed separately.

Other codes or standards not mentioned in the SRP may be utilized in specific system applications. These are identified in the system description and the corresponding reference section. Some IEEE standards applicable to the I&C equipment are addressed in other chapters in accordance with the SRP format. These are identified as follows:

IEEE 323 - Qualifying Class 1E Equipment for Nuclear Power Generating Stations — Safety-related systems are designed to meet the requirements of IEEE 323. Environmental qualification is addressed in Section 3.11.

IEEE 344 - Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations — Safety-related instrumentation and control equipment is classified as Seismic Category I and designed to withstand the effects of the safe shutdown earthquake (SSE) and remain functional during normal and accident conditions. Qualification and documentation procedures used for Seismic Category I equipment and systems satisfy the provisions of IEEE 344 as indicated in Section 3.10.

Conformance to Branch Technical Positions

Applicable branch technical positions (BTPs) are identified relative to the C&I systems in Table 7.1-1. The systems are generally designed to conform to the BTPs. The degree of conformance, along with any clarifications or exceptions, is discussed in the Safety Evaluation subsections of Sections 7.2 through 7.9.

In the BTP HICB-16 requirements, it is stated that the application should (1) describe the resolution of unresolved and generic safety issues applicable to the I&C systems, and (2) describe the interface requirements to be met by portions of the plant for which the application does not seek certification and which are necessary to ensure proper functioning of the I&C system, and (3) identify and describe the validation of innovative means of accomplishing I&C system safety functions. Applications that propose the use of computers for systems important to safety should describe the computer system development process. Application that propose the

use of computers for reactor trip system (RTS) and engineered safety features actuation system (ESFAS) functions should also describe the design of the overall I&C systems with respect to defense-in-depth and diversity requirements.

The ESBWR does not have any unresolved and generic safety issues applicable to the I&C systems. Such unresolved and generic safety issues are described in DCD Section 1.11. There are several new generic issues that are related to I&C systems, such as failure of protective devices on essential equipment, Electromagnetic pulse, identification of protection system instrument sensing lines, and protection system testability. The above issues either are not applicable to ESBWR safety I&C systems design or the ESBWR has addressed those issues in its safety I&C design.

Within the scope of the ESBWR DCD submitted for certification application, there are no such interface requirements as described here that falls into the above category.

The validation of innovative means of accomplishing I&C system safety functions does not apply to the ESBWR safety I&C design submitted for this certification application.

For the description of computer system development process, the compliance to BTP HICB-14 is explained and summarized in Appendix 7B of this chapter. GE will prepare and submit to NRC the software development process plans required by BTP HICB-14 for NRC's review and approval, as part of the ESBWR Certification activity.

ESBWR safety I&C systems (RPS and SSLC/ESF) use computers for their logic functions. Description of the safety I&C systems design with respect to defense-in-depth and diversity and defense against common mode failures is included in Section 7.8, together with the description of the Diverse Protection system, which specifically addresses to the issues of defense-in-depth and diversity and defense against common mode failures

7.1.2.3 Conformance to 10 CFR 50.55a(h) and IEEE Std. 603

As requested by 10 CFR 50.55a(h), IEEE Std. 603 endorsed by Reg. Guide 1.153, superceding IEEE Std. 279, is followed for compliance of criteria for safety systems for nuclear power generation stations. In this section, a summary description is included to demonstrate the overall ESBWR safety I&C systems compliance of IEEE Std. 603, according to the guidelines described in NUREG 0800, SRP Appendix 7.1-C. For specific descriptions of functional compliances of the IEEE Std 603 criteria by various safety-related systems, the discussions are referred to the various subsections of this chapter, as listed in the various sections below.

7.1.2.3.1 Scope per IEEE Std. 603

The scope of IEEE Std 603 includes all I&C safety systems which are systems covered in Section 7.2 through 7.6. Except for the requirements for independence between control systems and protection systems, IEEE Std 603 does not directly apply to nonsafety systems. Applicable considerations include design basis, redundancy, independence, single failures, qualification, bypasses, status indication, and testing. The IEEE Std 603 also applies to those parts of the digital data communication that supports safety system functions. The design of ESBWR I&C

safety systems is in compliance with the IEEE Std 603 requirements as described in the above scope, based on the definition and explanation of IEEE Std 603 Section 1.

7.1.2.3.2 Safety System Designation (Design Basis) per IEEE Std. 603

Section 4 of IEEE Std 603 requires in part that a specific basis be established for the design of each safety system. The design basis should address all system functions necessary to fulfill the system's safety intent. The design basis should address the requirements of 10 CFR 50 Appendix A, GDC 20, which requires that the protection system be initiated automatically to assure that acceptable fuel limits are not exceeded, and that accident condition be sensed so to initiate the operation of systems and components important to safety. This GDC mainly addresses to reactor trip systems (RTS) and engineered safety features actuation systems (ESFAS). Information provided for each design basis item should be sufficient to enable the detailed design of the system to be carried out. The design of ESBWR I&C safety systems is in compliance with the IEEE Std 603 requirements as described in the above summary. Safety system design basis descriptions are included in the various sections of this chapter as indicated below.

Reactor Trip System

Reactor Protection System: Section 7.2.1.1

Neutron Monitoring System: Section 7.2.2.1

Suppresion Pool Temperature Monitoring: Section 7.2.3.1

Engineered Safety Features Systems

Emergency Core Cooling System: Section 7.3.1

Leak Detection and Isolation System: Section 7.3.3.1

Safety System Logic and Control: Section 7.3.4.1

Standby Liquid Control System: Section 7.4.1.1

Remote Shutdown System: Section 7.4.2.1

Reactor Water Cleanup/Shutdown Cooling System: Section 7.4.3.1

Isolation Condenser System: Section 7.4.4.1

Containment Monitoring System: Section 7.5.2.1

7.1.2.3.3 Safety System Criteria per IEEE Std. 603

This section mainly requires that the safety systems shall maintain plant parameters within acceptable limits established by design basis events, that the safety systems meet all key design criteria stated in this section, and that the protection system has been qualified to demonstrate that the performance requirements are met.

Single Failure Criterion (IEEE-603, 5.1)

This section requires that any single failure within the safety system shall not prevent proper protective action at the system level when required, and it should be confirmed that requirements of the single failure criterion are satisfied. The ESBWR safety-related I&C systems satisfy the single failure criteria. All safety-related I&C systems have multiple (four) redundant and independent channels, including redundant and independent sensors assigned to each of the redundant channels. The trip logic is 2-out-of-4 logic. Any failed channel caused by single failure associated with this channel does not affect the safety system to perform its safety protection functions because of this 2-out-of-4 logic. The failed channel can be bypassed without affecting the performance of the safety system functions, with the logic reverted to 2-out-of-3. Descriptions of design of the safety-related I&C systems that addressed the single failure criterion are included in the various subsections as shown in Table 7.1-2.

Digital computer-based I&C systems share data, data transmission, and functions which may become a source of concern that a design using shared databases and process equipment has the potential to propagate a common-mode failure of redundant equipment. The ESBWR safety-related I&C systems include a diverse protection system design to specifically address and mitigate any common-mode failure concern of digital computer-based systems. This design, in addition to the ATWS/SLCS design, fully addresses the requirements of Staff Requirements Memorandum SECY-93-087 and BTP HICB-19. This design is described in Section 7.8.

Completion of Protective Action (IEEE Std. 603, 5.2)

In the ESBWR, completion of protective action, once initiated automatically or manually, is accomplished by the RPS with seal in logic. Specific description is included in Section 7.2.1.2 and in other subsections as shown in Table 7.1-2.

Quality (IEEE Std. 603, 5.3)

All equipment is provided under GE's Appendix B quality program. The NRC accepted GE Quality Assurance Program with its implementing procedures constitute the Quality Assurance system that is applied to the GE ESBWR safety-related I&C system design. It satisfies all applicable requirements of the following: 1) 10 CFR 50 Appendix B; 2) ANSI/ASME NQA-1; 3) ISO 9001. As an example, Section 9 of Reference 7.1-5 describes special quality program aspects related to GE's programmable digital safety-related I&C equipment.

Equipment Qualification (IEEE Std. 603, 5.4)

It is required that safety system equipment be designed to meet the functional performance requirements over the range of normal environmental conditions for the area in which it is located. Equipment qualification typically includes electromagnetic interference qualification, seismic qualification, and other environmental condition qualification such as temperature, humidity, radiation, and pressure. The ESBWR safety I&C systems are designed to meet the equipment qualification requirements set forth in IEEE Std. 603 and other associated equipment qualification requirements. The qualification was established using qualification methods set forth in General Electric Environmental Qualification Program, (Reference 7.1-7). The ESBWR safety I&C system components are designed to be qualified to operate in the normal and abnormal environments in which they are located.

For environmental qualification, the following areas are addressed:

Temperature and Humidity: The ESBWR safety I&C components are designed to be qualified using type testing and analysis to demonstrate that the components will perform all specified functions correctly when operated within the specified temperature range and relative humidity range. The components will be qualified in accordance with Reg. Guide 1.89 (IEEE 323 - 1974) and IEEE 323 – 1983. All qualification will be based on type testing. Plant-specific action will be required to confirm that the maximum control room temperatures plus mounting panel temperature rise, allowing for heat load of the safety I&C equipment, does not exceed the temperature limit, and that control room humidity is maintained within limits.

Pressure : The ESBWR safety I&C components are designed to be qualified by analysis to perform to specification for any absolute pressure in the range specified. Plant-specific action will be required to confirm that the maximum control room pressure does not exceed the specified limits.

Radiation: The ESBWR safety I&C components are designed to be qualified by analysis to perform within specification limits over its service life under the specified radiation conditions. Plant-specific action will be required to confirm that the maximum radiation levels where the equipment is located do not exceed the allowed limits.

Seismic Qualification: The ESBWR safety I&C components are designed to be qualified by type testing and analysis to demonstrate that the components will perform all specified functions correctly when operated within the specified seismic limits, and when mounted in accordance with the specified mounting methods. The ESBWR safety I&C components are to be qualified in accordance with the requirements of Reg Guide 1.100 (IEEE 344 - 1975). Qualification is based on type testing. Plant-specific action or analysis will be required to confirm that the maximum seismic accelerations at the mounting locations of the equipment do not exceed the allowed limits.

EMI Qualification: The ESBWR safety I&C components, when mounted in accordance with the specified mounting methods, are designed to be qualified by type testing and analysis to demonstrate that the components will perform all specified functions correctly when operated within the specified EMI limits. The ESBWR safety I&C equipment is designed to be not susceptible to electromagnetic disturbances from neighboring modules and does not cause electromagnetic disturbances to neighboring modules. The EMI qualification design follows the requirements specified in Mil-Std-462D, Mil Std. 461D, and IEC Standard 801, depending the specific requirement conditions. The ESBWR safety I&C equipment is to be qualified to perform within its specifications continuously while exposed to EMI environmental limits at the hardware mounting location. EPRI Report TR-102323 (Reference 7.1-8) is used for the envelope limits. The EMI susceptibility and emissions testing is performed by type testing using. In addition to the equipment design considerations, plant-specific actions are required to establish practices to control emission sources, maintain good grounding practices and maintain equipment and cable separation. Reference 7.1-5 has included more detailed descriptions of equipment qualification practices of GE's typical safety-related I&C equipment used in ABWR and is applicable to ESBWR.

System Integrity (IEEE Std. 603, 5.5)

The safety I&C systems are required to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. Other areas that are necessary to address as requirements include adequate system real-time performance for digital computer-based systems to ensure completion of protective action, evaluation of hardware integrity and software integrity (software safety analysis, as part of BTP HICB-14 requirements), fail in a safe state upon loss of energy or adverse environmental conditions, and the requirements for manual reset.

The ESBWR safety I&C systems meet the integrity requirements described in IEEE Std. 603. The ESBWR Reactor Trip System functions fail in the tripped state. The ESF logics fail to a state that the actuated component remains as-is. For the ESBWR RTIF functions, inoperable input instrument being detected will lead to channel trip. Hardware and software failures detected by self-diagnostics will cause trip actuation. Also, failure of hardware and software will not inhibit manual initiation of protective functions. More descriptions of system integrity design consideration are included in the system description subsections of the respective safety systems as outlined in Table 7.1-2.

Independence (IEEE Std. 603, 5.6)

The independence requirements address the independence between redundant portions of a safety system, between the safety systems and the effects of design basis events, and between the safety systems and other systems. Three aspects of independence are addressed in each case, i.e., physical independence, electrical independence, and communication independence. The ESBWR safety I&C systems meet these requirements. The ESBWR safety I&C systems have four redundant and independent channels, which are physically independent and separated, with independent electrical power source applied to each channel. There are no common switches shared by the four channels. The sensors used for each of the four channels are independent and physically separated from one another. Communication directly between the four channels are limited to the minimum such as channel trip signals and bypass status signals, and are through proper isolation devices such as using optic fibers.

For the independence between the safety systems and the effects of design basis events, these requirements are achieved basically through proper equipment qualification. Safety equipment is qualified for continued functional capability under the environment and location, in which the equipment is located where design basis events conditions are considered. Safety systems are totally separated and independent from nonsafety systems. Communication from safety systems to nonsafety systems is carried out with proper signal isolation devices (e.g., fiber optic cables) and data path gateway. Communication from nonsafety systems to safety systems are strictly prohibited, with only one exception, i.e., the data transmission of LPRM calibration gain adjustment factors which are calculated in the nonsafety plant computer function of the Non-Essential DCIS, to the safety-related LPRM/APRM equipment using proper signal isolation. However, this data transmission can only be implemented and accepted by the safety equipment with operator acknowledgment. This data transmission does not interfere with RPS or SSLC/ESF protection functions. More descriptions of safety system independence design are included in the system description subsections of the respective safety systems as outlined in Table 7.1-2.

Capability for Testing and Calibration (IEEE Std. 603, 5.7)

The capability for testing and calibration of safety system equipment are required to be provided during power operation and required to duplicate the performance of the safety function as closely as practicable. It is permitted that tests can be performed in overlapping test segments in order to test one safety function. Also, the I&C design should allow for tripping or bypass of individual functions in each safety system channel. The ESBWR safety I&C systems meet the requirements as outlined in this IEEE 603 section. The safety functions of each safety channel can be tested on line with the tested channel bypassed from the 2-out-of-4 trip logic. The I&C equipment has built-in self-diagnostic functions to identify critical failures such as loss of power and data errors, etc. More descriptions of system testing and calibration are included in the system description subsections of the respective safety systems as outlined in Table 7.1-2.

Information Displays (IEEE Std. 603, 5.8)

Displays for manually controlled actions: Type A variables are those variables that provide the primary information required for the control room operators to take the specified manual actions for which no automatic control is provided and that are required for safety-related systems to accomplish their safety functions for design basis accident events. For ESBWR, there are no instruments in this application as Type A variables. More discussion on this subject is included in Section 7.5.1.

System Status Indication: The ESBWR safety and nonsafety I&C systems are provided with system status information that meet the requirements of IEEE 603. All pertinent system trip/logic status, parameter data values, equipment functional status and ESF actuator status are available to be displayed to the operator upon request. For safety systems, such information is available for each division/channel. Certain information important to plant operation and status monitoring are permanently displayed (on large wide display panels) in the main control room. Alarm (and annunciation) indications are also available in the main control room per system design requirements. Other than post accident safety display, the system status information is not safety-related.

Indication of Bypasses: For safety system protection functions, bypass status is continuously displayed to the operator. All bypass status information is available to be displayed per system design requirements. Certain bypass information is accompanied with alarm, when activated not as under normal operation conditions. More descriptions of system bypass and alarm conditions are included in the system description subsections of the respective safety systems as outlined in Table 7.1-2.

Location of Display: The locations of all displays located in the main control room are either on the main control console or on the large wide display panels visible and accessible to the operator. The ESBWR man machine interface system design (human system interface) includes design requirements and specifications on the classification of locations of various displays in the main control room. More detailed description of requirements on location of displays are included in Chapter 18, and the associated references of Chapter 18.

Control of Access (IEEE Std. 603, 5.9)

There are several means to implement access control to plant I&C equipment especially safety-related systems. Administrative control is used to implement control of access such as only

qualified plant personnel is allowed to have access of keys (doors, cabinets, keylock switches) and passwords to get access to plant equipment especially safety systems equipment. Only qualified plant personnel is allowed to exercise operations such as change of setpoints, instrument calibration, equipment testing, logic bypass operation, and access to other plant operation switches. Keys, passwords, and other security devices as per the requirements of RG 1.152 are used for qualified plant personnel to enter specific rooms, open specific equipment cabinets, get permission to enter specific electronic instrument for calibration, testing, setpoint changes, and gain access to safety system software and data, etc. However, software of safety systems are typically not changeable at the plant site as the safety system software is implemented as firmware (PROM) microprocessor. There is no access to safety system equipment and control via network from nonsafety system equipment.

Repair (IEEE Std. 603, 5.10)

The ESBWR safety I&C systems are designed to allow the timely recognition (such as through periodic self-diagnostic functions), location, replacement (such as through module replacement), repair and adjustment of malfunctioning equipment. The self-diagnostic function will locate the failure to the component level. Through individual channel bypassing, the failure component can be replaced or repaired on line without affecting the safety system protection function, with the trip logic reverted from 2-out-of-4 to 2-out-of-3. Single failure criterion is still maintained.

Identification (IEEE Std. 603, 5.11)

The ESBWR safety I&C system equipment satisfies with the identification requirements as specified in IEEE 603. Color coding is used as one of the major methods of identification. Safety system equipment is distinctly identified for each redundant portion of a safety system and with identifying markings. For digital computer-based system equipment, versions of computer hardware, programs, and software are distinctly identified. Configuration management is implemented to assist system program and software identification. Typically all hardware component or equipment units have identification label or nameplate.

Auxiliary Features (IEEE Std. 603, 5.12)

ESBWR safety I&C system auxiliary supporting features satisfy the requirements of this standard where applicable, such as safety related electrical system equipment of batteries, diesel generators, inverters, etc. Safety I&C systems are supported by four divisions of Class 1E uninterruptible power supply, and separately, four divisions of instrument power supply. They are also supported by dc batteries in case there is a loss of off-site and on-site AC power.

HVAC is an important auxiliary supporting feature that supports to maintain the necessary environmental conditions for the safety ESBWR I&C equipment. Under normal operating conditions and whenever the diesel generators is available, HVAC is provided to control the temperature/humidity of all I&C equipment in all of the buildings. Under loss of power condition (SBO or other), batteries are provided for continued safety I&C operation for 24 hours or 72 hours (post accident monitoring equipment), and continued operation of the nonsafety I&C equipment for two hours. HVAC will no longer be available to either control building or reactor building equipment (except the control building area as noted below). The safety I&C equipment will be qualified for the expected temperature rise. In the main control room area,

battery-operated nonsafety HVAC is provided to allow continued operation of the safety and nonsafety I&C for the approximate two hours of nonsafety battery capacity. Should the nonsafety HVAC (redundant) not be available, safety-related temperature sensors (with 2/4 logic) will trip the control room power that feeds the nonsafety I&C; the safety I&C is qualified for the resulting temperature rise. This scheme is used to protect the C&I equipment and maximize operator comfort. More description of the HVAC design is included in Chapter 9.

Other auxiliary features that support the safety I&C systems functions are designed such that these components will not degrade the safety system below an acceptable level.

Multi-Unit Stations (IEEE Std. 603, 5.13)

The ESBWR standard design submitted for NRC certification is a single-unit plant.

Human Factors Considerations (IEEE Std. 603, 5.14)

In the ESBWR I&C design, human factors are considered at the initial stage and will be considered throughout the design process, following the necessary regulatory and design guidelines (e.g., NUREG-0711), to assure that safety system design goals are met. Since the ESBWR safety I&C system design concept and architecture follows very closely and similar to the design of the ABWR, the ABWR human factors design practices will largely and effectively support the human factor engineering design of the ESBWR safety I&C systems. More specific information on human factor engineering design program, consideration and requirements are included in Chapter 18 and its associated references.

Reliability (IEEE Std. 603, 5.15)

The degree of redundancy, diversity, testability, and quality of the ESBWR safety I&C design is adequate to achieve the functional reliability necessary to perform its function. All equipment is provided under GE's Appendix B quality program. As an example, Section 9 of Reference 7.1-5 describes special quality program aspects related to GE's programmable digital safety-related I&C equipment. BTP-14 will be followed for software development processes to achieve reliable software design and implementation. Design measures to achieve defense against common mode failure have been included in the safety I&C design through many defense in depth and diversity measures including the incorporation of the Diverse Protection system described in Section 7.8. The ESBWR safety I&C system are included in the consideration of the ESBWR Probabilistic Risk Assessment (PRA), referenced in Chapter 19.

Common Cause Failure Criteria (IEEE Std. 603, 5.16)

The ESBWR has included defense in depth and diversity design consideration, and also has included a Diverse Protection System using both manual action and nonsafety diverse systems to provide means to accomplish the function that could otherwise be defeated by the common cause failure such as common mode software failure. The above design measures including the inclusion of the Diverse Protection System meet the requirements of RG 1.152 on common cause failure and the guidance of BTP HICB – 19. More descriptions of the defense against common mode failure and the Diverse Protection system are included in Section 7.8.

7.1.2.3.4 Sense, Command, and Execute Features per IEEE Std. 603

Automatic and Manual control

The ESBWR RPS and SSLC/ESF logics are designed to automatically initiate reactor scram trip and actuate the engineered safety features to mitigate the consequences of anticipated operational occurrences and design basis accidents. Such automatic protection actions are implemented via a 2-out-of-4 voting (of 4 divisions) whenever one or more process variables monitored and measured by the RPS and SSLC/ESF logics (in 4 divisions) reach the scram or ESF actuation setpoint. In the setpoint determination, appropriate setpoint value is selected for each process variable based on GE setpoint methodology that includes margins and errors. Appropriate instrument and equipment response times are also considered in the safety analyses.

The ESBWR safety I&C systems of RPS and SSLC/ESF manual initiation of protective functions at the system-level and division level is available. The manual controls are designed such that the information provided and display content and location are taken into consideration for easy operator access and action in the main control room. No single failure will prevent the initiation of the protection action. Further information regarding the design of manual controls and human factor engineering consideration, as well as plant manual operation procedure requirements, are included in Chapter 18 and its associated references. Additional descriptions of automatic and manual controls at system levels (RPS and SSLC/SEF) are included in Section 7.2.1.1, 7.2.1.2, 7.2.1.3, 7.2.1.5, 7.3.1.1, and 7.3.1.2.

Interaction between the Sense and Command Features and Other Systems

The ESBWR safety I&C protection systems are totally separated and independent from the nonsafety control systems such that any failure of nonsafety systems will not affect and will not prevent the safety protection system from performing its safety protection functions. Sensors used by safety I&C systems are not shared by nonsafety control systems. The Safety I&C systems meet the requirements of GDC 24. Additional descriptions of the safety I&C systems of RPS and SSLC/ESF are included in Section 7.2.1 and 7.3.4. (The only interface from nonsafety system to safety-related I&C is the data transmission of LPRM gain adjustment factor data from the plant computer system to the LPRM units. However such data transmission to LPRM units needs operator acknowledgment for implementation, and dose not interfere with reactor protection function or ESF actuation function.)

Derivation of system Inputs

To the extent feasible, the protection system inputs are derived from signals that directly measure the designated process variables. The only two RPS sensing inputs that are not direct measures of the variables are the reactor pressure vessel (RPV) water level and the loss of feedwater flow in the RPS scram logics. The RPV water level is measured by the delta pressure derived from the sensing line with a reference point. This method is a proven technology in BWR application. The loss of feedwater flow variable is represented by the loss of power generation bus signal, because when the power to the feedwater pump motor is lost, the feedwater flow also is immediately lost. The use of loss of power generation bus signal to represent the loss of feedwater flow signal meet the requirements of the safety analysis of Chapter 15. The RPS initiating circuits and SSLC/ESF logics are described in Section 7.2.1 and Section 7.3.

Capability for Testing and Calibration

The operational availability of the protection system sensors can be checked by perturbing the monitored variables, by cross-checking between redundant channels that bear a know relationship to each other and that have read-outs available, or introducing and varying a substitute input to the sensor of the same nature as the measured variable.

Operating Bypasses

Operating bypasses are implemented in the ESBWR safety I&C systems such as RPS, NMS, and SSLC. One example of such operating bypasses is associated with the trip function dependence on reactor operating mode. Requirements of IEEE Std. 603 are met by the ESBWR safety I&C operating bypass design. Specific descriptions of safety system operating bypasses are included in Section 7.2.1.5, Section 7.2.2.2, and Section 7.3.4.2.

Maintenance Bypass

Maintenance bypasses capability is incorporated in the design of the safety I&C systems. This is mainly for the purpose of equipment maintenance, testing, and repair of one individual division (channel) with the plant still under operating condition and without initiating any protection functions. Single failure criterion is maintained under such bypass condition. Maintenance bypass is always alarmed or indicated in the main control room. Maintenance bypass for safety I&C systems is typically applied through joystick bypass switch (with exclusive logic) where only one channel (out of four channels) is allowed to be bypassed at any given time. Technical Specification defines the time duration that a specific maintenance bypass condition is allowed to exist. Maintenance bypasses are initiated manually by the plant operator per administrative control. Specific descriptions of safety system maintenance bypasses are included in Section 7.2.1.5, Section 7.2.2.2, and Section 7.3.4.2.

Setpoints

The ESBWR Safety I&C system setpoints are defined, determined, and implemented based on the GE setpoint methodology approved by the NRC, referenced in Reference 7.2-1. This methodology meets the requirements of IEEE Std. 603.

7.1.2.3.5 Power Source Requirements

The ESBWR Safety I&C protection systems are supported by two independent power sources. Four divisions of Class 1E vital (uninterruptible) 120 VAC are used as the primary power source for the SSLC cabinets in which most components of the safety related protection systems are located. Similarly four Divisional Associated 120VAC Instrument and Control Power (ICP) are used as a secondary power source. Two divisions of the vital (uninterruptible) 120 VAC are also used as the power sources for the solenoids of the scram pilot valves. Two divisions of the 250VDC power sources are used for the backup scram valves solenoids, for scram reset permissive logic. Specific descriptions of safety system power sources are included in Section 7.2.1.2, 7.2.2.2, and 7.3.1.1, as well as in Chapter 8.

7.1.2.3.6 Additional IEEE Std. 603 Compliance Discussion applicable to RPS

In addition to above general descriptions of compliance to IEEE Std. 603, a more specific discussion on compliance of IEEE Std. 603 by the RPS and its supporting SSLC functions is included in this section. More supporting descriptions of the RPS and SSLC designs that address to the compliance of IEEE Std. 603 are included in Section 7.2.1 and 7.3.4.

Safety System Criteria

The RPS, including its SSLC logic, trip actuator logic, and trip actuators, is designed to comply with this requirement through automatic removal of electric power to the CRD scram pilot valve solenoids when a sufficient number of RPS variables exceeds the specified trip setpoint.

Single-Failure Criterion

The RPS has four completely separate divisions with separate sensors whose only interaction is at the trip logic level via optical isolation. The system is in full compliance with the single-failure criterion and Regulatory Guide 1.53

Quality

All RPS and SSLC components and modules and safety-related equipment of other systems providing inputs to the RPS are designed to maintain necessary functional capability under the extremes of conditions (as applicable) relating to environment, energy supply, malfunctions, and accidents, within which the equipment has been designed and qualified to operate continuously and without degradation.

Equipment Qualification

Instrument sensors and electrical components of the RPS and interfacing systems which are used for RPS functions are qualified for nuclear safety-related service for the function times and for the environment in which they are located. The RPS electrical Class 1E equipment, including the SSLC controllers and cabinets, is qualified by type test, data from previous operating experience or analysis, or any combination of these three methods to substantiate that all equipment which must operate to provide the safety system actions will be capable of meeting, on a continuing basis, the necessary performance requirements.

System Integrity

All RPS instrument channels, components, supporting SSLC equipment, and safety- related equipment of other systems providing inputs to the RPS are designed to maintain necessary functional capability under the extreme conditions relating to environment, energy supply, malfunctions, and accidents, within which the equipment has been designed and qualified to operate continuously and without degradation. See above Section 7.1.2.3.3 for general discussion.

Channel Independence

The RPS and supporting SSLC equipment are designed to assure that the effects of natural phenomena and of normal operation, maintenance, testing and postulated accident conditions on

redundant channels, divisions and equipment of the RPS will not result in the loss of the safety function of the system.

The redundant divisions of RPS/SSLC are electrically and physically separated from each other such that (1) no design basis event is capable of damaging equipment in more than one division and (2) no single failure, test, calibration or maintenance operation can prevent the safety function of more than one division.

Instrument channels that provide signals for the same protective function are independent and physically separated to accomplish the decoupling of the effects of unsafe environmental factors, electric transients and physical accident consequences and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunctions.

Control and Protection System Interaction

The channels for the RPS trip variables are electrically isolated and physically separated from the plant control systems in compliance with this design requirement.

Multiple redundant sensors and channels assure that no single failure can prevent protective action.

Derivation of System Inputs

The following RPS trip variables are direct measures of a reactor overpressure condition, a reactor overpower condition, a reactor instability condition, a gross fuel damage condition, or abnormal conditions within the reactor coolant pressure boundary:

- Reactor vessel low water level trip
- NMS (APRM/OPRM) divisional trip
- NMS (SRNM) divisional trip
- Drywell high pressure trip
- Reactor vessel high pressure trip

Other variables that could affect the RPS scram function itself, are thus monitored to induce scram directly include:

- Low charging pressure to control rod HCU accumulators
- High suppression pool temperature

The detection of MSIV closure and turbine stop valve closure (if a sufficient number of bypass valves do not open in time) is an appropriate variable for the Reactor Protection System. The desired variable is loss of the reactor heat sink; however, isolation (MSIV closure) or stop valve closure is the logical variable to inform that the steam path has been blocked between the reactor and the heat sink.

Due to the normal throttling action of the turbine control valves with changes in the plant power level, measurement of control valve position is not an appropriate variable from which to infer the desired variable, which is rapid loss of the reactor heat sink. Consequently, a measurement related to control valve closure rate is necessary. Protection system design practice has discouraged use of rate-sensing devices for protective purposes. In this instance, it was determined that detection of hydraulic actuator operation would be a more positive means of determining fast closure of the control valves. Loss of hydraulic pressure in the electrohydraulic control (EHC) oil lines, which initiates fast closure of the control valves, is monitored. These measurements provide indication that fast closure of the control valves is imminent. This measurement is adequate and is a proper variable for the protective function, taking into consideration the reliability of the chosen sensors relative to other available sensors and the difficulty in making direct measurements of control valve fast-closure rate.

The Turbine Stop Valve closure and the steam governing Turbine Control Valve fast closure reactor scram is automatically bypassed when reactor power is below a preset setpoint value, or if sufficient number of the bypass valves are opening as indicated by their 10% position sensors.

Capability for Test and Calibration

The RPS and SSLC fully meet this requirement in that they conform with Regulatory Guides 1.22 and 1.118. The four-channel SSLC logic allows cross-checking between channels and the ability to take any one channel out of service during reactor operation. Such a condition is annunciated and automatically causes the channel trip logic to revert from two-out-of-four to two-out-of-three.

Most sensors have a provision for actual testing and calibration during reactor operation. The exceptions are defined as follows:

During plant operation, the operator can confirm that the MSIV and turbine stop valve limit switches operate during valve motion. Precise calibration of these sensors requires reactor shutdown.

Independent functional testing of the air header dump valves can be performed during each refueling outage. In addition, operation of at least one valve can be confirmed following each scram occurrence.

Operating Bypasses

Operating bypasses of the RPS system are described in Section 7.2.1.5.2. Whenever the applicable conditions for instrumentation scram bypasses are not met, the RPS will automatically accomplish one of the following: prevent the actuation of an operating bypass; remove any active operating bypass; obtain or retain the permissive conditions for the operating bypass; and initiate the protective function.

Maintenance Bypass

Maintenance bypasses of the RPS system are described in Section 7.2.1.5.2.

Indication of Bypasses

Although operating bypasses do not require annunciation, certain operating bypasses are annunciated in the MCR. The CRD HCU accumulator low charging water pressure trip operating bypass, the MSIV closure trip operating bypass, the turbine stop and control valve fast closure trips operating bypass, and the division-of-sensors bypass are individually annunciated to the operator. Individual SRNM and APRM instrument channel bypasses are indicated on displays for each division on the MCR panels.

Multiple Setpoints

All RPS trip variables are fixed except for the following, which are individually addressed.

The trip setpoint of each SRNM channel is generally fixed. However, there is also the scram initiated by intermediate high neutron flux counting level (corresponding to nominally 5E + 5 counts per second). This is only activated in a non-coincidence scram mode by a switch in the NMS cabinet. The conditions under which such trip is to be activated are included in plant operating procedures.

In modes other than RUN, the APRM setdown function automatically selects a more restrictive scram trip setpoint at a fixed lower value (nominally at 15%). The devices used to prevent improper use of the less restrictive setpoints are designed in accordance with criteria regarding performance and reliability of protection system equipment.

Operation of the mode switch from one position to another bypasses various RPS trips and channels and automatically alters NMS trip setpoints in accordance with the reactor conditions implied by the given position of the mode switch. All equipment associated with these setpoint changes are considered part of the protection system and are qualified Class 1E components.

Completion of Protective Action

It is only necessary that the process sensors remain in a tripped condition for a sufficient length of time to trip the digital trip modules and operate the seal-in circuitry, provided the two-out-of-four logic is satisfied. Once this action is accomplished, the trip actuator logic proceeds to initiate reactor scram regardless of the state of the process sensors that initiated the sequence of events. The same holds true for the manual scram pushbuttons.

Manual Control

Two manual scram pushbutton controls are provided on the principal MCR console to permit manual initiation of reactor scram at the system level. Both switches must be depressed to initiate a scram. Backup to these manual controls is provided by the SHUTDOWN position of the reactor system mode switch. Failure of the manual scram portion of the RPS cannot prevent the automatic initiation of protective action, nor can failure of an automatic RPS function prevent the manual portions of the system from initiating the protective action.

No single failure in the manual or automatic portions of the system can prevent either a manual or automatic scram.

Control of Access

The RPS/SSLC design permits the administrative control of access to all setpoint adjustments, module calibration adjustments and test points. These administrative controls are supported by provisions within the safety system design, by provisions in the generating station design, or by a combination of both.

System Status Indication

When any one of the redundant sensor trip modules exceeds its setpoint value for the RPS trip variables, a MCR display is initiated to identify the particular variable. In the case of NMS trips to the RPS, the specific variable or variables that exceed setpoint values are identified as a function of the NMS. Identification of the particular trip channel exceeding its setpoint is accomplished by permanent storage in the plant computer system. When any manual scram pushbutton is depressed, a MCR annunciation is initiated and a plant computer system record is produced to identify the tripped RPS trip logic.

Repair

Generally, all components can be replaced, repaired, and adjusted during operation. Exceptions are listed below.

During periodic testing of the sensor channels for the following trip variables, all defective components can be identified. Replacement and repair of failed sensors can only be accomplished during reactor shutdown.

- Neutron Monitoring System detectors
- Turbine control valve fast closure sensors
- MSIV closure sensors
- Turbine stop valve closure sensors

Provisions have been made to facilitate repair of NMS components during plant operation except for the detectors. Replacement of the detectors can be accomplished during shutdown.

Identification

The RPS logic is housed in the safety system logic and control (SSLC) reactor trip and isolation functions (RTIF) cabinets. There are four distinct and separate cabinets in accordance with the four electrical divisions. Each division is uniquely identified by color code including cables and associated cables. The SSLC cabinets are marked with the words "Safety System Logic and Control". Each of the safety systems controlled is clearly identified on the cabinets in accordance with their system grouping and labeling. MCR panels are identified by tags on the panels, which indicate the function and identify the contained logic channels. Redundant racks are identified by the identification marker plates of instruments on the racks.

7.1.3 COL Information

None.

7.1.4 References

7.1-1 U.S. NRC, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants,” NUREG-0800.

7.1-2 NEDE-33232P (Proprietary), NEDO-33232 (Non-Proprietary), SSLC/RTIF System Performance Specification, Oct., 2005

7.1-3 NEDE-33233P (Proprietary), NEDO-33233 (Non-Proprietary),, Safety System Logic and Control/Reactor Trip and Isolation Functions (SSLC/RTIF) Hardware/Software Specification, Oct., 2005

7.1-4 NEDE-33234P (Proprietary), NEDO-33234 (Non-Proprietary),, RTIF Digital Trip Module (DTM) Function Software Design Specification, Oct., 2005

7.1-5 NEDC-32410P-A (Proprietary), Nuclear Measurement Analysis and Control Power Range Neutron Monitor (NUMAC PRNM) Retrofit Plus Option III Stability Trip Function, Oct., 1995

7.1-6 NEDO-31439-A (Non Proprietary), The Nuclear Measurement Analysis and Control Wide Range Neutron Monitor System (NUMAC WRNMS), Oct., 1990

7.1-7 NEDE-24362-1-P, Revision 1, "General Electric Environmental Qualification Program," General Electric Company, Class III (proprietary), January 1983.

7.1-8 EPRI TR-102323, “Guidelines for Electromagnetic Interference Testing in Power Plants”, Final Report, June 1994.

Table 7.1-1 Regulatory Requirements Applicability Matrix, Part 1

Applicable Criteria	10 CFR														
	50.55a(a)(1)	50.55a(h)	50.34 (f) (2) (v) (I.D.3)	50.34 (f) (2) (xvii) (II.F.1)	50.34 (f) (2) (xviii) (II.F.2)	50.34 (f) (2) (xiv) (II.E.4.2)	50.34 (f) (2) (xix) (II.F.3)	50.34 (f) (2) (xxiv) (II.K.3.23)	50.62	52.47 (a) (1) (iv)	52.47 (a) (1) (vi)	52.47 (a) (1) (vii)	52.47 (a) (2)	52.47 (b) (2) (i)	52.79 (c)
Reference Standard Guidelines: SRP NUREG-0800 App. 7.1-A		ANSI/IEEE Std 279	NUREG 718, 737, 694	NUREG 718, 737, 694	NUREG 694	NUREG 737	NUREG 718	NUREG 718		(Tier 2)	(Tier 1)	(Tier 1)	(Tiers 1&2)	(Tier 2)	(Tier 1)
Reactor Protection System	X	X	X							X	X	X	X	X	X
Neutron Monitoring System	X	X	X							X	X	X	X	X	X
Suppression Pool Temperature Monitor Function	X	X	X							X	X	X	X	X	X
Automatic Depressurization System	X	X	X			X				X	X	X	X	X	X
Gravity-Driven Cooling System	X	X	X			X				X	X	X	X	X	X
Leak Detection & Isolation System	X	X	X			X				X	X	X	X	X	X
Safety System Logic & Control System	X	X	X			X				X	X	X	X	X	X
Standby Liquid Control System	X	X								X	X	X	X	X	X
Remote Shutdown System	X	X								X	X	X	X	X	X
Reactor Water Cleanup/Shutdown Cooling System	X	X								X	X	X			X
Isolation Condenser System	X	X								X	X	X	X	X	X
Post Accident Monitoring System	X	X	X	X	X		X	X		X	X	X	X	X	X
Containment Monitoring System	X	X	X	X			X			X	X	X	X	X	X
Process Radiation Monitoring System	X	X	X	X			X			X	X	X	X	X	X
Area Radiation Monitoring System	X	X		X			X			X	X	X			X
Interlock Systems	X	X	X							X	X	X	X	X	X
Nuclear Boiler System	X	X								X	X	X	X	X	X
Rod Control & Information System										X	X	X			X
Feedwater Control System										X	X	X			X
Plant Automation System										X	X	X			X
Steam Bypass & Pressure Control System										X	X	X			X
Neutron Monitoring System (Non-safety portion)										X	X	X			X
Containment Inerting System										X	X	X			X
Diverse Instrumentation & Controls	X	X							X	X	X	X	X		X
Essential Distributed Control & Information System	X	X	X						X	X	X	X	X	X	X
Non-Essential Distributed Control & Info. System	X	X							X	X	X	X			X

Table 7.1-1 Regulatory Requirements Applicability Matrix, Part 2

	General Design Criteria (GDC)												SRM to SECY 93-087	
Applicable Criteria	1	2	4	13	19	20	21	22	23	24	25	29	II.Q	II.T
Reference Standard Guidelines: SRP NUREG-0800 App. 7.1-A				BTP HICB-12		IEEE 603	IEEE 603	IEEE 603	IEEE 603	IEEE 603	IEEE 603		BTP HICB-19	
Reactor Protection System	X	X	X	X	X	X	X	X	X	X	X	X	X	
Neutron Monitoring System	X	X	X	X	X	X	X	X	X	X	X	X	X	
Suppression Pool Temperature Monitor Function	X	X	X	X	X	X	X	X	X	X	X	X	X	
Automatic Depressurization System	X	X	X	X	X	X	X	X	X	X			X	
Gravity-Driven Cooling System	X	X	X	X	X	X	X	X	X	X			X	
Leak Detection & Isolation System	X	X	X	X	X	X	X	X	X	X			X	
Safety System Logic & Control System	X	X	X	X	X	X	X	X	X	X			X	
Standby Liquid Control System	X	X	X	X	X					X				
Remote Shutdown System	X	X	X	X	X					X				
Reactor Water Cleanup/Shutdown Cooling System		X	X	X	X					X				
Isolation Condenser System	X	X	X	X	X					X				
Post Accident Monitoring System	X	X	X	X	X					X				X
Containment Monitoring System	X	X	X	X	X					X				X
Process Radiation Monitoring System	X	X	X	X	X					X				X
Area Radiation Monitoring System		X	X	X	X					X				
Interlock Systems	X	X	X	X	X					X	X			
Nuclear Boiler System	X	X	X	X	X					X			X	
Rod Control & Information System				X	X					X		X		
Feedwater Control System				X	X					X				
Plant Automation System				X	X					X				
Steam Bypass & Pressure Control System				X	X					X				
Neutron Monitoring System (Non-safety portion)				X	X					X				
Containment Inerting System				X	X					X				
Diverse Instrumentation & Controls	X			X	X					X			X	
Essential Distributed Control & Information System	X	X	X	X	X		X	X	X	X		X	X	X
Non-Essential Distributed Control & Info. System				X	X					X				

Table 7.1-1 Regulatory Requirements Applicability Matrix, Part 3

Applicable Criteria	Regulatory Guides															
	1.22	1.47	1.53	1.62	1.75	1.97	1.105	1.118	1.151	1.152*	1.153	1.168*	1.169*	1.170*	1.171*	1.172*	1.173*
Reference Standard Guidelines: SRP NUREG-0800 App. 7.1-A	BTP HICB-8 & 17	IEEE 279	IEEE 379	IEEE 279	IEEE 384	ANSI/ANS 4.5	BTP HICB-12	IEEE 338	ANSI/ISA-S67.02	IEEE 7-4.3.2	IEEE 603	IEEE 1012, 1028	IEEE 828, 1042	IEEE 829	IEEE 1008	IEEE 830	IEEE 1074
Reactor Protection System	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X
Neutron Monitoring System	X	X	X		X		X	X		X	X	X	X	X	X	X	X
Suppression Pool Temperature Monitor Function	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X
Automatic Depressurization System	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X
Gravity-Driven Cooling System	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X
Leak Detection & Isolation System	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X
Safety System Logic & Control System	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X
Standby Liquid Control System			X		X		X	X		X	X	X	X	X	X	X	X
Remote Shutdown System			X		X			X		X	X	X	X	X	X	X	X
Reactor Water Cleanup/Shutdown Cooling System																	
Isolation Condenser System			X		X		X	X		X	X	X	X	X	X	X	X
Post Accident Monitoring System						X											
Containment Monitoring System		X	X		X		X	X		X	X	X	X	X	X	X	X
Process Radiation Monitoring System		X	X		X		X	X		X	X	X	X	X	X	X	X
Area Radiation Monitoring System																	
Interlock Systems		X	X		X		X	X		X	X	X	X	X	X	X	X
Nuclear Boiler System					X		X		X	X	X	X	X	X	X	X	X
Rod Control & Information System																	
Feedwater Control System																	
Plant Automation System																	
Steam Bypass & Pressure Control System																	
Neutron Monitoring System (Non-safety portion)																	
Containment Inerting System																	
Diverse Instrumentation & Controls	X			X	X		X	X		X	X	X	X	X	X	X	X
Essential Distributed Control & Information System	X	X	X		X		X	X		X	X	X	X	X	X	X	X
Non-Essential Distributed Control & Info. System																	

* These criteria are addressed in conjunction with the Safety System Logic and Control System (SSLC)

Table 7.1-1 Regulatory Requirements Applicability Matrix, Part 4

Applicable Criteria SRP NUREG-0800 App 7-A	Branch Technical Positions (BTP) HICB														
	HICB-1	HICB-3	HICB-6	HICB-8	HICB-9	HICB-10	HICB-11	HICB-12	HICB-13	HICB-14*	HICB-16	HICB-17*	HICB-18*	HICB-19*	HICB-21*
Reference Standard Guidelines: SRP NUREG-0800 App. 7.1-A	RG 1.153	IEEE 603	IEEE 603	RGs 1.22, 1.153	RG 1.153	RG 1.97	RGs 1.75, 1.153	RG 1.105	RG 1.153	RG 1.152	RG 1.70, Tier 1,2	RGs 1.22, 1.153	NUREG/CR-6090	SECY 93-087 II.Q	NUREG/CR-6083
Reactor Protection System		X		X	X		X	X	X	X	X	X	X	X	X
Neutron Monitoring System		X		X			X	X		X	X	X	X	X	X
Suppression Pool Temperature Monitor Function		X		X			X	X	X	X	X	X	X	X	X
Automatic Depressurization System		X	X	X			X	X		X	X	X	X	X	X
Gravity-Driven Cooling System		X	X	X			X	X	X	X	X	X	X	X	X
Leak Detection & Isolation System				X			X	X	X	X	X	X	X	X	X
Safety System Logic & Control System		X	X	X			X	X	X	X	X	X	X	X	X
Standby Liquid Control System							X	X		X	X	X	X		X
Remote Shutdown System							X			X	X	X	X		X
Reactor Water Cleanup/Shutdown Cooling System											X				
Isolation Condenser System							X	X	X	X	X	X	X		X
Post Accident Monitoring						X									
Containment Monitoring System							X	X	X	X	X	X	X		X
Process Radiation Monitoring System							X	X	X	X	X	X	X		X
Area Radiation Monitoring System											X				
Interlock Systems	X						X	X		X	X	X	X		X
Nuclear Boiler System							X	X		X	X	X	X	X	X
Rod Control & Information System											X				
Feedwater Control System											X				
Plant Automation System											X				
Steam Bypass & Pressure Control System											X				
Neutron Monitoring System (Non-safety portion)											X				
Containment Inerting System											X				
Diverse Instrumentation & Controls				X			X	X		X	X	X	X	X	X
Essential Distributed Control & Information System				X			X	X		X	X	X	X	X	X
Non-Essential Distributed Control & Info. System											X				

* These criteria are addressed in conjunction with the Safety System Logic and Control System (SSLC)

Table 7.1-2 Section Roadmap of Evaluation of IEEE Std 603 Specific Criteria Compliance

IEEE Section #	Subject	SSLC/RTIF	NMS	SSLC/ESF	RSS	PAM	E-DCIS
	Logic function	*RPS, LDIS, SLC*		*ADS, GDCS, ICS*			
5. Safety system criteria							
5.1	Single-failure criterion	7.2.1.1, 7.2.1.2.4, 7.2.1.3, 7.3.3.1, 7.3.3.2, 7.3.3.3	7.2.2.3.2	7.3.1.1.2, 7.3.1.1.3, 7.3.1.2.2, 7.3.1.2.3, 7.3.4.2, 7.7.1.3, 7.8.1.2.2	7.4.2.2	Tab.7.5-1	7.9.1.2, 7.9.1.3
5.2	Completion of protective action	7.2.1.1, 7.2.1.2.4.2, 7.2.1.3, 7.3.3.1		7.3.1.2.2			
5.3	Quality	7.2.1.3		7.3.4.3		Tab.7.5-1	
5.4	Equipment qualification	7.2.1.3	7.2.2.2, 7.2.2.3.2	7.3.4.3		Tab.7.5-1	
5.5	System integrity	7.2.1.3	7.2.2.1.1, 7.2.2.1.2	7.3.4.3			
5.6	Independence	7.2.1.1, 7.2.1.2.4, 7.2.1.3, 7.3.3.3.2	7.2.2.1, 7.2.2.3	7.3.1.1.3, 7.3.1.2.3, 7.3.4.2, 7.3.4.3		Tab.7.5-1	7.9.1.2, 7.9.1.3
5.7	Testing and calibration	7.2.1.3, 7.3.3.3.2	7.2.2.3.2, 7.2.3.3.2	7.3.1.1.3, 7.3.1.1.4, 7.3.1.2.3, 7.3.4.3		Tab.7.5-1	7.9.1.2, 7.9.1.3
5.8	Information displays	7.2.1.2.4.3, 7.2.1.3, 7.2.3.3	7.2.2.1.3, 7.2.2.1.4	7.3.1.1.2, 7.3.1.2.2, 7.3.1.2.3		Tab.7.5-1	
5.9	Control of access	7211, 7213, 72152			7.4.2.2	Tab.7.5-1	
5.10	Repair	7.2.1.1, 7.2.1.2.4.4, 7.2.1.4, 7.2.1.5.2, 7.3.3.3	7.2.2.2.1, 7.2.2.2.3	7.3.4.1, 4.3.4.2		Tab.7.5-1	7.9.1.2, 7.9.1.5
5.11	Identification	7.2.1.3		7.3.1.2.3, 7.8.2.2		7512, Tab.7.5-1	
5.12	Auxiliary features	7.2.1.2.3			7.4.2.2	Tab.7.5-1	
5.13	Multi-unit stations	N/A	N/A	N/A	N/A	N/A	N/A
5.14	Human factors considerations	Chapter 18	Chapter 18	Chapter 18		7512, Tab.7.5-1	
5.15	Reliability	Chapter 19	Chapter 19	Chapter 19			Chapter 19
5.16	Common cause failure criteria	7.2.1.3, 7.8					

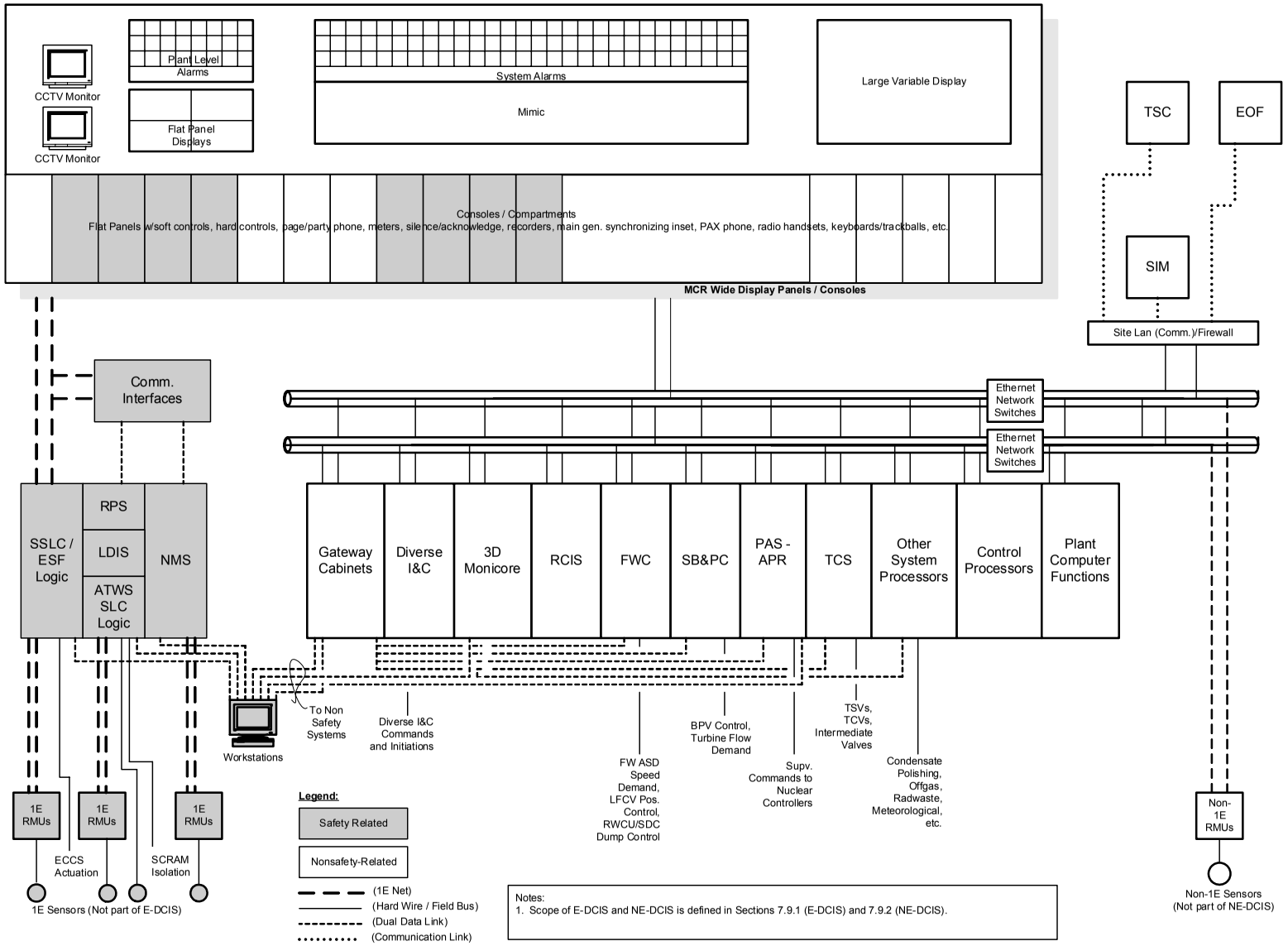
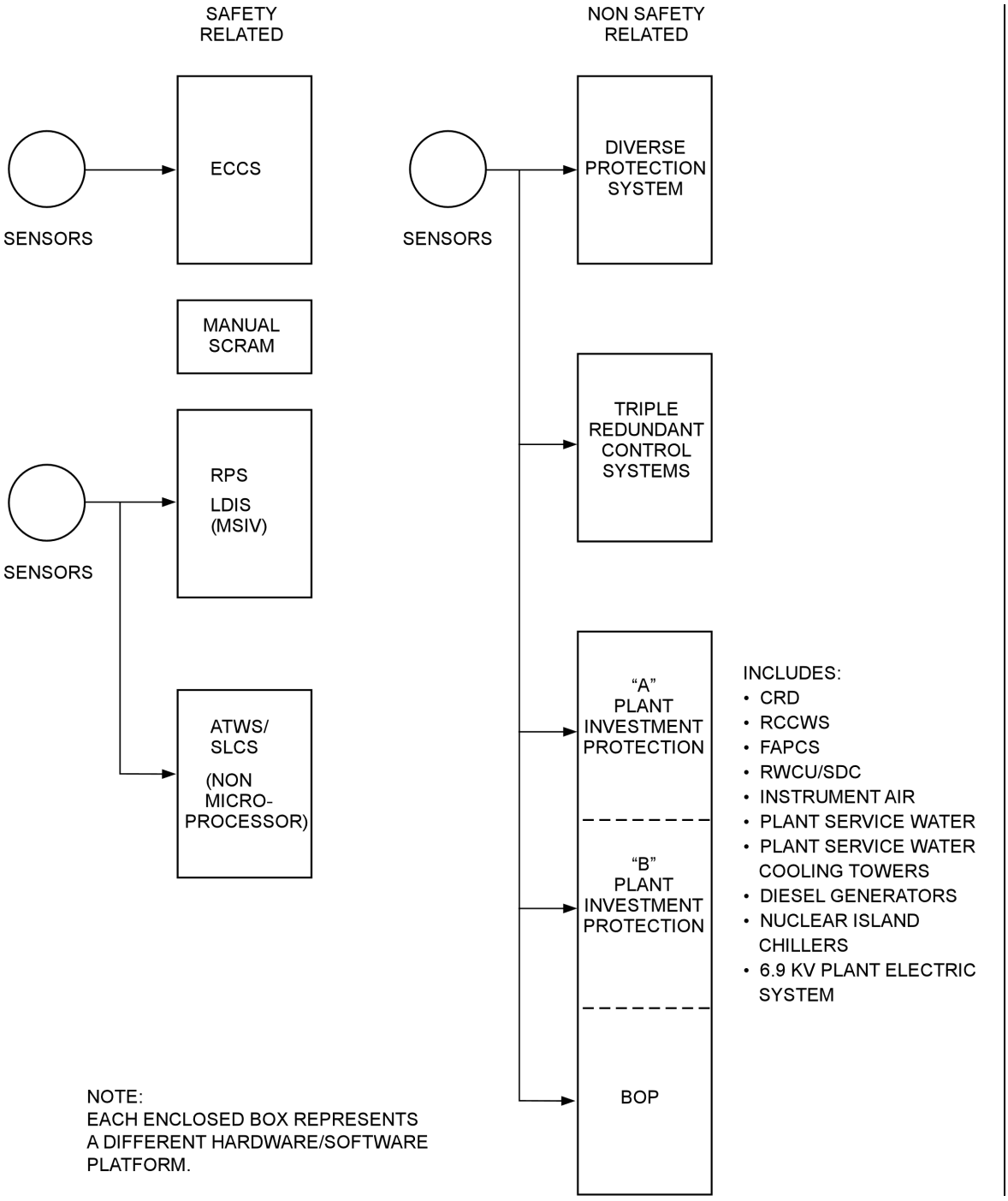


Figure 7.1-1 ESBWR Instrumentation and Control Simplified Block Diagram



(Note: RPS and ATWS/SLCS uses different water level sensors)

Figure 7.1-2 Diversity of ESBWR Instrumentation and Controls