3.4 Instrumentation and Control

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

STD DEP T1 3.4-1

Introduction

Subsection A provides a description of the configuration of safety-related, digital instrumentation and control (I&C) equipment encompassed by Safety System Logic and Control (SSLC). Subsection B contains a description of the hardware and software development process used in the design, testing, and installation of I&C equipment. This includes descriptions of the processes used to establish programs that assess and mitigate the effects of electromagnetic interference, establish setpoints for instrument channels, and ensure the qualification of the installed equipment. Subsection C discusses the diverse features implemented in I&C system design to provide backup support for postulated worst-case common-mode failures of SSLC.

The devices addressed in this section are electronic components of the ABWR's I&C systems. These components ~~are configured as~~ include *real-time ~~microcontrollers that use~~ microprocessors and ~~other programmable~~* configurable *logic devices to perform data acquisition, data communications, and system logic processing. These components also contain automatic, on-line self-diagnostic features to monitor these tasks and off-line test capability to aid in maintenance and surveillance. The operating programs for these controllers are integrated into the hardware as firmware ~~[software permanently stored in programmable read-only memory (PROM)]~~. A controller's operating system can permit field adjustment of selected parameters under proper change control. Adjustable parameters are stored in ~~electrically-alterable read-only~~ memory ~~(EAROM) or equivalent~~* that can only be altered through the use of special equipment or procedures.

3.4.1 *Safety System Logic and Control*

Design Description

~~Safety-related monitoring and trip logic for the plant protection systems resides in SSLC equipment. SSLC integrates the automatic decision-making and trip logic functions and manual operator initiation functions associated with the safety actions of the safety- related systems.~~ Safety System Logic and Control (SSLC) is a general term that encompasses the logic and controls associated with safety-related systems. This includes automatic and manual protection and control functions. *~~SSLC generates the protective function signals that activate reactor trip and provide safety-related mitigation of reactor accidents.~~* SSLC is primarily implemented through the Reactor Trip and Isolation System (RTIS), which supports the reactor protection and main steam isolation functions, and the ESF Logic and Control System (ELCS), which supports the accident mitigation functions. Also included in SSLC are the Neutron Monitoring System (NMS), the Containment Monitoring System (CMS) and the safety-related portions of the radiation monitoring systems. *The relationship between SSLC and systems for plant protection is shown in Figure 3.4a.*

SSLC equipment comprises microprocessor-based, software-controlled signal processors that perform signal conditioning, setpoint comparison, trip logic, system initiation and reset, self-test, calibration, and bypass functions. The signal processors associated with a particular safety-related system are an integral part of that system. Functions in common, such as self test, calibration, bypass control, power supplies and certain switches and indicators, belong to SSLC. However, SSLC is not, by itself, a system; SSLC is the aggregate of signal processors for several safety-related systems. SSLC hardware and software are classified as Class 1E, safety-related.

Sensors used by the safety-related systems can be either analog, such as process control transmitters, or discrete, such as limit switches and other contact closures. While some sensor signals are hardwired directly to the SSLC processors, most sensor signals are transmitted from the instrument racks in the Reactor Building to the SSLC equipment in the Control Building via the Essential Multiplexing System (EMS) Sensor signals interface with the SSLC through input/output (I/O) devices located remotely or in the control room. The I/O devices communicate with other divisional devices through networks and datalinks as discussed in Subsection 2.7.5. *Both analog and discrete sensors are connected to remote multiplexing units (RMUs) in local areas, which*These devices also *perform signal conditioning, analog-to-digital conversion for continuous process inputs, change-of-state detection for discrete inputs, and message formatting prior to signal transmission.* In applicable cases, they also perform other system functions, such as interlock-type functions related specifically to the actuated equipment. *The RMUs are limited to acquisition of sensor data and the output of control signals. Trip decisions and other* primary *control logic functions are performed in SSLC processors in the main control room area*Control Building.

*The basic hardware*functional *configuration for one division of SSLC is shown in Figure 3.4b. Each division runs independently (i.e., asynchronously) with respect to the other divisions. The following steps describe the processing sequence and associated function descriptions for incoming sensor signals and outgoing control signals. These steps are performed simultaneously and independently in each of the four divisions:*

For the RTIS portion of SSLC, including reactor trip and main steam isolation valve (MSIV) isolation, the steps are:

(1) Remote sensor inputs are acquired, conditioned, and digitized.

(2) *(1) The digitized sensor inputs from RMUs are received in the control room at control room multiplexing units (CMUs), which associate sensor signals with their logic processing channel. These sensor signals are decoded by a microprocessor-based function, the Digital Trip Module (DTM). For sensor signals hardwired to the control room, the DTM also performs digitizing and signal conditioning tasks. For each system function, the DTM then compares these inputs to preprogrammed threshold levels (setpoints) for possible trip action. The DTM provides a discrete trip decision for each setpoint comparison.*This digitized sensor information is used as input to the Digital Trip Function (DTF). For each system function, the DTF is a comparison of

sensor inputs to pre-programmed threshold levels (setpoints) for possible trip action. The result of the DTF is a discrete trip decision for each setpoint comparison. Each safety division performs the same DTF trip decision based on the independent sensor inputs associated with its own division.

(3) ~~*(2) Ford Reactor Protection System (RPS) trip and main steam isolation valve (MSIV) closure functions, trip outputs from the DTM are then compared, using a 2- out-of-4 coincidence logic format, with trip outputs from the DTMs of the other three divisions. The trip outputs are compared in by the trip logic unit (TLU), another microprocessor-based device. The logic format for the DTM and TLU is fail-safe (i.e., de-energize-to-operate). Thus, a reactor trip or MSIV closure signal occurs on loss of input signal or power to the DTM, but, because of the 2- out-of-4 logic format in the TLU, a tripped state does not appear at the output of the TLU (for a single division loss of power). Loss of signal or power to a division's TLU also causes a tripped output state, but the 2- out-of-4 configuration of actuator load drivers prevents de-energization of the pilot valve solenoids.*~~ The trip decisions from the DTF in each division are used as input to the Trip Logic Function (TLF) performed by each of the four safety divisions. The DTF trip decision results are passed to other divisions through isolated communication links as described in Section 2.7.5. The TLF is another microprocessor-based function that is a comparison of DTF trip decisions from all four safety divisions resulting in trip output decisions based on 2-out-of-4 coincidence logic format. The logic format is fail-safe (i.e. loss of signal causes trip conditions) for the TLF and associated DTF. Loss of signal or power to a single division's equipment performing the TLF causes a tripped output state from the TLF, but the 2-out-of-4 configuration of the actuator load drivers prevents simultaneous de-energization of both pilot valve solenoids.

The TLF also receives input directly from the Neutron Monitoring System and manual control switches.

(4) ~~*(3)*~~ The trip coincident logic output ~~*Trip outputs are sent*~~ *from the* ~~*TLU*~~ TLF is sent to ~~*to the RPS and MSIV output logic units*~~ Output Logic Units *(OLUs). The OLUs use non-microprocessor* ~~*circuitry*~~ devices *to provide a diverse (i.e., not software-based) interface for the following manual functions:*

(a) Manual reactor trip (per division: 2-out-of-4 for completion).

(b) MSIV closure (per division: 2-out-of-4 for completion).

(c) MSIV closure (eight individual control switches).

(d) RPS and MSIV trip reset.

(e) ~~*TLU*~~ TLF *output bypass*

The OLUs distribute the automatic and manual trip outputs to the MSIV pilot valve and scram pilot valve actuating devices and provide control of trip seal-

in, reset, and ~~TLU~~ TLF *output bypass (division-out-of-service bypass). Bypass inhibits automatic trip but has no effect on manual trip. The OLUs also provide a manual test input for de-energizing a division's parallel load drivers (part of the 2-out-of-4 output logic arrangement) so that scram or MSIV closure capability can be confirmed without solenoid de-energization. The OLUs are located external to the ~~TLU~~* equipment that implements the TLF *so that manual MSIV closure or manual reactor trip (per division) can be performed either when a division's microprocessor logic is bypassed or when failure of sensors or microprocessor logic equipment causes trip to be inhibited.*

(5) If a 2-out-of-4 trip condition is satisfied within the TLF, all four divisions' trip outputs produce a simultaneous coincident trip signal (e.g., reactor trip) and transmit the signal through hardwired connections to load drivers that control the protective action of the final actuators. The load drivers for the solenoids are themselves arranged in a 2-out-of-4 configuration, so that at least two divisions must produce trip outputs for protective action to occur. *~~Trips are transmitted across divisions for 2- out-of-4 voting via fiber optic data links to preserve signal isolation among divisions. The TLU also receives inputs directly from the trip outputs of the Neutron Monitoring System, manual control switches, and contact closures from limit switches and position switches used for equipment interlocks. In addition, plant sensor signals and contact closures that do not require transmittal to other divisions for 2- out-of-4 trip comparison are provided as inputs directly to the TLU. In this case, the TLU also performs the trip setpoint comparison (DTM) function.For Leak Detection and Isolation System (LDS) functions (except MSIV), emergency core cooling system (ECCS) functions, other safety-related supporting functions, and Electrical Power Distribution System functions such as diesel generator start and load sequencing, logic processing is performed as above, but in DTMs separate from the RPS/MSIV DTMs and in Safety System Logic Units (SLUs). The SLUs are similar to TLUs, but are dual redundant in each processing channel for protection against inadvertent initiation. Dual SLUs both receive the same inputs from the DTM, manual control switch inputs, and contact closures. Both SLU outputs must agree before the final trip actuators are energized. The logic format for the DTM and SLUs is fail-as- is (i.e., energize-to-operate) for ECCS and other safety-related supporting functions. Thus, loss of power or equipment failure does not cause a trip or initiation action. However, containment isolation signals are in fail-safe format and cause an isolation signal output on loss of power or signal. Besides performing 2-out-of-4 voting logic, the SLUs also provide interlock logic functions conforming to the logic diagram requirements of each supported safety system.~~*

~~As shown in Figure 3.4b, a pair of SLU are located in each of two engineered safety feature (ESF) processing channels, ESF1 and ESF2. ESF1 processes initiation logic for functions which service the reactor vessel at low pressure (e.g. RHR), while ESF2 provides the same support for the~~

~~vessel at high pressure (e.g. Reactor Core Isolation Cooling (RCIC) System and High Pressure Core Flooder (HPCF) System). Associated LDS and ESF functions are also allocated to these logic channels.~~

The ELCS portion of SSLC is implemented by equipment that is independent from that of the RTIS. For ELCS, the steps are:

(1) Remote sensor inputs are acquired, conditioned, and digitized.

(2) This digitized sensor information is used as input to the DTF, which is functionally the same as that described for the RTIS portion of SSLC.

(3) The actuation decisions from the DTF in each division are used as input to the Safety System Logic Function (SLF) performed by each of the four safety divisions. The DTF actuation decision results are passed to other divisions through isolated communication links as described in Section 2.7.5. The SLF is a microprocessor-based function that includes a comparison of DTF actuation decisions from all four safety divisions resulting in actuation output decisions based on 2-out-of-4 coincidence logic format. The logic format for the SLF and associated DTF is fail-as-is (i.e., loss of signal does not cause change of operational state) for ECCS and other safety-related supporting functions. However, air and solenoid-operated containment isolation signals are in fail-safe format and cause an isolation signal output on loss of power or signal. Besides performing 2-out-of-4 voting logic, the SLF also includes interlock logic functions conforming to the system functional requirements of each safety system.

The SLF logic for ECCS functions (i.e. initiation of Reactor Core Isolation Cooling, High Pressure Core Flooder, Low Pressure Core Flooder or Automatic Depressurization) is implemented using redundant processing channels. The redundant channels receive the same input data from the DTF, manual control switch inputs and contact closures and perform the same trip decision logic. A majority of the redundant processors must agree for initiation of the function to occur, in order to assure that failure of a single electronic module will not result in inadvertent coolant injection into the core or inadvertent depressurization. The final majority vote of the system initiation signals is accomplished with non-microprocessor based equipment in the logic or with a separate actuation of system valves and pumps, where both are required to initiate coolant injection.

The SLF logic for some isolation and supporting ESF functions are also implemented using redundant channels where such implementation increases the operator response time to avoid plant operational impact following postulated failure in the control equipment. In these cases, an operator bypass that reduces the logic to a single channel may be utilized where such logic reduces the risk of unnecessary adverse plant operational impact.

Other ELCS functions are implemented using redundancy where such logic provides overall plant operating or maintenance benefits.

~~*(4)*~~ ~~*(4)For reactor trip or MSIV closure if a 2- out-of-4 trip condition of sensors is satisfied, all four divisions' trip outputs produce a simultaneous coincident trip signal (e.g., reactor trip) and transmit the signal through hardwired connections (and isolators where necessary) to load drivers that control the protective action of the actuators. The load drivers are themselves arranged in a 2- out-of-4 configuration, so that at least two divisions must produce trip outputs for protective action to occur.*~~

(4) ~~*For ESF functions, the trip signals in three divisions are transmitted by the Essential Multiplexing System to the RMUs*~~ local inputs.~~*-where a final 2- out-of-2 logic comparison is made prior to distribution of the control signals to the final actuators. ESF outputs do not exist in Division IV.*~~The final SLF actuation outputs are distributed to the final system control elements through remote I/O devices. ELCS logic and controls are implemented through three divisions corresponding to the three divisions of controlled equipment.

~~*The DTM, TLU, and OLUs for RPS and MSIV in each of the four instrumentation divisions are powered from their respective divisional Class 1E AC sources. The DTMs and SLUs for ESF-1 and ESF-2 in Divisions I, II, and III are powered from their respective divisional Class 1E DC sources.*~~ RTIS and ELCS equipment is divisionally powered from multiple Class 1E AC power sources, at least one of which is DC backed (uninterruptible). ~~*In SSLC, independence*~~Independence is *provided between Class 1E divisions, and also between Class 1E divisions*~~*,*~~ *and* ~~*also*~~ *non-Class 1E equipment.*

For both RTIS and ELCS, ~~*Bypassing*~~bypassing of any single division of sensors (i.e., those sensors whose ~~*trip*~~ status is ~~*confirmed by*~~ part of a 2--out-of-4 logic) ~~*is*~~can be accomplished ~~*from each divisional SSLC cabinet*~~ by means of the manually-operated bypass unit. When such bypass is made, all four divisions of 2-out-of-4 ~~*input*~~ logic become 2-out-of-3 while the bypass state is maintained.~~*-During bypass, if any two of the remaining three divisions reach trip level for any sensed input parameter, then the output logic of all four divisions' trips (for RPS and MSIV functions) or the three ECCS divisions initiate the appropriate safety system equipment*~~.

Bypassing ~~*of any single*~~ a *division of* ~~*output*~~ *trip logic (i.e., taking a logic channel out of service)* ~~*is*~~can *also* be *accomplished by means of the bypass unit. This type of bypass is* ~~*limited*~~ applied *to the fail-safe* ~~*(de-energize-to-operate)*~~ *reactor trip and MSIV closure functions* (i.e. RTIS)~~*, since removal of power from energize-to-operate signal processors is sufficient to remove that channel from service*~~*.When a trip logic output bypass is* ~~*made*~~in effect*, the* ~~*TLU*~~ TLF *trip output in a division is inhibited from affecting the output load drivers by maintaining that division's load drivers in an energized state. Thus, the 2-out-of-4 logic arrangement of output load drivers for the RPS and MSIV functions effectively becomes 2-out-of-3 while the bypass is maintained.*

For both RTIS and ELCS, ~~Bypass~~ bypass *status is indicated in the main control room until the bypass condition is removed. An electrical interlock rejects attempts to remove more than one ~~SSLC~~ division from service at a time.*

~~*ESF1 and ESF2 logic are each processed in two redundant channels within each divisional train of ESF equipment. In order to prevent spurious actuation of ESF equipment, final output signals are voted 2-out-of-2 at the remote multiplexing units by means of series-connected load drivers at the RMU outputs. However, in the event of a failure detected by self-test within either processing channel, a bypass (ESF output channel bypass) is applied automatically (with manual backup) such that the failed channel is removed from service. The remaining channel provides 1-out-of-1 operation to maintain availability during the repair period. Channel failures are alarmed in the main control room. If a failed channel is not automatically bypassed, the operator is able to manually bypass the channel by a hardwired connection from the main control room.*~~

A portion of the anticipated transient without scram (ATWS) mitigation features is provided by SSLC circuitry, with initiating conditions as follows:

(1) Initiation of automatic Standby Liquid Control System (SLCS) injection: *High dome pressure and startup range neutron monitor (SRNM) ATWS permissive for 3 minutes or greater, or low reactor water level and SRNM ATWS permissive for 3 minutes or greater.*

(2) Initiation of feedwater runback: *High dome pressure and SRNM ATWS permissive for 2 minutes or greater. Reset permitted only when both signals drop below the setpoints.*

These ATWS features are implemented in four divisions of SSLC control circuitry that are functionally independent and diverse from the circuitry used for the Reactor Protection System (Figure 3.4c).

SSLC has the following alarms, displays, and controls in the main control room:

(1) SSLC signal processor inoperative (INOP).

(2) SSLC manual controls for bypass as described above.

(3) Displays for bypass status.

(4) Divisional flat display panels that provide display and control capability for manual ESF functions.

(5) Display and control of calibration and ~~*off-line*~~ self-test functions.

3.4.2 *I & C Development and Qualification Processes*

Hardware and Software Development Process

The ABWR design uses programmable digital equipment to implement operating functions of instrumentation and control (I&C) systems. The equipment is in the form of embedded controllers (i.e., a control program developed in software is permanently stored in ~~PROM~~ read only memory*, and thus becomes part of the controller's hardware).*

Electromagnetic Compatibility

Electromagnetic compatibility (EMC) is the ability of equipment to function properly when subjected to anticipated *~~an~~ electromagnetic ~~environment~~* environments. *An EMC compliance plan to confirm the level of immunity to ~~electrical~~* electromagnetic *noise is part of the design, installation, and pre-operational testing of I&C equipment*.

Electrical and electronic components supporting the systems and functions listed below are qualified according to the established plan for the anticipated levels of electrical interference at the installed locations of the components:

(1) *Safety System Logic and Control.*

(2) *~~Essential Multiplexing System~~* Essential Communication Functions (ECF)*.*

(3) *~~Non-Essential Multiplexing System~~* Non-Essential Communication Functions (NECF)*.*

(4) *Other microprocessor-based, software controlled systems or equipment.*

Instrument Setpoint Methodology

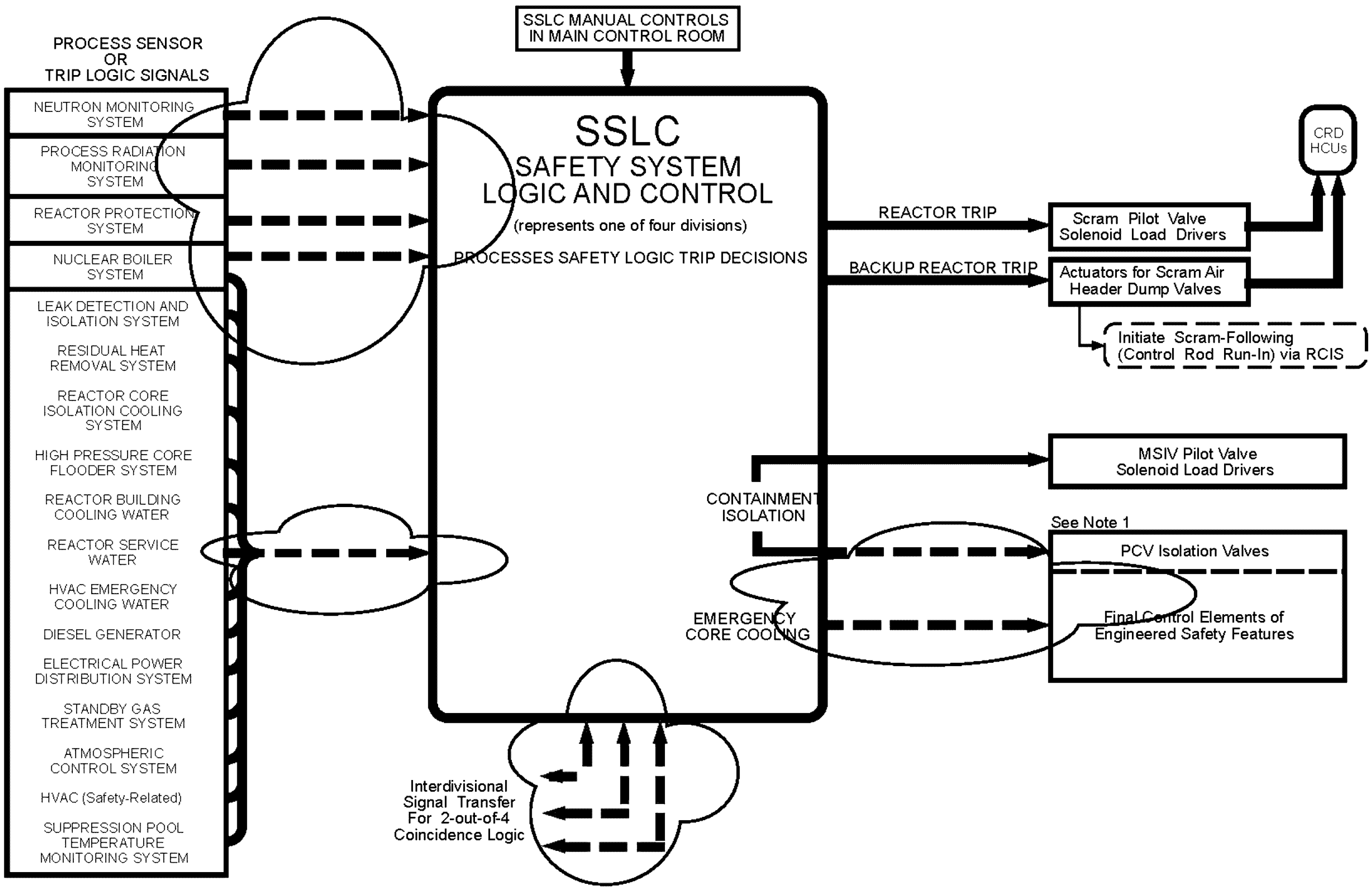
Signal Processing Devices in the Instrument Channel

Within an instrument channel, there may exist other components or devices that are used to further process the ~~electrical~~ signal provided by the sensor (e.g., analog-to-digital converters, signal conditioners, and *temperature compensation circuits~~, and multiplexing and demultiplexing components~~*)*. The worst-case instrument accuracy, calibration accuracy, and instrument drift contributions of each of these additional signal conversion components are separately or jointly accounted for when determining the characteristics of the entire instrument loop.*

3.4.3 Diversity and Defense-in-Depth Considerations

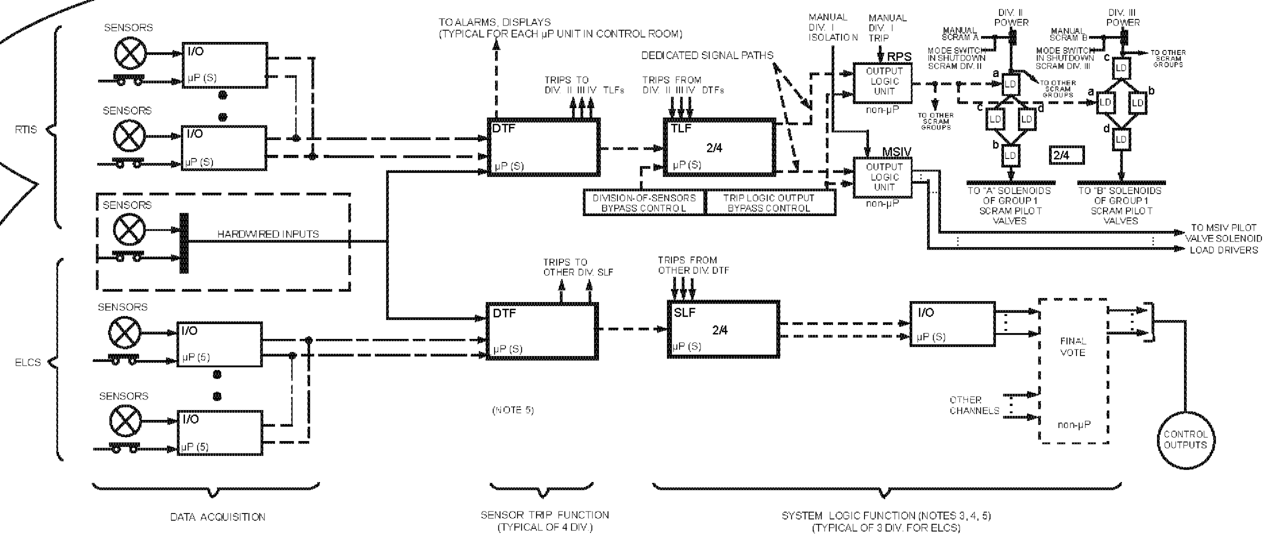
Subsection B discusses processes for developing hardware and software qualification programs that will assure a low probability of occurrence of both random and common-mode system failures for the installed ABWR I&C equipment. However, to address the concern that software design faults or other initiating events common to redundant, multi-divisional logic channels could disable significant portions of the plant's automatic standby safety functions (the reactor protection system and engineered safety features systems) at the moment when these functions are needed to mitigate an accident, several diverse backup features are provided for the primary automatic logic:

- *Manual scram and isolation by the operator in the main control room in response to diverse parameter indications.*
- *Core makeup water capability from the feedwater system, Control Rod Drive (CRD) System, and condensate system, which are diverse from SSLC ~~and the EMS~~.*
- *Availability of manual high pressure injection capability.*
- *Long term shutdown capability provided in a conventionally hardwired, 2-division, ~~analog~~* diverse *Remote Shutdown System (RSS); local displays of process variables* are provided *in RSS, are continuously powered, and so are available for monitoring at any time.*



Notes:
1. No PCV isolation trips or ECCS initiation outputs in Division IV

Figure 3.4a Safety System Logic and Control (SSLC) ~~Control~~ Interface Diagram



NOTES:

1. ARRANGEMENT SHOWN IS A SIMPLIFIED EXAMPLE FOR ONE DIVISION.

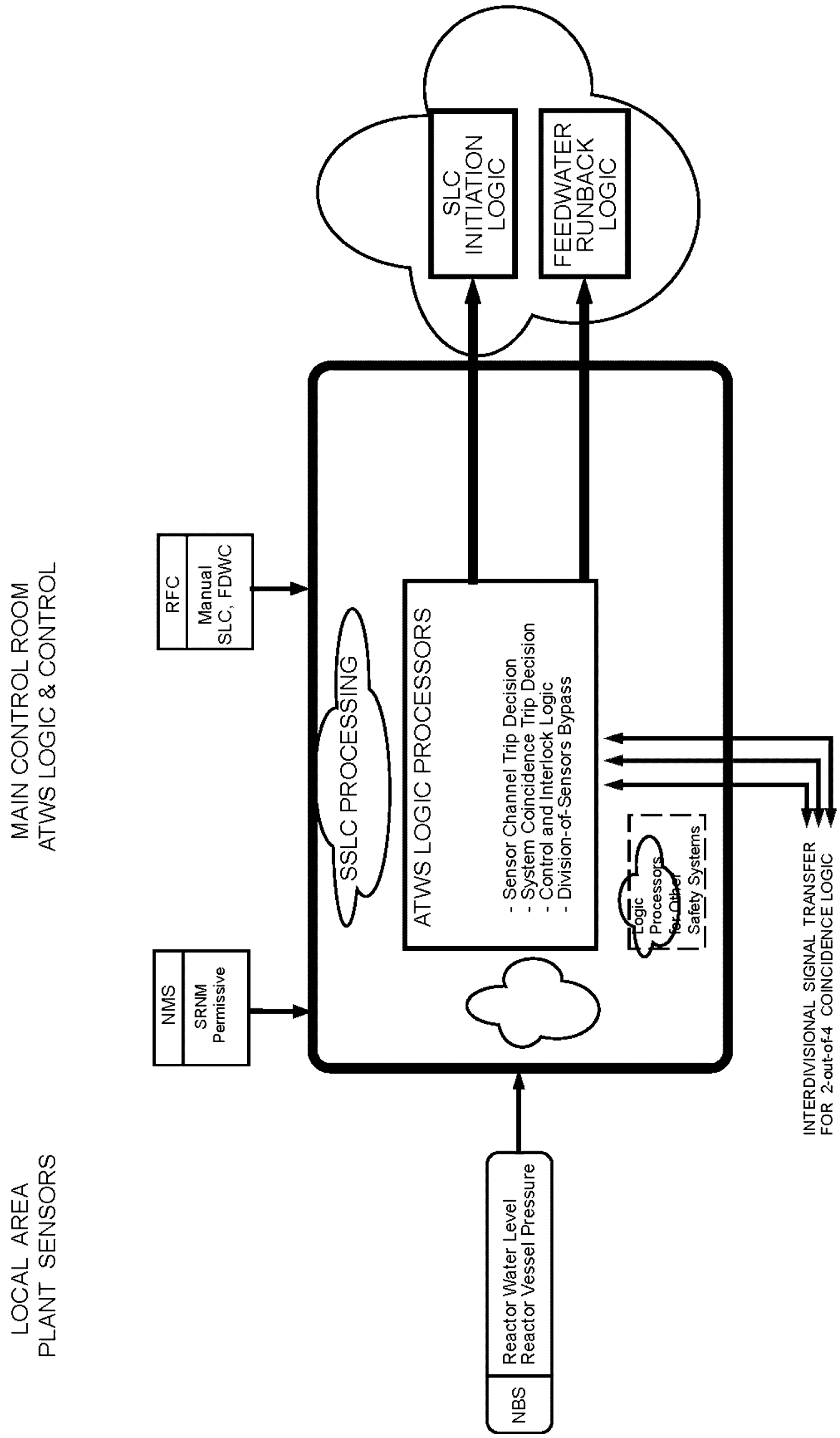
2. A. NOT ALL CONTROL SWITCH INPUTS SHOWN.
   B. INPUTS FROM NMS AND PRM NOT SHOWN.
   C. INTERDIVISIONAL COMMUNICATIONS USE FIBER - OPTIC DATA LINKS.

3. SYSTEM LOGIC FUNCTION (SLF) FOR ECCS FUNCTIONS IS IMPLEMENTED WITH REDUNDANT CHANNELS WITH A MINIMUM 2/2 VOTE OF THE OUTPUT SIGNALS TO PREVENT INADVERTENT COOLANT INJECTION OR DEPRESSURIZATION DUE TO SINGLE SLF ELECTRONICS FAILURE. THE OUTPUT VOTE MAY BE ACCOMPLISHED EITHER BY DIRECT VOTE OF SLF OUTPUT SIGNALS OR BY A "SYSTEM VOTE" WHERE BOTH VALVE AND PUMP ACTUATION IS REQUIRED TO INITIATE SYSTEM ACTION. BYPASS OF A FAILED SLF CHANNEL MAY BE PROVIDED AS LONG AS THE REMAINING OPERATIONAL CHANNELS PROVIDE A MINIMUM OF TWO SLF CHANNELS FOR ECCS FUNCTIONS.

4. SYSTEM LOGIC FUNCTION (SLF) FOR SOME ISOLATION AND SUPPORTING ESF FUNCTIONS MAY BE IMPLEMENTED WITH REDUNDANT CHANNELS WITH A NORMAL MINIMUM 2/2 VOTE OF THE OUTPUT SIGNALS WHERE INADVERTENT ACTUATION OF THE FUNCTION MIGHT REQUIRE UNREASONABLY SHORT REPAIR TIMES TO ELIMINATE OPERATIONAL IMPACT. FOR THESE FUNCTIONS, OPERATOR CONTROLLED BYPASS TO ALLOW OPERATION WITH A FINAL 1/1 VOTE IS PERMITTED.

5. EACH FUNCTION MAY BE ACCOMPLISHED BY MULTIPLE PROCESSORS TO MINIMIZE THE HARDWARE AND SOFTWARE COMPLEXITY OR OPERATIONAL IMPACT OF HARDWARE FAILURES, PROVIDED THE MINIMUM REDUNDANCY OF NOTES 3 AND 4 IS MAINTAINED.

Figure 3.4b Safety System Logic & Control Block Diagram



Notes:
1. Diagram represents one of four ATWS divisions.
2. Remaining ATWS functions are processed as part of Recirculation Flow Control System logic and Nuclear Boiler System logic.

Figure 3.4c Anticipated Transient Without Scram (ATWS) Control Interface Diagram

Table 3.4 Instrumentation and Control

Inspections, Tests, Analyses and Acceptance Criteria		
Design Commitment	**Inspections, Tests, Analyses**	**Acceptance Criteria**
Safety System Logic and Control		
3. The ~~*DTM, TLU*~~ **equipment implementing the DTF, TLF,** and OLUs for RPS and MSIV in each of the four instrumentation divisions are powered from their respective divisional Class 1E AC sources. The ~~*DTMs and SLUs*~~ **equipment implementing the DTF and SLF** for ESF ~~*1 and ESF 2*~~ in Divisions I, II, and III are powered from their respective divisional Class 1E DC sources, as ~~*are*~~ is the **equipment implementing the** ESF ~~*DTMs*~~ DTF in Division IV. In SSLC, independence is provided between Class 1E divisions and between Class 1E divisions and non-Class 1E equipment.	3. a. Tests will be performed on SSLC-by providing a test signal to the I&C equipment in only one Class 1E division at a time. b. Inspection of the as-installed Class 1E divisions in SSLC will be performed.	3. a. The test signal exists only in the Class 1E division under test in SSLC. b. In SSLC, physical separation or electrical isolation exists between Class 1E divisions. Physical separation or electrical isolation exists between these Class 1E divisions and non-Class 1E equipment.
4. SSLC provides the following bypass functions: a. Division-of-sensors bypass b. Trip logic output bypass c. ESF output channel bypass**, where applied**	4. Tests will be performed on the as-built SSLC as follows: a(1) Place one division of sensors in bypass. Apply a trip test signal in place of each sensed parameter that is bypassed. At the same time, apply a redundant trip signal for each parameter in each other division, one division at a time. Monitor the voted trip output ~~*at*~~ from each ~~*TLU and SLU*~~ **equipment component that implements a TLF or SLF**. Repeat for each division. a(2) For each division in bypass, attempt to place each other division in division-of- sensors bypass, one at a time.	4. Results of bypass tests are as follows: a(1)No trip change occurs at the voted trip output ~~*of*~~ **from** each ~~*TLU and SLU*~~ **equipment component that implements a TLF or SLF**. Bypass status is indicated in main control room. a(2) Each division not bypassed cannot be placed in bypass, as indicated at OLU output; bypass status in main control room indicates only one division of sensors is bypassed.

Table 3.4 Instrumentation and Control (Continued)

Inspections, Tests, Analyses and Acceptance Criteria		
Design Commitment	**Inspections, Tests, Analyses**	**Acceptance Criteria**
4. (continued)	4. (continued) b(1) Place one division in trip-logic-output bypass. Operate manual auto-trip test switch. Monitor the trip output at the RPS OLU. Operate manual auto-isolation test switch. Monitor the trip output at the MSIV OLU. Repeat for each division. b(2) For each division in bypass, attempt to place the other divisions in trip-logic- output bypass, one at a time. c~~(1)~~ Apply common test signal to any one pair of ~~*dual SLU*~~ **redundant SLF** signal inputs. Monitor test signal at ~~*voted 2-out-of-2*~~ output ~~*in RMU area*~~ **from equipment performing the ECF in local areas**. Remove power from **equipment performing** one ~~*SLU*~~ **SLF**, restore power, then remove power from equipment performing other ~~*SLU*~~ **SLF**. Repeat test for all pairs of ~~*dual SLUs*~~ **redundant sets of equipment implementing a SLF** in each division. ~~*c(2) Disable auto-bypass circuit in bypass unit. Repeat test c(1), but operate manual ESF loop bypass switch for each affected loop.*~~	4. (continued) b(1) No trip change occurs at the trip output of the RPS OLU or MSIV OLU, respectively. Bypass status is indicated in main control room. b(2) Each division not bypassed cannot be placed in bypass, as indicated at OLU output; bypass status in main control room indicates only one trip logic output is bypassed. c~~(1)~~ Monitored test output signal does not ~~*change state*~~ **initiate the system function** when power is removed from ~~*either SLU*~~ **the equipment performing any single SLF**. Bypass status and loss of power to ~~*SLU*~~ **equipment performing the SLF** are indicated in main control room. ~~*c(2) Monitored test output signal is lost when power is removed from either SLU, but is restored when manual bypass switch is operated. Bypass status, auto-bypass inoperable, and loss of power to SLU are indicated in main control room.*~~

Table 3.4 Instrumentation and Control (Continued)

Inspections, Tests, Analyses and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
Setpoint Methodology		
13. Setpoints for initiation of safety-related functions are determined, documented, installed and maintained using a process that establishes a plan for: a. Specifying requirements for documenting the bases for selection of trip setpoints. b. Accounting for instrument inaccuracies, uncertainties, and drift. c. Testing of instrumentation setpoint dynamic response. d. Replacement of setpoint-related instrumentation. The setpoint methodology plan requires that activities related to instrument setpoints be documented and stored in retrievable, auditable files.	13. Inspections will be performed of the setpoint methodology plan used to determine, document, install, and maintain instrument setpoints.	13. The setpoint methodology plan is in place. The plan generates requirements for: a. Documentation of data, assumptions, and methods used in the bases for selection of trip setpoints. b. Consideration of instrument channel inaccuracies (including those due to analog-to-digital converters, signal conditioners, **and** temperature compensation circuits, ~~and multiplexing and demultiplexing components)~~, instrument calibration uncertainties, instrument drift, and uncertainties due to environmental conditions (temperature, humidity, pressure, radiation, EMI, power supply variation), measurement errors, and the effect of design basis event transients are included in determining the margin between the trip setpoint and the safety limit. c. The methods used for combining uncertainties. d. Use of written procedures for preoperational testing and tests performed to satisfy the Technical Specifications. e. Documented evaluation of replacement instrumentation which is not identical to the original equipment.