7.0 Instrumentation and Control Systems

7.1 Introduction

The information in this section of the reference ABWR DCD, including all subsections and tables, and figures, is incorporated by reference with the following departures and supplements.

STD DEP T1 2.3-1

STD DEP T1 2.14-1 (Table 7.1-1)

STD DEP T1 3.4-1 (Figure 7.1-1, 7.1-2)

STD DEP 1.8-1 (Table 7.1-2)

STD DEP 7.1-1

STD DEP 7.1-2

STD DEP 7.4-1

STD DEP Admin (Table 7.1-1)

7.1.1 Identification of Safety-Related Systems

Refer to Subsections 7.1S.1 and 7.1S.2 for terminology related to the Reactor Trip and Isolation System (RTIS), the Neutron Monitoring System (NMS), and the Engineered Safety Features Logic and Control Sytem (ELCS).

7.1.1.1 General

STD DEP T1 3.4-1

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 action of several safety-related nuclear steam supply systems (NSSS) are accomplished by ~~a four-division correlated and separated protection logic complex called~~ the safety system logic and control (SSLC). The SSLC includes multiple redundant divisions, which are separated from each other. The SSLC has four redundant divisions of sensors. Each division of sensors has a corresponding division that determines the trip status of the safety functions relative to the safety function setpoint. The SSLC has four redundant divisions for all actuation functions except for the engineered safety features. The engineered safety features have three divisions, corresponding to the maximum redundancy of the engineered safety features actuated components. Some engineered safety features functions are less than three-fold redundant and are assigned to the appropriate set of redundant divisions. *The SSLC multi-divisional complex includes divisionally separate control room and other panels which house the SSLC equipment for controlling the various safety function actuation devices. The SSLC receives input signals from the redundant*

channels of instrumentation in the safety-related system, and uses the input information to perform logic functions in making decisions for safety actions.

Sensor signals are hardwired to the RTIS. These sensors are divisionally separated.

Divisional separation is applied to the Essential Communication Functions (ECFs) of ELCS, which provides communication for the sensor input to the logic units and for the logic output to the system actuators (actuated devices such as pump motors and motor-operated valves).

~~*Divisional separation is also applied to the essential multiplexing system (EMS) , 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 pump motors and motor operated valves).*~~ *Systems which utilize the SSLC* ~~*are*~~ include*: (1) Reactor Protection (trip) System; (2) High Pressure Core Flooder System; (3) Residual Heat Removal System; (4) Automatic Depressurization System; (5) Leak Detection and Isolation System; (6) Suppression* ~~Temperature~~ *Pool* Temperature *Monitoring System; and (7) Reactor Core Isolation Cooling System. The equipment arrangement for these systems and other supporting systems is shown in Figure 7.1-2.*

7.1.1.3 Engineered Safety Features (ESF) Systems

7.1.1.3.9 HVAC Emergency Cooling Water System

STD DEP Admin

Automatic instrumentation and control is provided to assure that adequate cooling is provided for the main control room, the control building essential electrical equipment rooms, and the ~~*diesel generator cooling coils*~~ reactor building essential electrical equipment rooms.

7.1.1.4 Safe Shutdown Systems

7.1.1.4.1 Alternate Rod Insertion Function (ARI)

STD DEP 7.4-1

Though not required for safety, instrumentation and controls for the ARI provide a means to mitigate the consequences of anticipated transient without scram (ATWS) events. ~~*Upon receipt of an initiation signal (based on either high reactor dome pressure or low reactor water level from the Recirculation Flow Control System), the RCIS System controls the fine motion control rod drive (FMCRD) motors such that all operable control rods are driven to their full in position.*~~ The Recirculation Flow Control System (upon detection of either high reactor dome pressure, low reactor water level or Manual ARI initiation) activates opening signals for the ARI valves of the Control Rod Drive (CRD) System (i.e., for backup hydraulic insertion of the control rods) and activates ARI initiation command signals to the Rod Control and Information System (i.e., for electric motor insertion of all operable control rods to the full-in position). *This provides a method, diverse from* ~~*the hydraulic control units (HCUs), for scramming the*~~

~~reactor.~~ the SCRAM function of the Reactor Protection System and associated CRD hydraulic control units (HCUs), for achieving insertion of control rods.

7.1.1.6 Other Safety-Related Systems

7.1.1.6.1 Neutron Monitoring System (NMS)

STD DEP Admin

(1) Startup Range Neutron Monitoring (SRNM)

(2) Local Power Range Monitoring (LPRM)

(3) Average Power Range Monitoring (APRM)

(4) Automated Traversing Incore Probe (ATIP)

(5) Multi-channel Rod Block Monitoring (MRBM)

The SRNM, LPRM, and APRM are the only safety-related subsystems of NMS.

7.1.1.6.2 Process Radiation Monitoring System (PRM~~S~~) Instrumentation and Controls

STD DEP Admin

The Process Radiation Monitoring System (PRM~~S~~) monitors the main steamlines, vent discharges and all liquid and gaseous effluent streams which may contain radioactive materials. Main control room display, recording and alarm capability is provided along with automatic trip inputs that initiate protection functions.

7.1.1.6.6 Containment Atmospheric Monitoring System

STD DEP T1 2.14-1

The Containment Atmospheric Monitoring System (CAMS) measures and records radiation levels and the oxygen/hydrogen concentration in the primary containment under post-accident conditions. It is designed to operate continuously and is automatically put in service upon detection of LOCA conditions. The only CAMS safety-related function is measuring radiation levels in primary containment.

7.1.2 Identification of Safety Criteria

7.1.2.1.4 Instrument Errors

STD DEP 7.1-1

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

(safety limits, setpoints, and margins are ~~provided in Chapter 16~~ determined in accordance with the instrument setpoint methodology document described in Section 16.5.5.2.11, Setpoint Control Program*) The amount of instrument error is determined by test and experience. The setpoint is selected based on the known error. The recommended test frequency is greater on instrumentation that demonstrates a stronger tendency to drift.*

7.1.2.1.4.1 Safety System Setpoints

STD DEP 7.1-1

The methods for calculating *safety system setpoints are ~~listed~~*determined *in* accordance with *the ~~Chapter 16~~* instrument setpoint methodology document described in Section 16.5.5.2.11, Setpoint Control Program, *for each safety system. The 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 system settings. Instrument drift, setting error, and repeatability are considered in the setpoint determination (Subsection 7.1.2.1.4). The margin between the limiting safety system settings and the actual safety limits includes consideration of the maximum credible transient in the process being measured.*

7.1.2.1.6 [Protection System Inservice Testability

STD DEP T1 3.4-1

The ~~RPS~~ RTIS *and ~~ESF~~*ELCS *Systems can be tested during reactor operation~~ by six separate tests~~. The first five tests are primarily manual tests and, although each individually is a partial test, combined with the sixth test they constitute a complete system test. The sixth test is the~~ self~~ test of the safety system logic and control which~~ automatically~~ tests the complete system excluding sensors and actuators.*

(4) The fourth test checks calibration of analog sensor inputs ~~at the analog inputs of the remote multiplexing units~~. With a division-of-sensors bypass in place, calibrated, variable ~~ramp~~ signals are injected in place of the sensor signals and monitored ~~at the SSLC control room panels~~ for linearity, accuracy, fault response, and downscale and upscale trip response. ~~The test signals are adjustable manually from the control room and also are capable of performing an automatic sequence of events.~~ When surveillance testing during plant shutdown, trip coincidence and actuated device operation can be verified by simultaneous trip tests of coincident channels. Pressure transmitters and level transmitters are located on their respective local panels. The transmitters can be individually valved out of service and subjected to test pressure to verify operability of the transmitters as well as verification of calibration range. To gain access to the field controls on each transmitter, a cover plate or sealing device ~~must~~ may *be removed. Access to the field controls is granted only to qualified personnel for the purpose of testing or calibration adjustments.*

(6) *The sixth test ~~is an integrated self test provision built into the microprocessors within the SSLC. It~~ consists of an online, continuously operating, self~~-diagnostic~~* diagnostics.~~*monitoring network,*~~ *and ~~an~~ offline ~~semi-automatic (operator initiated, but automatic to completion),~~ end-to-end surveillance program.* Cross channel comparison of sensor inputs is performed by plant computer functions. *Both online and offline functions operate independently within each of the four divisions. There are no multi-divisional interconnections associated with self~~-testing~~* diagnostics.

The primary purpose of the self~~-test~~ diagnostic function *is to improve the availability of the SSLC by optimizing the time to detect and determine the location of a failure in the functional system. It is not intended that the self-~~test~~* diagnostic function *eliminate the need for the other five manual tests. However, most faults are detected more quickly than with manual testing alone.*

The self~~-test~~ diagnostic *function is classified as safety-related. Its hardware and software are an integral part of the SSLC and, as such, are qualified to Class 1E standards.*

The hierarchy of test capability is provided to ensure maximum coverage of all ~~EMS~~ ECF*/SSLC functions, including logic functions and data communication links. Testing shall include:*

(a) *Online Continuous Testing*

*A self-diagnostic program monitors each signal processing module from input to output.~~ Testing is automatic and~~*Diagnostic testing *is performed ~~periodically~~*as part of the online functions *during normal operation. Tests will verify the basic integrity of each card or module~~ on the microprocessor bus~~. All operations are part of normal data processing intervals and will not affect system response to incoming trip or initiation signals. ~~Automatic initiation signals from plant sensors will override an automatic test sequence and perform the required safety function~~. Process or logic signals are not changed as a result of self~~-test~~* diagnostic *functions.*

The self-diagnostic function does not degrade system reliability. Indications of test results (pass, fail) is provided.

*Self-diagnosis includes monitoring of overall program flow, ~~reasonableness of process variables, RAM and PROM~~*and processor memory *condition~~, and device interlock logic~~. Testing includes continuous error checking of all transmitted and received data~~ on the serial data links of each SSLC controller~~; for example, error checking by parity check, checksum, or cyclic redundancy checking (CRC) techniques.*

~~*A fault is considered the discrepancy between an expected output of a permissive circuit and the existing present state.*~~

*Actuation of the trip function is not performed during this test. The self-~~test~~*diagnostic *function is capable of detecting ~~and logging~~ intermittent failures without stopping system operation. Normal surveillance by plant personnel will identify these failures, via a diagnostic display, for preventive maintenance.*

Self~~-test~~ diagnostic *failures (except intermittent failures) are annunciated to the operator at the main control room console and logged by the ~~process~~* plant *computer* functions (PCF)*. Faults are identified to the replacement board or module level and ~~positively~~* are generally *indicated at the failed unit.*

*The ~~continuous surveillance monitoring~~*self-diagnostic function *also includes power supply voltage levels~~, card out of file interlocks, and battery voltage levels on battery-backed memory cards (if used). Out-of-tolerance conditions will result in an inoperative (out-ofservice) condition for that particular system function.~~*and verification of the module configuration.

~~*Automatic system self-testing occurs during a portion of every periodic transmission period of the data communication network. Since exhaustive tests cannot be performed during any one transmission interval, the test software is written so that sufficient overlap coverage is provided to prove system performance during tests of portions of the circuitry, as allowed in IEEE 338.*~~

The ~~Essential Multiplexing System (EMS)~~ Essential Communication Function (ECF) *is included in the continuous, automatic self~~-test~~ diagnostic function. Faults at the ~~Remote Multiplexing Units (RMUs)~~* Remote Digital Logic Controllers (RDLCs) *are alarmed in the main control room. ~~Since the EMS~~* ECF *is dual in each division~~, self-test supports automatic reconfiguration or bypass of portions of EMS after a detected fault, such that the least effect on system availability occurs.~~* A fault on one of the two communication paths will not prevent system operation through the unfaulted path.

(b) Offline ~~Semi-automatic~~ End-to-End (Sensor Input to Trip Actuator) Testing

The more complete, manually-initiated ~~internal self~~ test is available when a unit is offline for surveillance or maintenance testing. This test exercises the trip outputs of the SSLC logic ~~processors~~. The channel containing the ~~processors~~ logic *will be bypassed during testing.*

A fault is considered the inability to open or close any control circuit.

*~~Self test~~*Test *failures are displayed on a front panel readout device or other diagnostic unit.*

*To reduce operator burden and decrease outage time, a ~~surveillance test controller (STC)~~*maintenance and test panel (MTP) *is provided as a dedicated instrument in each division of ~~SSLC~~* ELCS. *The ~~STC performs semi-automatic (operator initiated)~~*MTP is used for *testing of ~~SSLC~~* ELCS *functional logic, including trip, initiation, and interlock logic. Test coverage includes verification of correct operation of the following capabilities, as defined in each system IBD:*

(i) Each 2/4 coincident logic function.

(ii) Serial and parallel I/O, including manual control switches, limit switches, and other contact closures.

~~(iii) The 1/N trip selection function.~~

~~(iv)~~ (iii) *Interlock logic for each valve or pump.*

A separate test sequence for each safety system is operator-selectable~~; testing will proceed automatically to conclusion after initiation by the operator~~. Surveillance testing is performed in one division at a time. The surveillance test frequency is given in Chapter 16.

~~The STC injects test patterns through the EMS communications links to the RMUs. It then tests the RMUs' ability to format and transmit sensor data through and across the EMS/SSLC interface, in the prescribed time, to the load drivers. Under the proper bypass conditions, or with the reactor shut down, the load drivers themselves may be actuated.~~

7.1.2.4 Safe Shutdown Systems—Instrumentation and Controls

7.1.2.4.1 Alternate Rod Insertion Function (ARI)—Instrumentation and Controls

STD DEP 7.1-2

STD DEP 7.4-1

(2) Non-safety-Related Design Bases

The general functional requirements of the instrumentation and controls of the ARI function are to:

(a) Provide alternate and diverse method for inserting control rods using *~~fine motion control rod drive (FMCRD) electric motors.~~* the ARI valves

of the Control Rod Drive System or using the ARI motor run-in function of the Rod Control and Information System.

(b) Provide for automatic and manual operation of the ~~system~~ function*.*

(c) Provide assurance that the ARI shall be highly reliable and functional in spite of a single failure.

(d) Provide assurance that the ARI shall operate when necessary ~~(FMCRD motors shall be connected to the emergency diesel generators).~~ (e.g., the stepping motor driver modules (SMDMs), which control the fine motion control rod drive (FMCRD) motors, shall derive their input power from a power bus that can automatically receive power from an emergency diesel generator, if necessary).

(e) Mitigate the consequences of anticipated transient without scram (ATWS) events.

7.1.2.4.3 RHR—Reactor Shutdown Cooling Mode—Instrumentation and Controls

STD DEP Admin

(1) Safety Design Bases

*(c) Indicate performance of the shutdown cooling system by ~~main control room~~*separate *instrumentation and controls in the* main control room and in the *remote shutdown panel.*

7.1.2.6 Other Safety-Related Systems

7.1.2.6.1 Neutron Monitoring System (NMS)—Instrumentation and Controls

7.1.2.6.1.1 Startup Range Neutron Monitoring (SRNM) Subsystem

STD DEP 7.1-2

(1) Safety Design Bases

General Functional Requirements:

(d) The SRNM subsystem will provide Anticipated Transient Without Scram (ATWS) permissive signals to the ESF Logic and Control System (ELCS).

7.1.2.6.1.4 Average Power Range Monitor (APRM) Subsystem

STD DEP 7.1-2

(1) Safety Design Bases

General Functional Requirements:

The general functional requirements are that, under the worst permitted input LPRM bypass conditions, the APRM Subsystem shall be capable of generating a trip signal in response to average neutron flux increases in time to prevent fuel damage. The APRM generator trip functions with trip inputs to the RPS also include: simulated thermal power trip, APRM inoperative trip, core flow rapid decrease trip, and core power oscillation trip of the oscillation power range monitor (OPRM). The OPRM design basis is to provide a trip to prevent growing core flux oscillation to prevent thermal limit violation, while discriminating against false signals from other signal fluctuations not related to core instability. The independence and redundancy incorporated into the design of the APRM Subsystem shall be consistent with the safety design bases of the Reactor Protection System (RPS). The RPS design bases are discussed in Subsection 7.1.2.2.

The APRM subsystem also provides Anticipated Transient Without Scram (ATWS) permissive signals to the ESF Logic and Control System (ELCS) as described in Subsection 7.6.1.1.2.2(5).

7.1.2.6.2 Process Radiation Monitoring System

STD DEP T1 2.3-1

STD DEP 7.1-1

(1) Safety Design Bases

General Functional Requirements:

(d) Not Used ~~*Provide channel trip inputs to the RPS and LDS on high radiation in the MSL tunnel area. If the protection system logic is satisfied, the following shall be initiated:*~~

~~*(i) Reactor scram.*~~

~~*(ii) Closure of the main steamline isolation valves.*~~

~~*(iii) Shutdown of the mechanical vacuum pump and closure of the mechanical pump discharge line isolation valve.*~~

(2) Non-safety-Related Design Bases

(e) Provide alarm annunciation signals to the main control room if alarm or trip levels are reached or the radiation monitoring subsystem becomes inoperative, and provide input to the offgas system when the radioactive gas concentration in the offgas system discharge is at or in excess of the restrictive concentration limit derived from ~~*Technical Specification*~~ the Offsite Dose Calculation Manual *release rate limits and that discharge from the offgas system must be terminated.*

7.1.2.6.6 Containment Atmospheric Monitoring (CAM) Systems

STD DEP T1 2.14-1

(1) Safety Design Bases

General Functional Requirements:

~~*Monitor the atmosphere in the inerted primary containment for radiation levels and for concentration of hydrogen and oxygen gases, primarily during post-accident conditions. Monitoring shall be provided by two independent safety-related divisional subsystems.*~~

Monitor continuously the radiation environment in the drywell and suppression chamber during reactor operation and under post-accident conditions. Monitoring shall be provided by two independent safety-related divisional subsystems of radiation monitors.

~~*Sample and monitor the oxygen and hydrogen concentration levels in the drywell and suppression chamber under post-accident conditions, and also when required during reactor operation. The LOCA signal (low reactor water level or high drywell pressure) shall activate the system and place it into service to monitor the gaseous buildup in the primary containment following an accident.*~~

(2) Non-Safety-Related Design Bases

Separate hydrogen and oxygen gas calibration sources shall be provided for each CAM Subsystem for periodic calibration of the gas analyzers and monitors.

Monitor the atmosphere in the inerted primary containment for concentration of hydrogen and oxygen gases, primarily during post-accident conditions. Monitoring shall be provided by two independent and redundant nonsafety-related subsystems of Oxygen/Hydrogen Monitors.

Sample and monitor the oxygen and hydrogen concentration levels in the drywell and suppression chamber under post-accident conditions, and also when required during reactor operation. The loss of coolant accident (LOCA) signal (low reactor water level or high drywell pressure) shall activate the system and place it into service to monitor the gaseous buildup in the primary containment following an accident.

7.1.2.8 Independence of Safety-Related Systems

STD DEP Admin

(See Subsection~~s~~ ~~8.3.1.3 and 8.3.1.4~~ 8.3.3.6.2.*)*

7.1.2.9 Conformance to Regulatory Requirements

7.1.2.9.1 Regulation 10CFR50.55a

STD DEP 1.8-1

The only portion of 10CFR50.55a applicable to the I&C equipment is 10CFR50.55a(h), which requires the application of IEEE ~~279~~603 for protection systems (Subsection 7.1.2.11.1).

7.1.2.10 Conformance to Regulatory Guides

7.1.2.10.2 Regulatory Guide 1.47—Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems

STD DEP 1.8-1

Bypass indications are designed to satisfy the requirement of IEEE ~~279~~603, Paragraph ~~4.13~~5.8.3, Regulatory Guide 1.47~~,~~ and BTP ICSB 21. Regulatory Guide 1.47 requires designs to satisfy Paragraph 4.13 of IEEE 279, which has been subsequently superceded by Paragraph 5.8.3 of IEEE 603. Bypass indications also satisfy these requirements. *Additional information may be found in the system detail descriptions in Sections 7.2, 7.3, 7.4 and 7.6. The design of the bypass indications allows testing during normal operation and is used to supplement administrative procedures by providing indications of safety systems status.*

7.1.2.10.9 Regulatory Guide 1.105—Instrument Setpoints

STD DEP 7.1-1

The I&C systems are consistent with the requirements of Regulatory Guide 1.105. ~~The trip setpoint (instrument setpoint) allowance value (Tech Spec limit) and the analytical or design basis limit are all contained in the Technical Specifications (Chapter 16).~~ Safety limits, setpoints, and margins are determined in accordance with the instrument setpoint methodology document in Section 16.5.5.2.11, Setpoint Control Program. *~~These parameters are all 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.~~*

7.1.2.11 Conformance to Industry Standards

STD DEP 1.8-1

7.1.2.11.1 ~~IEEE-279—Criteria for Protection Systems for Nuclear Power Generating Stations~~ IEEE-603—Standard Criteria for Safety Systems for Nuclear Power Generating Stations

All safety related systems are designed to meet the requirements of IEEE ~~279~~603. Clarifications of any of the provisions are discussed for the applicable systems in the analysis portions of Sections 7.2, 7.3, 7.4, ~~and~~ 7.6, and 7.9S.

IEEE-603, Section 4, Safety System Designation

A specific basis is established to determine the design of each safety-related I&C system. This basis evolved from the identification of Design Basis Events (DBE) that are postulated in Chapter 15. The plant operating conditions and the safety analysis acceptance criteria applicable for each event are shown in Chapter 15. Credited systems, interlocks, and functions are evaluated for each DBE. Information provided for each design base item enables the detailed design of the system to be carried out. The number of sensors and their location, including spatial effects, is determined during this design basis analysis. The identification of variables are derived from the DBEs as well as the requirements for varied manual initiation and control of protective functions. Safety system design basis descriptions are included in the various sections of this Chapter.

IEEE-603, Sections 5, 6 and 7, Safety System Criteria

The safety-related systems are designed to maintain plant parameters within acceptable limits that are established by design basis events. This is done with precision and reliability meeting the requirements of IEEE-603. The scope of IEEE-603 includes safety-related I&C systems and is described in more detail in Sections 7.2 through 7.6 and 7.9S. The safety-related I&C design conforms with IEEE-603 and has been qualified to demonstrate that all required performance requirements are met. Nonsafety-related systems generally are not required to meet any of the requirements of IEEE-603 with the exception of their independence from safety-related systems. The STP 3&4 safety-related I&C design descriptions related to IEEE-603, Sections 5, 6, and 7 requirements are provided below.

(1) Paragraph 5.1, Single Failure: The safety-related I&C systems are designed to ensure that safety-related functions required for design basis events (DBE) are performed in the presence of: (a) single detectable failure within safety-related systems concurrent with all non-detectable failures; (b) failures caused by the single failure; and (c) failures and spurious system actions that cause, or are caused by the design basis event, requiring the safety-related functions as identified in the applicable failure modes and effects analysis (FMEA).

(2) Paragraphs 5.2 & 7.3, Completion of Protective Actions: The safety-related I&C systems are designed so that a) once initiated (automatically or manually), the intended sequence of the safety-related functions of the execution features continue until completion, and b) after completion, deliberate operator action is required to return the safety-related system to normal.

(3) Paragraph 5.3, Quality: A: safety-related I&C equipment is provided under the 10 CFR PArt 50 Appendix B quality program. This satisfies all applicable requirements of the following: 1) 10 CFR Part 50 Appendix B and 2) ANSI/ASME NQA-1. The safety-related digital I&C software and/or firmware conform with the quality requirements of IEEE 7-4.3.2.

(4) Paragraph 5.4, Equipment Qualification: The safety-related I&C equipment is designed to meet its functional requirements over the range of environmental

conditions for the area in which it is located. The equipment is designed to meet the equipment qualification requirements set forth by this criterion.

(5) Paragraph 5.5, System Integrity: The safety-related I&C systems are designed to demonstrate that the safety system performance is adequate to ensure completion of protective actions, over a range of transient and steady state conditions, as enumerated in the design basis.

(6) Paragraph 5.6, Independence: For the safety-related I&C systems, there is physical, electrical, and commmunication independence between redundant portions of safety-related systems and between safety-related systems and nonsafety-related systems, as discussed in the applicable Sections.

(7) Paragraph 5.7, Capability for Test & Calibration: The safety-related I&C systems are designed with the capability to have their equipment tested and calibrated while retaining their capability to accomplish their safety functions.

(8) Paragraph 5.8, Information Displays: The information display design is discussed in Chapter 18. This design process includes the necessary steps to ensure compliance with regulatory requirements and the guidance provided in RG 1.47 for bypass and inoperable status indication and in RG 1.97 for accident monitoring instrumentation as discussed in Section 7.5.

(9) Paragraph 5.9, Control of Access: The safety-related I&C systems have features that facilitate the administrative control of access to safety-related system equipment.

(10) Paragraph 5.10, Repair: The safety-related analog and digital based I&C systems are designed to allow the timely recognition of malfunctioning equipment location to allow the replacement, repair and/or adjustment. Self-diagnostic functions and periodic testing will identify and locate the failure. Individual bypassing allows the failed equipment to be replaced or repaired on-line without affecting the protection function.

(11) Paragraph 5.11, Identification: Safety-related I&C equipment conforms with the identification requirements of this criterion. Safety-related equipment is distinctly marked for each redundant portion of a system with identifying markings. Hardware components or equipment units have an identification label or a nameplate. For digital platforms, versions of computer hardware, software and/or firmware are distinctly identified. Proper configuration management plans are implemented as a way to formalize this identification process.

(12) Paragraph 5.12, Auxiliary Features: STP 3&4 safety-related I&C system auxiliary supporting features satisfy the requirements of this criterion where applicable. For example, power supply and HVAC are key auxiliary supporting systems that satisfy the applicable requirements of IEEE-603. Other key auxiliary features are designed such that these components will not degrade the safety-related I&C systems below an acceptable level.

(13) Paragraph 5.13, Multi Unit Stations: The safety-related I&C systems meet the requirements of GDC 5, Sharing of structures, systems and components. The

capability to simultaneously perform required safety functions in both Units is not impaired by interactions between Units.

(14) Paragraph 5.14, Human Factors Considerations: Human factor scenarios are considered throughout all stages of the design process. Detailed information regarding these considerations can be found in Chapter 18.

(15) Paragraph 5.15, Reliability: The degree of redundancy, diversity, testability, and quality of the STP 3&4 safety-related I&C design adequately addresses the functional reliability necessary to perform its safety protection functions. As stated above, the safety-related I&C equipment is provided under an Appendix B quality program.

(16) Paragraphs 6.1 and 7.1, Automatic Control: The safety-related I&C systems provide the means to automatically initiate and control the required safety-related functions.

(17) Paragraphs 6.2 and 7.2, Manual Control: The safety-related I&C systems have features in the main control room and remote shutdown system to manually initiate and control the automatically initiated safety-related functions at the division level.

(18) Paragraph 6.3, Interaction between the Sense and Command Features and Other Systems: The safety-related I&C systems meet the independence and separation requirements such that nonsafety-related systems failures will not affect of prevent any safety-related protection function. The normal communication path is one-way such that the safety-related systems will only broadcast to nonsafety-related systems and not vice versa. There is limited nonsafety-related communication under programmatic control to safety-related systems as discussed in Section 7.9S.

(19) Paragraph 6.4, Derivation of System Inputs: To the extent feasible, the protection system inputs are derived from signals that directly measure the designated process variables.

(20) Paragraph 6.5, 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 have a known relationship with each other, and that have read-outs available, or introducing and varying substitute input to the sensor of the same nature as the measured variable. When one channel is placed into maintenance bypass mode, the condition is alarmed in the MCR and actuation logic capability is maintained to ensure the continued availability of all protective actions. Most sensors and actuators are designed to provide actual testing and calibration during power operation.

(21) Paragraphs 6.6 and 7.4, Operating Bypasses: The safety-related I&C systems automatically prevent the activation of an operating bypass whenever the applicable permissive conditions for an operating bypass are not met, and remove activated operating bypasses if the plant conditions change so that an activated operating bypass is no longer permissible.

(22) Paragraphs 6.7 and 7.5, Maintenance Bypasses: The capability of safety-related systems to perform their safety-related functions is retained when one division of the I&C systems is in maintenance bypass.

(23) Paragraph 6.8, Setpoints: STP 3&4 safety-related instrument setpoints are determined by a methodology that follows the guidance contained in the STP 3&4 setpoint methodology program. This methodology uses STP 3&4 plant specific analyses to ensure that characteristics such as range, accuracy, and resolution of the instruments meet the performance requirements assumed n the safety analyses in Chapter 15. The response times of the I&C systems are assumed in the safety analyses and verified by STP 3&4 surveillance testing or system analyses.

The power source design requirements for the safety-related I&C systems are discussed in Chapter 8.

Table 7.1-1 Comparison of GESSAR II and ABWR I&C Safety Systems

I & C System	GESSAR II Design	ABWR Design
General Comparisons for All Safety Systems:	Hard wired sensor interfaces.	~~*Multiplexed*~~ **Hard Wired** sensor interfaces.
	Nuclear system protection system (NSPS) solid-state-based logic and self-test system controllers.	Safety system logic & control (SSLC) **configurable logic devices and** microprocessor-based logic ~~*and*~~ **with** ~~*self-test*~~**self diagnostic functions** ~~*system controllers*~~.
Flammability Control System:	Part of combustible gas control system.	~~*Independent system.*~~**This system deleted**
Standby Gas Treatment System:	Redundant active and passive components.	Redundant active components; ~~*single filter train.*~~**two filter trains, two separate divisions.**

Table 7.1-2 Regulatory Requirements Applicability Matrix for I&C Systems

Applicable Criteria	10CFR 50.55	GDC																					
		2	4	10	12	13	15	16	19	20	21	22	23	24	25	28	29	33	34	35	38	41	44
Reference Standard (RG, IEEE, ISA)	~~279~~**603**																						

Table 7.1-2 Regulatory Requirements Applicability Matrix for I&C Systems (Continued)

Applicable Criteria	Regulatory Guide								BTP						II-D	II-E	II-F		II-K						
	1.22	1.62	1.75	1.97	1.105	1.118		1.151	3	12	20 (7.6)	21	22	26 (7.9)	3	4.2	1	3	1.23	3.13	3.15	3.18	3.21	3.22	3.23
Reference Standard (RG, IEEE, ISA)	~~279~~**603**	~~279~~**603**	384		567.04	338		567.02	~~279~~**603**	~~279~~**603**	~~279~~**603**	RG 1.47	RG 1.22	~~279~~**603**				RG 1.97							

Note: IEEE 603 has superceded the use of IEEE 279. In instances where NRC documents applicable to STP 3&4 still refer to the outdated IEEE 279 standard, both the referenced IEEE 279 requirements and the analogous IEEE 603 requirements will be used. In cases of conflict between requirements in the different standards, IEEE 603 requirements govern.

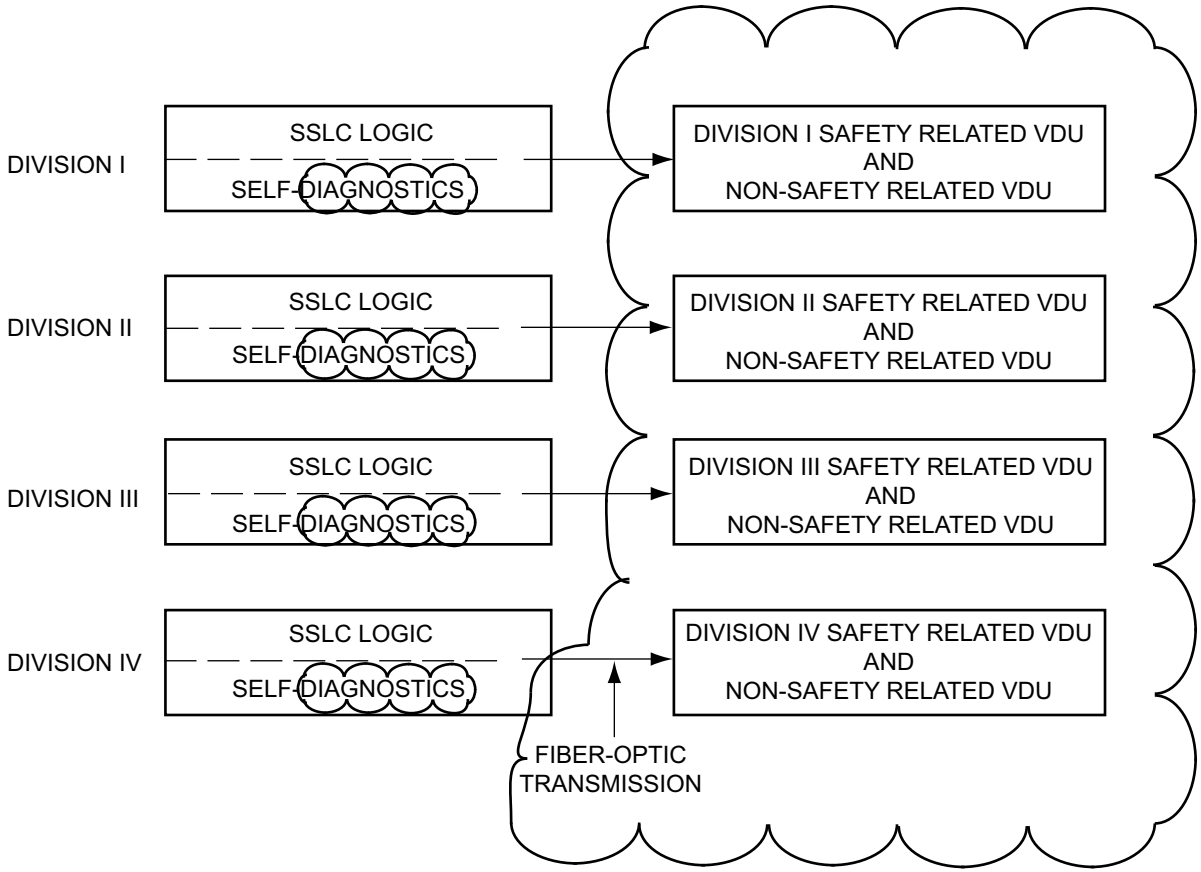
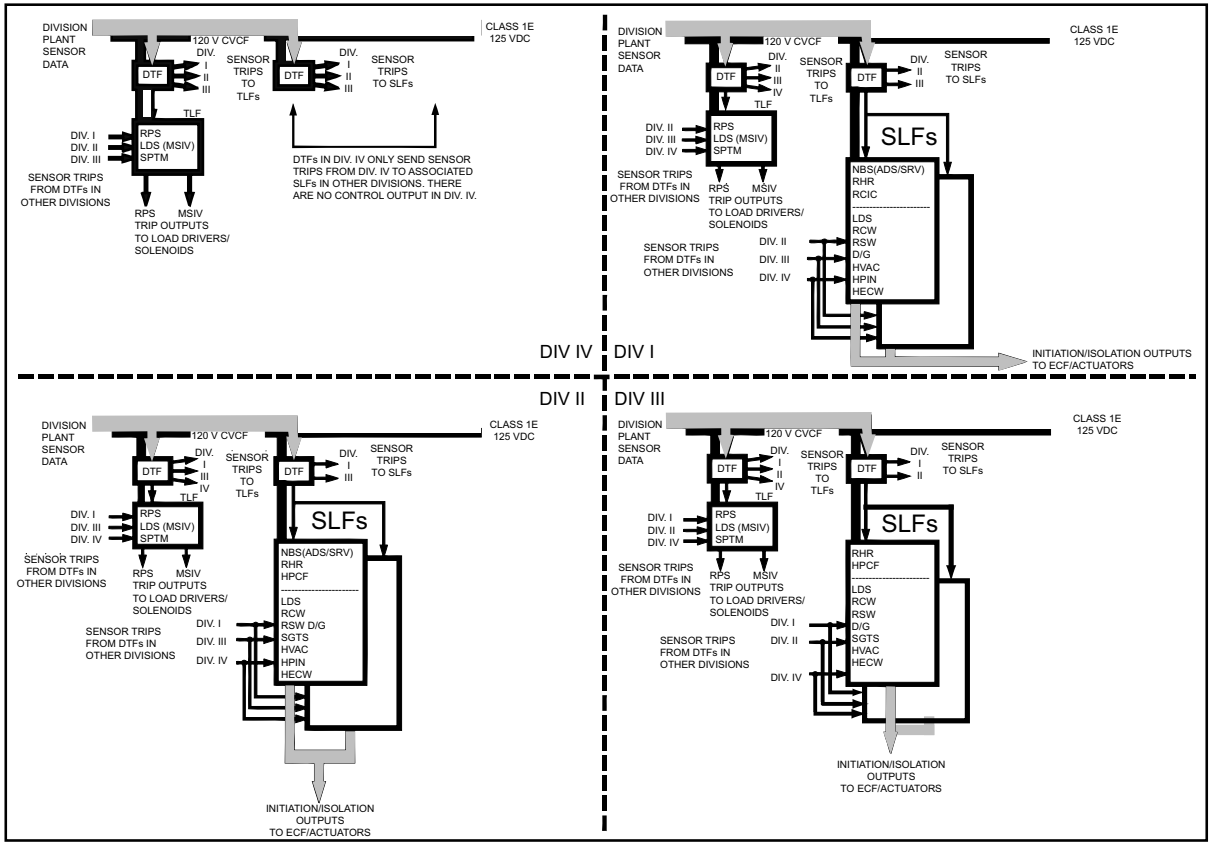


Figure 7.1-1 SSLC Self-~~*Test System*~~ Diagnosis



ABBREVIATIONS
DTF = DIGITAL TRIP FUNCTION
ECF = ESSENTIAL COMMUNICATION FUNCTION
SLF = SAFETY SYSTEM LOGIC FUNCTION
TLF = TRIP LOGIC FUNCTION

D/G = DIESEL GENERATOR
ESF = ENGINEERED SAFETY FEATURES
HECW = HVAC EMERGENCY COOLING WATER
HPCF = HIGH PRESSURE CORE FLOODER
HPIN = HIGH PRESSURE NITROGEN GAS SUPPLY
HVAC = HEATING, VENTILATING & AIR CONDITIONING
LDS = LEAK DETECTION & ISOLATION SYSTEM
MSIV = MAIN STEAM ISOLATION VALVE
NBS = NUCLEAR BOILER SYSTEM

NMS = NEUTRON MONITORING SYSTEM
PRM = PROCESS RADIATION MONITORING
RCIC = REACTOR CORE ISOLATION COOLING
RCW = REACTOR BUILDING CLOSED COOLING WATER
RHR = RESIDUAL HEAT REMOVAL
RPS = REACTOR PROTECTION SYSTEM
RSW = REACTOR SERVICE WATER
SGTS = STANDBY GAS TREATMENT SYSTEM
SPTM = SUPPRESSION POOL TEMPERATURE MONITORING

NOTES:
1. NMS AND PRM (NOT SHOWN) ARE STANDALONE SYSTEMS WITH TRIP OUTPUTS TO RPS AND ESF CONTROLLERS OF SSLC
2. POWER SOURCES (PER DIVISION)
ECF: CLASS 1E, 125 VDC and 120 CVCF
ESF: CLASS 1E, 125 VDC
RPS/MSIV: CLASS 1E, 120 CVCF
NMS/PRRM: CLASS 1E, 120 CVCF

Figure 7.1-2 Assignment of Interfacing Safety System Logic to SSLC Controllers