7.0 Instrumentation and Control Systems

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 7.1-1

STD DEP 7.1-2

STD DEP 7.1-3

STD DEP 7.2-1

STD DEP 7.4-1

STD DEP Admin (Table 7.1-1)

7.1.1 Identification of Safety-Related Systems

7.1.1.1 General

STD DEP T1 3.4-1

Divisional separation is also applied to the ~~essential multiplexing system (EMS)~~ Essential Communication Function (ECF) for Safety System Logic and Control (SSLC)*, 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: (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 Pool 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.

7.1.2 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).~~ 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 safety system setpoints are listed in the ~~Chapter 16~~ Instrument Setpoint Summary Report *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 and ESF 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.~~ Remote Digital Logic Controllers (RDLCs). *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 monitoring network, and an offline semi-automatic (operator initiated, but automatic to completion), end-to-end surveillance program. Both online and offline functions operate independently within each of the four divisions. There are no multi-divisional interconnections associated with self-testing.

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

The following standard supplement enhances the design description.

The test function does not degrade system reliability. The logic returns to its original state after the test sequence is completed. Indications of test status (normal or in-test) and results (pass, fail) is provided.

Self-diagnosis includes monitoring of overall program flow, reasonableness of process variables, RAM and PROM condition, and device interlock logic. Testing includes continuous error checking of all transmitted and received data on the ~~serial data~~ data communication *links of each SSLC controller; for*

example, error checking by parity check, checksum, or cyclic redundancy checking (CRC) techniques.

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

The ~~Essential Multiplexing System (EMS)~~ Essential Communication Function (ECF) *is included in the continuous, automatic self-test 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~~* ECF *after a detected fault, such that the least effect on system availability occurs.*

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

To reduce operator burden and decrease outage time, a surveillance test controller (STC) is provided as a dedicated instrument in each division of ~~SSLC~~ ELCS. *The STC performs semi-automatic (operator-initiated) 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.

The STC injects test patterns through the ~~EMS~~ Essential Communication Function (ECF) of the ELCS *communications links to the ~~RMUs~~* RDLCs. *It then tests the ~~RMUs~~* "RDLCs" *ability to format and transmit sensor data through and across the ~~EMS/SSLC~~* ECF of the ELCS *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 7.4-1

(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.

7.1.2.6 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).

(2) Non-safety-Related Design Bases

The SRNM Subsystem shall be able to perform the following functions:

(d) Provide a continuous measure of the time rate of change of neutron flux (reactor period) over the range from –100 s to (–) infinity and (+) infinity to ~~*+10s*~~ *+3s.*

7.1.2.6.1.2 Flow Rate Subsystem

STD DEP 7.1-2

(1) Safety Design Bases

General Functional Requirements:

The flow rate subsystem, as part of the APRM Subsystem, provides the control and reference signal for the APRM core flow-rate dependent trips. It ~~consists of a flow measurement from the recirculation system and signal conditioning equipment~~ does this by converting a core plate differential pressure signal from the Recirc Flow Control System (RFC) into a core flow rate signal.

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).

7.1.2.6.1.5 Automated Traversing Incore Probe (ATIP) Subsystem

STD DEP 7.1-3

(2) Non-Safety-Related Design Bases

The ATIP shall meet the following power generation design bases:

(d) Provide an automatic function of retracting ATIP and closing the containment isolation valves for the ATIP lines in response to an LDI signal

7.1.2.6.2 Process Radiation Monitoring System

STD DEP T1 2.3-1

STD DEP 7.2-1

STD DEP 7.1-1

(1) Safety Design Bases

General Functional Requirements:

(d) Provide channel trip inputs ~~to the RPS and LDS~~ to the system logic *on high radiation in the MSL tunnel area. If the ~~protection~~ system logic is satisfied, the ~~following shall be initiated:~~* system will initiate shutdown of the mechanical vacuum pump and closure of the mechanical pump discharge line isolation valve.

~~(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.

~~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 radiation levels and for concentration of hydrogen and oxygen gases, primarily during post-accident conditions.

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 ~~8.3.1.3 and 8.3.1.4~~ 8.3.3.6.2.)

7.1.2.10 Conformance to Regulatory Guides

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) and the analytical or design basis limit are contained in the Instrument Setpoint Summary Report. ~~*The trip setpoint (instrument setpoint) allowance value (Tech Spec limit) and the analytical or design basis limit are all*~~ The allowable values are contained in the Technical Specifications (Chapter 16). ~~*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

The following standard supplement addresses design-related information originally provided in Appendix 7A of the reference ABWR DCD.

7.1.2.11.7 IEEE 603 Standard Criteria for Safety Systems for Nuclear Power Generating Stations

The microprocessor hardware and software which make up the Safety System Logic and Control (SSLC) is designed to make logic decisions which automatically initiate safety actions

based on input from instrument monitored parameters for several nuclear safety systems. In that sense, the SSLC integrates the nuclear safety systems.

Most positions stated in IEEE 603 (as endorsed by RG 1.153) pertain to the nuclear safety systems, and are similar to those of IEEE 279, which are addressed for each system in the analysis sections of Chapter 7. Safety system design bases are described for all I&C systems in Section 7.1, beginning at Subsection 7.1.2.2. Setpoints and margin may be found in the Instrument Setpoint Summary Report.

The safety system criteria in Section 5 of IEEE 603 are not compromised by the introduction of the SSLC. All positions regarding single-failure, completion of protective actions, etc., are designed into the protection systems. All SSLC components associated with the protection systems are Class 1E and are qualified to the same standards as the protection systems.

Independence of the four SSLC electrical divisions is retained by using fiber-optic cable for cross-divisional communication such as the two-out-of-four voting logic. Capability for test and calibration is greatly enhanced by the SSLC's self-test subsystem (STS) as described in Subsection 7.1.2.1.6.

In summary, the hardware and software functions of the microprocessors used in the SSLC comply with applicable portions of IEEE 603 and Regulatory Guide 1.153 (i.e., quality, qualification, testability, independence). The remaining portions, which apply to the nuclear safety systems, are not compromised by the SSLC design, but are in fact enhanced by self-test.

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

I & C System	GESSAR II Design	ABWR Design
General	Hard wired sensor interfaces.	~~Multiplexed~~ **Networked** sensor interfaces.
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.**

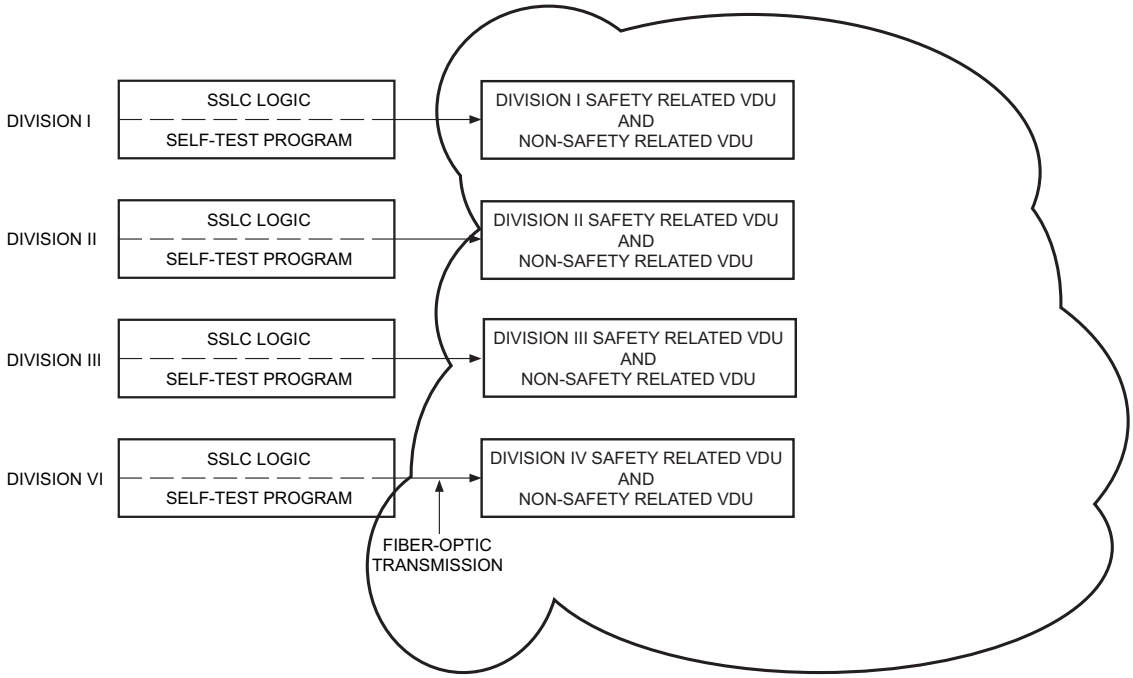

Figure 7.1-1 SSLC Self-Test System

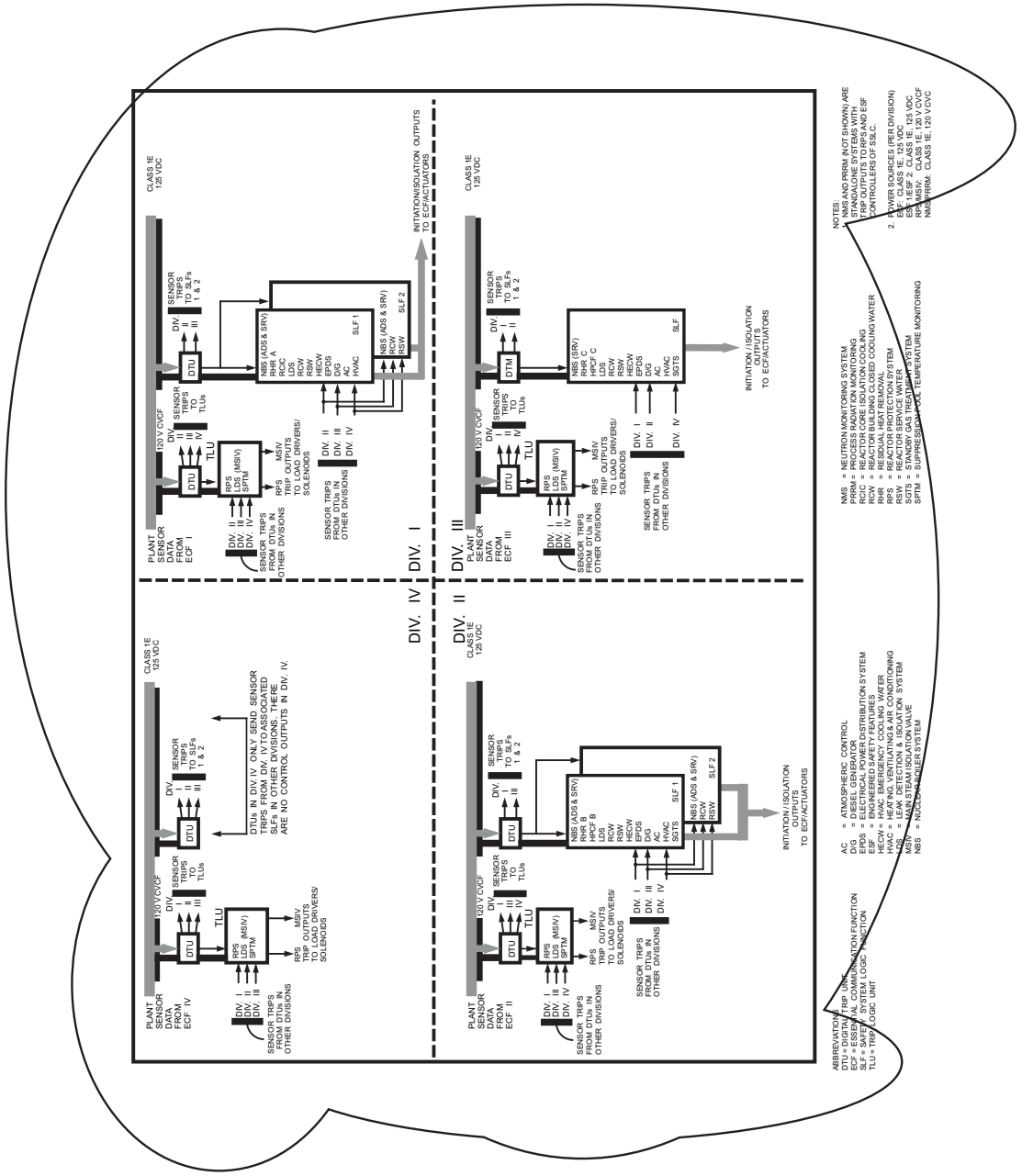

Figure 7.1-2 Assignment of Interfacing Safety System Logic to SSLC Controllers