

3.4 Instrumentation and Control

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 include real-time microprocessors and configurable logic devices to perform data acquisition, data communications, and system logic processing. These components also contain on-line self-diagnostic features and off-line test capability to aid in maintenance and surveillance. For microprocessor based systems (ESF Logic and Control), the operating programs for the controllers are integrated into the hardware in nonvolatile memory that cannot be modified with the system online. For configurable logic devices (RTIS and NMS), the functions are incorporated into the logic configuration. Adjustment of selected parameters is permitted under proper change control. Adjustable parameters are stored in memory that can only be altered through the use of special equipment and/or procedures.

A. Safety System Logic and Control

Design Description

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 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 safety-related portions of the Neutron Monitoring System (NMS), the Containment Atmospheric Monitoring System (CAMS) and 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 (ELCS) and/or configurable logic devices (RTIS and NMS) that perform signal conditioning, setpoint comparison, trip logic, system initiation and reset, self-test, and bypass functions. 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. 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. 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. Trip decisions and other primary control logic functions are performed in SSLC processors in the Control Building.

The basic 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 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) Sensor inputs are acquired, conditioned, and digitized.
- (2) 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) 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 processes 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 deenergization of both pilot valve solenoids.

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

- (4) The trip coincident logic output from the TLF is sent to Output Logic Units (OLUs). The OLU's use devices that provide a diverse 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) TLF output bypass

The OLU's 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 TLF output bypass (division-out-of-service bypass). Bypass inhibits automatic trip but has no effect on manual trip. The OLU's 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 OLU's are located external to the equipment that implements the TLF so that manual MSIV closure or manual reactor trip (per division) can be performed either when a division's logic is bypassed or when failure of sensors or 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 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.

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

- (1) 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) As described above, the ELCS contains four redundant divisions of DTFs. The four divisions of DTF safety function actuation status are communicated to three divisions of SLFs, which correspond to the three divisions of ESF actuated equipment. No ESF actuated equipment exists in Division IV. The final SLF actuation outputs are distributed to the final system actuated equipment through the RDLC remote I/O devices.

RTIS and ELCS equipment is powered from their respective divisional Class 1E power sources. For RTIS, the equipment implementing the DTF, TLF, and OLU for RPS and MSIV in each of the four instrumentation divisions is powered from their respective divisional Class 1E AC sources. For ELCS, the equipment implementing the DTF and SLF for ESF in Divisions I, II and III is powered from their respective divisional Class 1E DC sources, as is the equipment implementing the ESF DTF in Division IV. Independence is provided between Class 1E divisions, and also between Class 1E divisions and non-Class 1E equipment.

For both RTIS and ELCS, bypassing of any single division of sensors (i.e., those sensors whose status is part of a 2-out-of-4 logic) can be accomplished by means of the manually-operated bypass. 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.

Bypassing a division of trip logic (i.e., taking a logic channel out of service) can also be accomplished by means of the bypass interlock function. This type of bypass is applied to the fail-safe reactor trip and MSIV closure functions (i.e. RTIS).

When a trip logic output bypass is in effect, the 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 status is indicated in the main control room until the bypass condition is removed. An interlock rejects attempts to remove more than one division from service at a time.

In the ELCS, the two redundant SLF processing channels must agree for initiation of the ESF safety function to occur. Two SLF processing channels are used to prevent the inadvertent system level actuation of the ESF safety functions that inject coolant to the core or depressurize the reactor vessel.

However, in the event of a failure detected by self diagnostics within either processing channel, a bypass (ESF output channel bypass (with manual backup)) is provided such that the failed SLF processing channel is removed from service. The remaining SLF processing channel provides one-out-of-one operation to maintain availability during the repair period. SLF processing failures are alarmed in the main control room. If a failed channel is not automatically bypassed, the operator can manually bypass the failed channel.

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 maintenance and test functions.

Inspections, Tests, Analyses and Acceptance Criteria

Table 3.4, Items 1 through 6, provides a definition of the inspections, tests and analyses, together with associated acceptance criteria, which will be undertaken for SSLC.

B. I & C Development and Qualification Processes

Hardware and Software Development Process

The ABWR design uses programmable digital equipment and configurable logic devices to implement operating functions of instrumentation and control (I&C) systems. The ELCS system uses non-volatile memory.

A quality assurance program encompassing software is employed as a controlled process for software development, hardware integration, and final product and system testing. The development process for safety-related hardware and software includes a verification and validation (V&V) program. Non-safety-related hardware and software will be developed using a planned design process similar to the safety-related development program, but with periodic design reviews rather than formal V&V.

System functional performance testing for each system using the software-based controllers discussed herein is addressed in Section 2 system entries.

An overall software development plan establishes the requirements and methodology for software design and development. The plan also defines methods for auditing and testing software during the design, implementation, and integration phases. These phases are part of the software life cycle, a planned development method to ensure the quality of software throughout its period of usage. The relationship between components of the plan and I&C design activities is shown in Figure 3.4d.

As part of the design of software for safety-related applications, the software development plan, at each defined phase of the software life cycle, addresses software requirements that have been defined as safety-critical. Safety-critical is defined as those computer software components

(processes, functions, values or computer program states) in which errors (inadvertent or unauthorized occurrence, failure to occur when required, occurrence out of sequence, occurrence in combination with other functions, or erroneous values) can result in a potential hazard or loss of predictability or control of a system. Potential hazards are failure of a safety-related function to occur on demand and spurious occurrence of a safety-related function in an unsafe direction.

The overall software development plan comprises the following plans:

- (1) A Software Management Plan (SMP) that establishes standards, conventions and design processes for I&C software.

A SMP shall be instituted which establishes that software for embedded control hardware shall be developed, designed, evaluated, and documented per a design development process that addresses, for safety-related software, software safety issues at each defined life-cycle phase of the software development.

The SMP defines the following software life-cycle phases:

- (a) Planning
- (b) Design definition
- (c) Software design
- (d) Software coding
- (e) Integration
- (f) Validation
- (g) Change control

The SMP shall state that the output of each defined life-cycle phase shall be documents that define the current state of that design phase and the design input for the next design phase and the software products are developed using the SMP.

- (2) A Configuration Management Plan (CMP) that establishes the standards and procedures controlling software design and documentation.

A CMP shall be instituted that establishes the methods for maintaining, throughout the software design process, the design documentation, procedures, evaluated software, and the resultant as-installed software.

The CMP addresses:

- (a) Identification of CMP software documentation.
 - (b) Management of software change control.
 - (c) Control and traceability of software changes.
 - (d) Verification of software to design requirements.
 - (e) Dedication of commercial software.
- (3) A V&V plan that establishes verification reviews and validation testing procedures.

A V&V plan shall be developed which establishes that developed software shall be subjected to structured and documented verification reviews and validation testing, including testing of the software integrated into the target hardware.

The V&V plan addresses:

- (a) Independent design verification.
- (b) Baseline software reviews.
- (c) Testing.
- (d) Procedure for software revisions.

Electromagnetic Compatibility

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

Electrical and electronic components in the systems 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 Communication Functions (ECF).
- (3) Non-Essential Communication Functions (NECF).
- (4) Other microprocessor-based, software controlled systems or equipment.

The plan is structured on the basis that EMC of I&C equipment is verified by factory testing and site testing of both individual components and interconnected systems to meet electromagnetic compatibility requirements for protection against the effects of:

- (1) Electromagnetic Interference (EMI).
- (2) Radio Frequency Interference (RFI).
- (3) Electrostatic Discharge (ESD).
- (4) Electrical surge [Surge Withstand Capability (SWC)].

To be able to predict the degree of electromagnetic compatibility of a given equipment design, the following information is developed:

- (1) Characteristics of the sources of electrical noise.
- (2) Means of transmission of electrical noise.
- (3) Characteristics of the susceptibility of the system.
- (4) Techniques to attenuate electrical noise.

After these characteristics of the equipment are identified, noise susceptibility is tested for four different paths of electrical noise entry:

- (1) Power feed lines.
- (2) Input signal lines.
- (3) Output signal lines.
- (4) Radiated electromagnetic energy.

Instrument Setpoint Methodology

Setpoints for initiation of safety-related functions are determined, documented, installed and maintained using a process that establishes a general program for:

- (1) Specifying requirements for documenting the bases for selection of trip setpoints.
- (2) Accounting for instrument inaccuracies, uncertainties, and drift.
- (3) Testing of instrumentation setpoint dynamic response.
- (4) Replacement of setpoint-related instrumentation.

The determination of nominal trip setpoints includes consideration of the following factors:

Design Basis Analytical Limit

In the case of setpoints that are directly associated with an abnormal plant transient or accident analyzed in the safety analysis, a design basis analytical limit is established as part of the safety analysis. The design basis analytical limit is the value of the sensed process variable prior to or at the point which a desired action is to be initiated. This limit is set so that associated licensing safety limits are not exceeded, as confirmed by plant design basis performance analysis.

Allowable Value

An allowable value is determined from the analytical limit by providing allowances for the specified or expected calibration capability, the accuracy of the instrumentation, and the measurement errors. The allowable value is the limiting value of the sensed process variable at which the trip setpoint may be found during instrument surveillance.

Nominal Trip Setpoint

The nominal trip setpoint value is calculated from the analytical limit by taking into account instrument drift in addition to the instrument accuracy, calibration capability, and the measurement errors. The nominal trip setpoint value is the limiting value of the sensed process variable at which a trip action will be set to operate at the time of calibration.

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 signal provided by the sensor (e.g., analog-to-digital converters, signal conditioners, and temperature compensation circuits). 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.

Not all parameters have an associated design basis analytical limit (e.g., main steamline radiation monitoring). An allowable value may be defined directly based on plant licensing requirements, previous operating experience or other appropriate criteria. The nominal trip setpoint is then calculated from this allowable value, allowing for instrument drift. Where appropriate, a nominal trip setpoint may be determined directly based on operating experience.

Procedures will be used that provide a method for establishing instrument nominal trip setpoint and allowable value. Because of the general characteristics of the instrumentation and processes involved, two different methods are applied:

- (1) Computational
- (2) Historical data

The computational method is used when sufficient information is available regarding a dynamic process and the associated instrumentation. The procedure takes into account channel instrument accuracy, calibration accuracy, process measurement accuracy, primary element accuracy, and instrument drift. If the resulting nominal trip setpoint and allowable value are not acceptable when checked to ensure that they will not result in an unacceptable level of trips caused by normal operational transients, then more rigorous statistical evaluation or the use of actual operational data may be considered.

Some setpoint values have been historically established as acceptable, both for regulatory and operational requirements. These setpoints have non-critical functions or are intended to provide trip actions related to gross changes in the process variable. The continued recommendation of these historically accepted setpoint values is another method for establishing nominal trip setpoint and allowable values. This approach is only valid where the governing conditions remain essentially unaltered from those imposed previously and where the historical values have been adequate for their intended functions.

The setpoint methodology plan requires that activities related to instrument setpoints be documented and stored in retrievable, auditable files.

Equipment Qualification (EQ)

Qualification of safety-related instrumentation and control equipment is implemented by a program that assures this equipment is able to complete its safety-related function under the environmental conditions that exist up to and including the time the equipment has finished performing that function. Qualification specifications consider conditions that exist during normal, abnormal, and design basis accident events in terms of their cumulative effect on equipment performance for the time period up to the end of equipment life.

The material discussed herein identifies an EQ program that addresses the spectrum of design basis environmental conditions that may occur in plant areas where I&C equipment is installed. Not all safety-related I&C equipment will experience all of these conditions; the intent is that qualification be performed by selecting the conditions applicable to each particular piece of equipment and performing the necessary qualification.

As-built I&C components are environmentally qualified if they can withstand the environmental conditions associated with design basis events without loss of their safety functions for the time needed to be functional. Safety-related I&C components are designed to continue normal operation after loss of HVAC. The environmental conditions are as follows, as applicable to the bounding design basis events: Expected time-dependent temperature and pressure profiles, humidity, chemical effects, radiation, aging, seismic events, submergence, and synergistic effects which have a significant effect on equipment performance.

I&C equipment environmental qualification is demonstrated through analysis of the environmental conditions that would exist in the location of the equipment during and following a design basis accident and through a determination that the equipment is qualified

to withstand those conditions for the time needed is functional. This determination may be demonstrated by:

- (1) Type testing of an identical item of equipment under identical or similar conditions with a supporting analysis to show that the equipment to be qualified.
- (2) Type testing of a similar item of equipment with a supporting analysis to show that the equipment is qualified.
- (3) Experience with identical or similar equipment under similar conditions with a supporting analysis to show that the equipment is qualified.
- (4) Analysis in combination with partial type test data that supports the analytical assumptions and conclusions to show that the equipment is qualified.

The installed condition of safety-related I&C equipment is assured by a program whose objective is to verify that the installed configuration is bounded by the test configuration and test conditions.

Inspections, Tests, Analyses and Acceptance Criteria

Table 3.4, Items 7 through 15, provides a definition of the inspections, tests and analyses, together with associated acceptance criteria, which will be used to demonstrate compliance with the above commitments for hardware and software development, electromagnetic compatibility, instrument setpoint methodology, and equipment qualification.

C. 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.
- Availability of manual high pressure injection capability.

- Long term shutdown capability provided in a conventionally hardwired, 2-division, 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.

Thus, to maintain protection system defense-in-depth in the presence of a postulated worst-case event (i.e., undetected, 4-division common mode failure of protection system communications or logic processing functions in conjunction with a large break LOCA), diversity is provided in the form of hardwired backup of reactor trip, diverse display of important process parameters, defense-in-depth arrangement of equipment, and other equipment diversity as outlined in the following table:

Diverse Backup Support for SSLC Equipment

| Diverse Features of Protection System | Functional Diversity in Protection System | Defense-in-Depth Configuration | Equipment Diversity |
|--|--|---------------------------------------|----------------------------|
| (1) 2-button scram | H | | |
| (2) Manual division trip | H | | |
| (3) Reactor mode switch placed in shutdown mode. | H | | |
| (4) Manual MSIV closure | H | | |
| (5) ATWS mitigation | D | | |
| (6) Fail-safe RPS and fail-as-is ESF in separate processing channels | | D | |
| (7) Communication Functions (NECF) independent and diverse from ECF | | D | |
| (8) OLUs diverse from software-based logic | | | H |

Diverse Backup Support for SSLC Equipment (Continued)

| Diverse Features of Protection System | Functional Diversity in Protection System | Defense-in-Depth Configuration | Equipment Diversity |
|---|---|--------------------------------|---------------------|
| (9) <u>Independent Displays</u> | | | H |
| (a) Reactor water level | | | |
| (b) Reactor water level low alarm | | | |
| (c) Drywell pressure | | | |
| (d) Drywell pressure high alarm | | | |
| (e) Reactor Water Cleanup System (CUW) isolation valve status | | | |
| (f) RCIC stream line isolation valve status | | | |
| (g) HPCF flow | | | |
| (10) <u>Containment Isolation</u> | | | H |
| (a) CUW line inboard isolation valve | | | |
| (b) RCIC steam line inboard isolation valve manual initiation | | | |

Diverse Backup Support for SSLC Equipment (Continued)

| Diverse Features of Protection System | Functional Diversity in Protection System | Defense-in-Depth Configuration | Equipment Diversity |
|---|---|--------------------------------|---------------------|
| (11)HPCF manual start in loop C (Division III) | | | H |
| (12)RSS with continuous display of monitored process parameters | | | H |

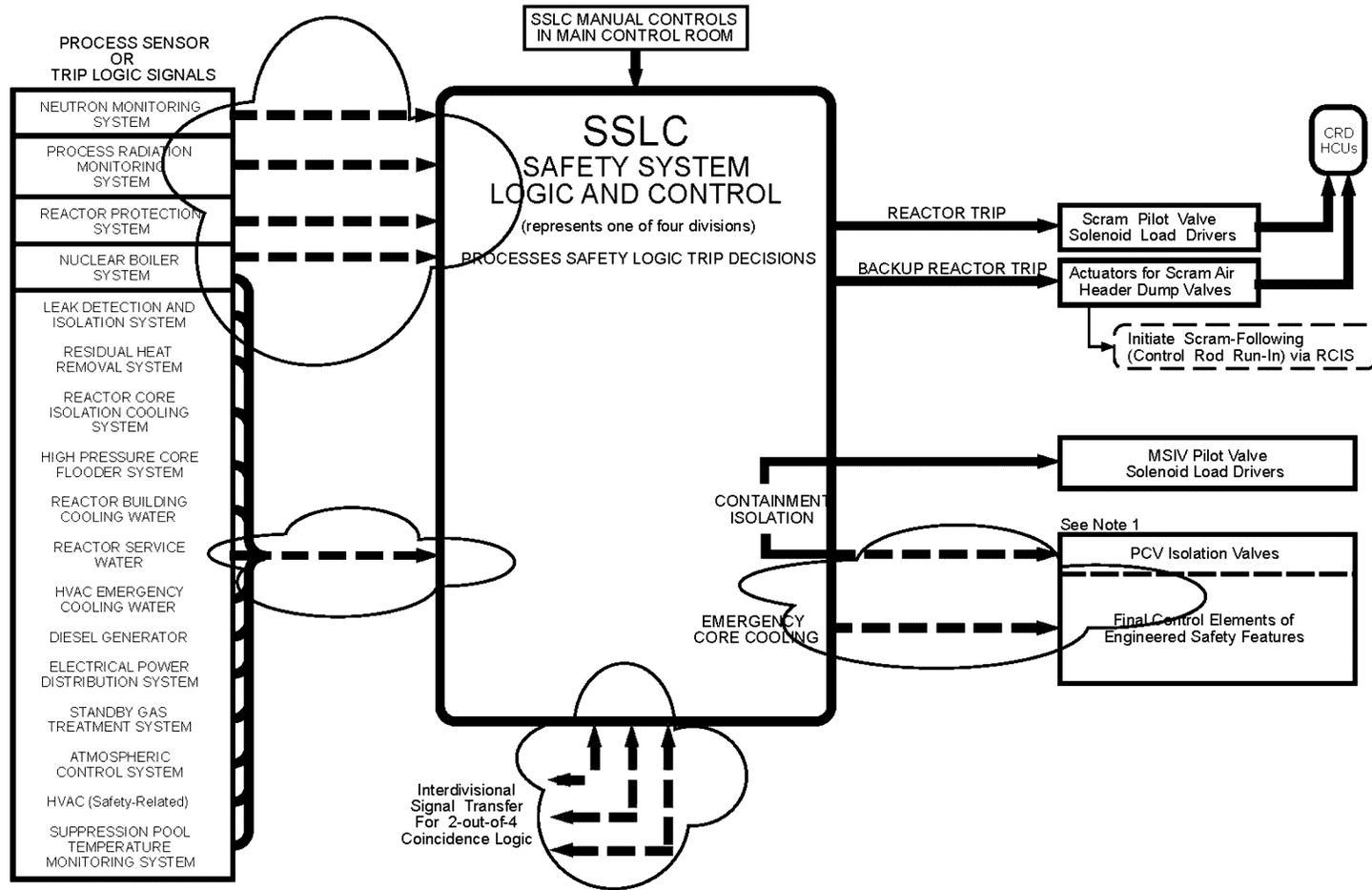
H = Function hardwired from sensor or control switch to actuator; control logic, if needed, is diverse from that of the primary protection system.

D =Function uses logic diverse from primary protection system but is not necessarily hardwired.

Diverse equipment can be in the form of digital devices, digital software-based devices, or non-digital as long as these devices are not subject to the same common mode failure as the primary protection system components.

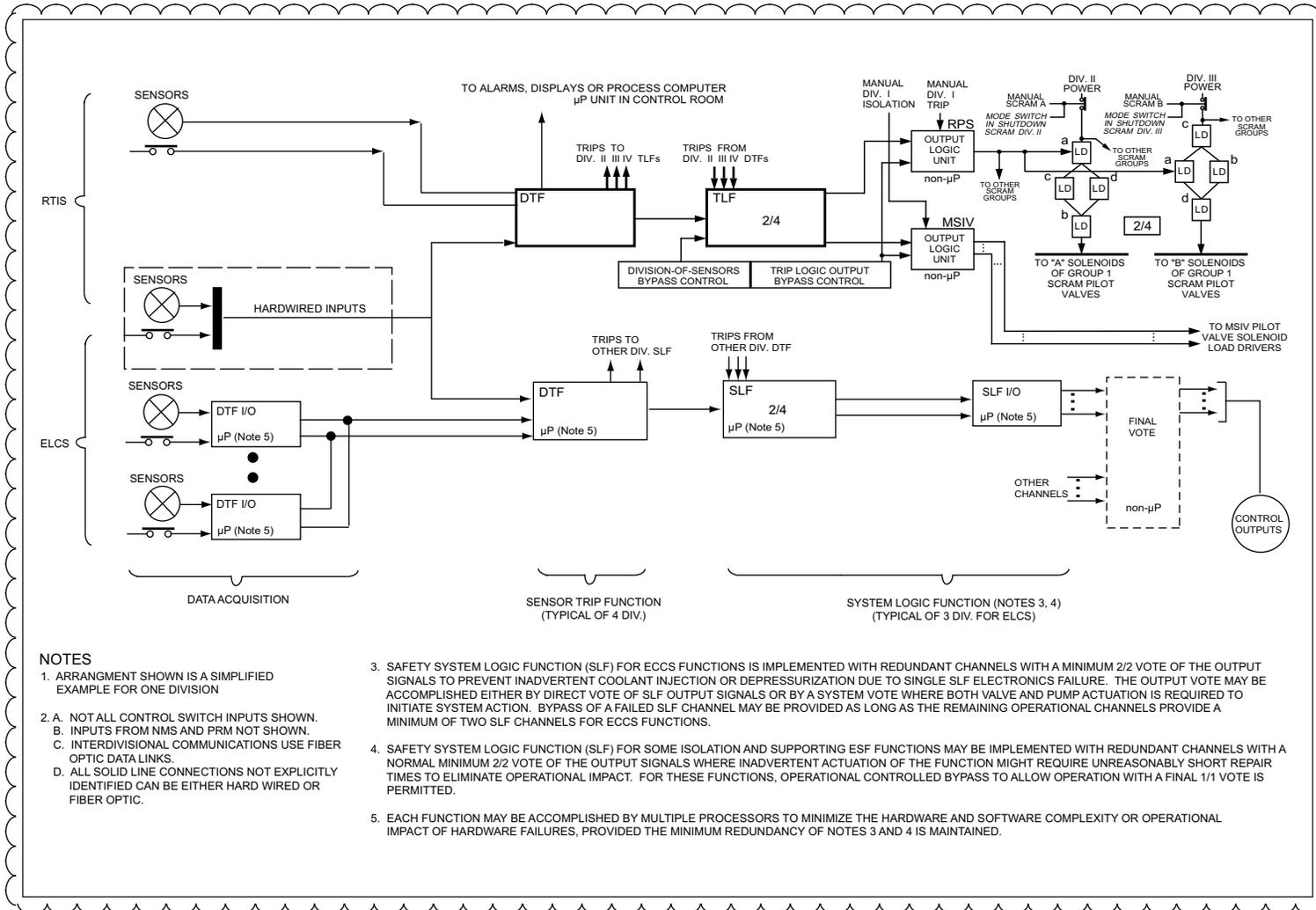
Inspections, Tests, Analyses and Acceptance Criteria

Table 3.4, Item 16, provides a definition of the inspection, tests and analyses, together with associated acceptance criteria, which will be used to demonstrate compliance with the above commitments for diverse backup support SSLC.



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

- ARRANGEMENT SHOWN IS A SIMPLIFIED EXAMPLE FOR ONE DIVISION
- NOT ALL CONTROL SWITCH INPUTS SHOWN.
 - INPUTS FROM NMS AND PRM NOT SHOWN.
 - INTERDIVISIONAL COMMUNICATIONS USE FIBER OPTIC DATA LINKS.
 - ALL SOLID LINE CONNECTIONS NOT EXPLICITLY IDENTIFIED CAN BE EITHER HARD WIRED OR FIBER OPTIC.
- SAFETY 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.
- SAFETY 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, OPERATIONAL CONTROLLED BYPASS TO ALLOW OPERATION WITH A FINAL 1/1 VOTE IS PERMITTED.
- 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

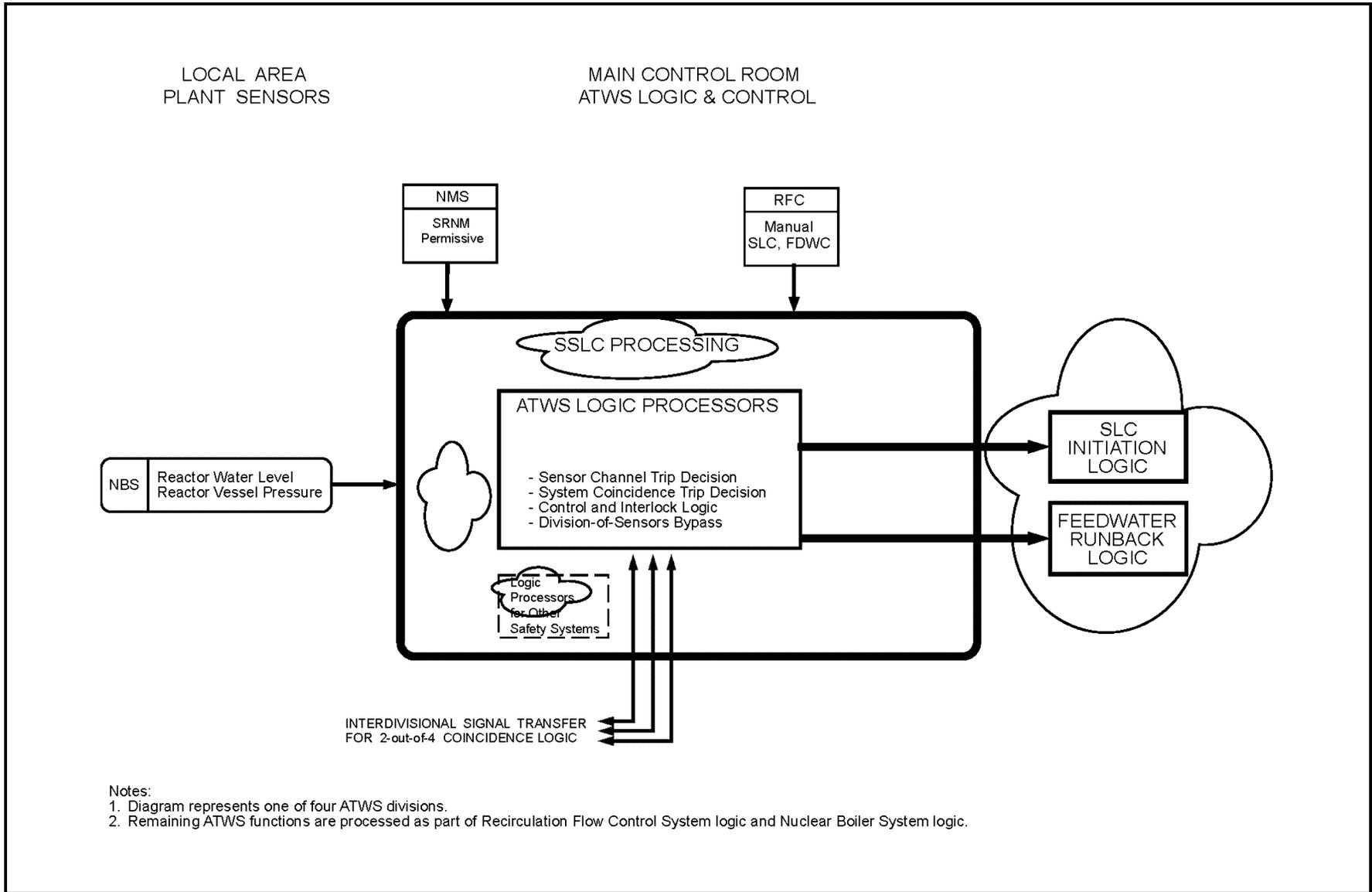


Figure 3.4c Anticipated Transient Without Scram (ATWS) Control Interface Diagram

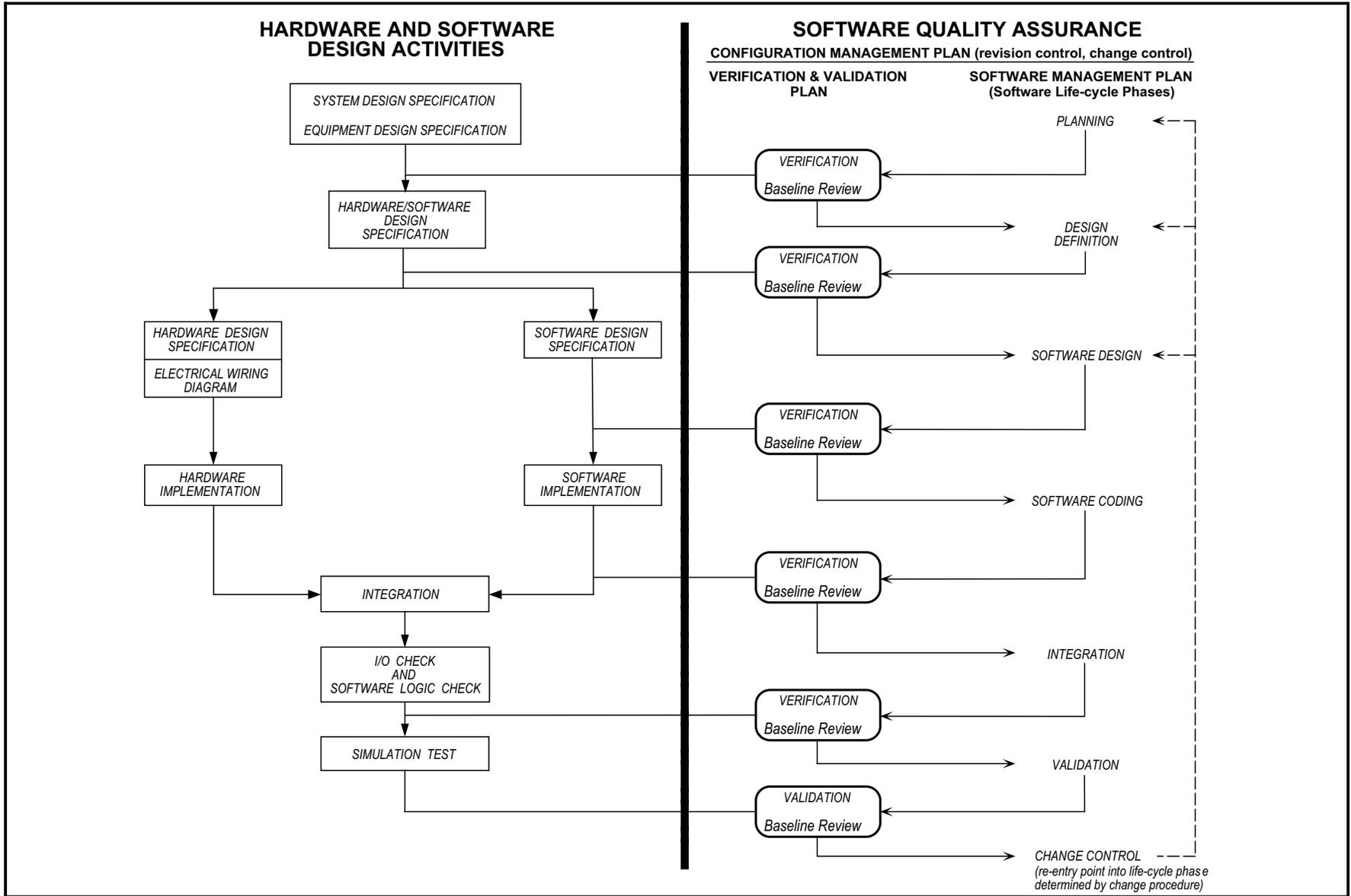


Figure 3.4d Integrated Hardware/Software Development Process

Table 3.4 Instrumentation and Control

| Inspections, Tests, Analyses and Acceptance Criteria | | |
|---|---|--|
| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
| <i>Safety System Logic and Control</i> | | |
| 1. The equipment comprising SSLC is defined in Section 3.4(A). The equipment comprising diverse backup support functions for SSLC is defined in Section 3.4 (C). | 1. Inspections of the as-built SSLC will be conducted. | 1. The as-built SSLC conforms with the description in Section 3.4(A). Diverse backup support equipment for SSLC conforms with the description in Section 3.4 (C). |
| 2. 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. SSLC generates the protective function signals that activate reactor trip and provide safety-related mitigation of reactor accidents. | 2. Tests will be performed on as-installed SSLC using simulated input signals. System outputs will be monitored to determine operability of safety-related functions. | 2. A test report exists which concludes that the SSLC design basis performance requirements are met. |
| 3. The 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 equipment implementing the DTF and SLF for ESF in Divisions I, II, and III are powered from their respective divisional Class 1E DC sources, as is the equipment implementing the ESF DTF in Division IV. In SSLC, independence is provided between Class 1E divisions and between Class 1E divisions and non-Class 1E equipment. | 3. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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. |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--|--|--|
| <i>Safety System Logic and Control</i> | | |
| <p>4. SSLC provides the following bypass functions:</p> <ul style="list-style-type: none"> a. Division-of-sensors bypass b. Trip logic output bypass c. ESF output channel bypass where applied | <p>4. Tests will be performed on the as-built SSLC as follows:</p> <ul style="list-style-type: none"> 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 from each 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. 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. | <p>4. Results of bypass tests are as follows:</p> <ul style="list-style-type: none"> a(1) No trip change occurs at the voted trip output from each 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. 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. |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--|---|---|
| <i>Safety System Logic and Control</i> | | |
| <p>4. (continued)</p> | <p>4. (continued)</p> <p>b(2) For each division in bypass, attempt to place the other divisions in trip-logic-output bypass, one at a time.</p> <p>c(1) Apply common test signal to any one pair of redundant SLF signal inputs. Monitor test signal at output from equipment performing the ECF in local areas. Remove power from equipment performing one SLF, restore power, then remove power from equipment performing other SLF. Repeat test for all pairs of redundant sets of equipment implementing an SLF in each division.</p> <p>c(2) Disable auto-bypass circuit in bypass unit. Repeat test c(1), but operate manual ESF loop bypass switch for each affected loop.</p> | <p>4. (continued)</p> <p>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.</p> <p>c(1) Monitored test output signal does not initiate the system function when power is removed from the equipment performing any single SLF. Bypass status and loss of power to equipment performing the SLF are indicated in main control room.</p> <p>c(2) Monitored test output signal is lost when power is removed from either SLF, but is restored when manual bypass switch is operated. Bypass status, auto-bypass inoperable, and loss of power to SLF are indicated in main control room.</p> |

Table 3.4 Instrumentation and Control (Continued)

| Inspections, Tests, Analyses and Acceptance Criteria | | |
|--|--|--|
| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
| <i>Safety System Logic and Control</i> | | |
| <p>5. A portion of the anticipated transient without scram (ATWS) mitigation features is provided by SSLC circuitry, with initiating conditions as follows:</p> <p>a. Initiation of automatic SLCS injection on high dome pressure and SRNM ATWS permissive for 3 minutes or greater, or low reactor water level and SRNM ATWS permissive for 3 minutes or greater.</p> <p>b. Initiation of feedwater runback on high dome pressure and SRNM ATWS permissive for 2 minutes or greater. Reset is permitted only when both signals drop below the setpoints.</p> | <p>5. Tests will be conducted using simulated input signals for the process variables used by the ATWS logic.</p> <p>For feedwater runback logic, reset attempts will be made before initiating test signals drop below setpoints.</p> | <p>5. Four redundant output signals occur for each of the following ATWS mitigating functions (one set in each of the four divisions of ATWS outputs) that lead to initiation of these functions:</p> <p>a. Initiation of automatic SLCS injection on high dome pressure and SRNM ATWS permissive for 3 minutes or greater, or low reactor water level and SRNM ATWS permissive for 3 minutes or greater.</p> <p>b. Initiation of feedwater runback on high dome pressure and SRNM ATWS permissive for 2 minutes or greater. Reset is permitted only when both signals drop below the setpoints.</p> |
| <p>6. Main control room alarms, displays and controls provided for SSLC are as defined in Section 3.4.</p> | <p>6. Inspections will be performed on the main control room alarms, displays and controls for SSLC</p> | <p>6. Alarms, displays and controls exist or can be retrieved in the main control room as defined in Section 3.4.</p> |

Table 3.4 Instrumentation and Control (Continued)

| Inspections, Tests, Analyses and Acceptance Criteria | | |
|--|--|---|
| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
| <i>Hardware/Software Development</i> | | |
| <p>7. A quality assurance program encompassing software is employed as a controlled process for software development hardware integration, and final product and system testing.</p> <p>8. A Software Management Plan (SMP) shall be instituted which establishes that software for embedded control hardware shall be developed, designed, evaluated, and documented per a design development process that addresses, for safety-related software, software safety issues at each defined life-cycle phase of the software development.</p> <p>The SMP shall state that the output of each defined life-cycle phase shall be documents that define the current state of that design phase and the design input for the next design phase.</p> | <p>7. The program for quality assurance that encompasses software shall be reviewed.</p> <p>8. The Software Management Plan shall be reviewed.</p> | <p>7. A quality assurance program is in place that defines controlled processes for software development, hardware integration, and final product and system testing. As a minimum, the program requires a Software Management Plan, Configuration Management Plan and Verification and Validation Plan as described in the following items.</p> <p>8. The Software Management Plan shall define:</p> <ol style="list-style-type: none"> a. The organization and responsibilities for development of the software design; the procedures to be used in the software development; the interrelationships between software design activities; and the methods for conducting software safety analyses. b. That the software safety analyses to be conducted for safety-related software applications shall: <ol style="list-style-type: none"> (1) Identify software requirements having safety-related implications. (2) Document the identified safety-critical software requirements in the software requirements specification for the design. |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--------------------------------------|------------------------------|---|
| <i>Hardware/Software Development</i> | | |
| 8. (continued) | 8. (continued) | 8b. (continued) <ul style="list-style-type: none"> <li data-bbox="1423 440 1892 561">(3) Incorporate into the software design the safety-critical software functions specified in the software requirements specification. <li data-bbox="1423 578 1892 667">(4) Identify in the coding and test of the developed software, those software modules which are safety-critical. <li data-bbox="1423 683 1892 935">(5) Evaluate the performance of the developed safety-critical software modules when operated within the constraints (including the effects of potential unintended functions) imposed by the established system requirements, software design, and computer hardware requirements. <li data-bbox="1423 951 1892 1016">(6) Evaluate software interfaces of safety-critical software modules. <li data-bbox="1423 1032 1892 1187">(7) Perform equipment integration and validation testing that demonstrate that safety-related functions identified in the design input requirements are operational. |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--------------------------------------|------------------------------|--|
| <i>Hardware/Software Development</i> | | |
| 8. (continued) | 8. (continued) | 8. (continued) <ul style="list-style-type: none"> c. The software engineering process, which is composed of the following life-cycle phases: <ul style="list-style-type: none"> (1) Planning (2) Design Definition (3) Software Design (4) Software Coding (5) Integration (6) Validation (7) Change control d. The Planning phase design activities, which shall address the following system design requirements and software development plans: <ul style="list-style-type: none"> (1) Software Management Plan. (2) Software Configuration Management Plan. (3) Verification and Validation Plan. (4) Equipment design requirements. (5) Safety analysis of design requirements. (6) Disposition of design and/or documentation nonconformances identified during this phase. |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--------------------------------------|------------------------------|---|
| <i>Hardware/Software Development</i> | | |
| 8. (continued) | 8. (continued) | 8. (continued) <ul style="list-style-type: none"> e. The Design Definition phase design activities, which shall address the development of the following implementing equipment design and configuration requirements: <ul style="list-style-type: none"> (1) Equipment schematic. (2) Equipment hardware and software performance specification. (3) Equipment user's manual. (4) Data communications protocol, including timing analysis and test methods. (5) Safety analysis of the developed design definition. (6) Disposition of design and/or documentation nonconformances identified during this phase. |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--------------------------------------|-------------------------------------|--|
| <i>Hardware/Software Development</i> | | |
| <p>8. (continued)</p> | <p>8. (continued)</p> | <p>8. (continued)</p> <ul style="list-style-type: none"> f. The Software Design phase, which shall address the design of the software architecture and program structure elements, and the definition of software module functions: <ul style="list-style-type: none"> (1) Software Design Specification. (2) Safety analysis of the software design. (3) Disposition of design and/or documentation nonconformances identified during this phase. g. The Software Coding phase, which shall address the following software coding and testing activities of individual software modules: <ul style="list-style-type: none"> (1) Software source code. (2) Software module test reports. (3) Safety analysis of the software coding. (4) Disposition of nonconformances identified in this phase's design documentation and test results. |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--------------------------------------|------------------------------|--|
| <i>Hardware/Software Development</i> | | |
| 8. (continued) | 8. (continued) | 8. (continued) <ul style="list-style-type: none"> <li data-bbox="1373 423 1902 841">h. The Integration phase, which shall address the following equipment testing activities that evaluate the performance of the software when installed in hardware prototypical of that defined in the Design Definition phase: <ul style="list-style-type: none"> <li data-bbox="1423 630 1745 654">(1) Integration test reports. <li data-bbox="1423 675 1902 732">(2) Safety analysis of the integration test results. <li data-bbox="1423 753 1850 841">(3) Disposition of nonconformances identified in this phase's design documentation and test results. <li data-bbox="1373 862 1902 1338">i. The Validation phase, which comprises the development and implementation of the following documented test plans and procedures: <ul style="list-style-type: none"> <li data-bbox="1423 1000 1759 1057">(1) Validation test plans and procedures. <li data-bbox="1423 1078 1734 1102">(2) Validation test reports. <li data-bbox="1423 1123 1864 1148">(3) Description of as-tested software. <li data-bbox="1423 1169 1902 1226">(4) Safety analysis of the validation test results. <li data-bbox="1423 1247 1850 1338">(5) Disposition of nonconformances identified in this phase's design documentation and test results |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--|--|--|
| <i>Hardware/Software Development</i> | | |
| <p>8. (continued)</p> <p>9. A Configuration Management Plan (CMP) shall be instituted that establishes the methods for maintaining, throughout the software design process, the design documentation, procedures, evaluated software, and the resultant as-installed software.</p> | <p>8. (continued)</p> <p>9. The Configuration Management Plan shall be reviewed.</p> | <p>8i. (continued)</p> <p>(6) Software change control procedures.</p> <p>j. The Change Control phase, which begins with the completion of validation testing, and addresses changes to previously validated software and the implementation of the established software change control procedures.</p> <p>9. The Configuration Management Plan shall define:</p> <p>a. The specific product or system scope to which it is applicable.</p> <p>b. The organizational responsibilities for software configuration management.</p> <p>c. Methods to be applied to:</p> <p>(1) Identify design interfaces.</p> <p>(2) Produce software design documentation.</p> <p>(3) Process changes to design interface documentation and software design documentation.</p> |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--------------------------------------|------------------------------|---|
| <i>Hardware/Software Development</i> | | |
| 9. (continued) | 9. (continued) | 9c. (continued) <ul style="list-style-type: none"> (4) Process corrective actions to resolve deviations identified in software design and design documentation, including notification to end user of errors discovered in software development tools or other software. (5) Maintain status of design interface documentation and developed software design documentation. (6) Designate and control software revision status. Such methods shall require that software code listings present direct indication of the software code revision status. d. Methods for, and the sequencing of, reviews to evaluate the compliance of software design activities with the requirements of the CMP. e. The configuration management of tools (such as compilers) and software development procedures. f. Methods for the dedication of commercial software for safety-related usage. |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|--|--|
| <i>Hardware/Software Development</i> | | |
| <p>9. (continued)</p> <p>10. A Verification and Validation Plan (V&VP) shall be developed which establishes that developed software shall be subjected to structured and documented verification reviews and validation testing, including testing of the software integrated into the target hardware.</p> | <p>9. (continued)</p> <p>10. The Verification and Validation Plan shall be reviewed.</p> | <p>9. (continued)</p> <ul style="list-style-type: none"> g. Methods for tracking error rates during software development, such as the use of software metrics. h. The methods for design record collection and retention. <p>10. The Verification and Validation Plan shall define:</p> <ul style="list-style-type: none"> a. That baseline reviews of the software development process are to be conducted during each phase of the software development life cycle. b. The scope and methods to be used in the baseline reviews to evaluate the implemented design, design documentation, and compliance with the requirements of the Software Management Plan and Configuration Management Plan. c. The requirements for use of commercial software and commercial development tools for safety-related applications and that such use is a controlled and documented procedure. |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--------------------------------------|------------------------------|---|
| <i>Hardware/Software Development</i> | | |
| 10. (continued) | 10. (continued) | 10. (continued) <ul style="list-style-type: none"> d. That verification shall be performed as a controlled and documented evaluation of the conformity of the developed design to the documented design requirements at each phase of baseline review. e. That validation shall be performed through controlled and documented testing of the developed software as installed in the target hardware that demonstrates compliance of the software with the software requirements specifications and compliance of the device(s) under test with the system design specifications. f. That for safety-related software, verification reviews and validation testing are to be conducted by personnel who are knowledgeable in the technologies and methods used in the design, but who did not develop the software design to be reviewed and tested. |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--------------------------------------|------------------------------|---|
| <i>Hardware/Software Development</i> | | |
| 10. (continued) | 10. (continued) | 10. (continued) <ul style="list-style-type: none"> <li data-bbox="1373 456 1902 805">g. That for safety-related software, design verification reviews shall be conducted as part of the baseline reviews of the design material developed during the Planning through Integration phases of the software development life-cycle (as defined in Criterion 8b, above), and that validation testing shall be conducted as part of the baseline review of the Validation phase of the software development life-cycle. <li data-bbox="1373 821 1902 911">h. That validation testing shall be conducted per a documented test plan and procedure. <li data-bbox="1373 927 1902 1243">i. That for non-safety-related software development, verification and validation shall be performed through design reviews conducted as part of the baseline reviews completed at the end of the phases in the software development life cycle. These design reviews shall be performed by personnel knowledgeable in the technologies and methods used in the design development. |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--|--|--|
| <i>Electromagnetic Compatibility</i> | | |
| <p>12. Electrical and electronic components in the systems listed below are qualified for the anticipated levels of electrical interference at the installed locations of the components according to an established plan:</p> <ol style="list-style-type: none"> a. Safety System Logic and Control b. Equipment performing the Essential Communication Function (ECF) c. Equipment performing the Non Essential Communication Function (NECF) d. Other microprocessor-based, software controlled systems or equipment <p>The plan is structured on the basis that electromagnetic compatibility (EMC) of I&C equipment is verified by factory testing and site testing of both individual components and interconnected systems to meet EMC requirements for protection against the effects of:</p> <ol style="list-style-type: none"> a. Electromagnetic Interference (EMI) b. Radio Frequency Interference (RFI) c. Electrostatic Discharge (ESD) d. Electrical surge [Surge Withstand Capability (SWC)] | <p>12. The EMC compliance plan will be reviewed.</p> | <p>12. An EMC compliance plan is in place. The plan requires, for each system qualified, system documentation that includes confirmation of component and system testing for the effects of high electrical field conditions and current surges. As a minimum, the following information is documented in a qualification file and subject to audit:</p> <ol style="list-style-type: none"> a. Expected performance under test conditions for which normal system operation is to be ensured. b. Normal electrical field conditions at the locations where the equipment must perform as above. c. Testing methods used to qualify the equipment, including: <ol style="list-style-type: none"> (1) Types of test equipment. (2) Range of normal test conditions. (3) Range of abnormal test conditions for expected transient environment. |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--|--|--|
| <p data-bbox="260 342 613 370"><i>Electromagnetic Compatibility</i></p> <p data-bbox="149 394 327 422">12. (continued)</p> | <p data-bbox="741 394 919 422">12. (continued)</p> | <p data-bbox="1329 394 1507 422">12.(continued)</p> <p data-bbox="1423 428 1892 675">(4) Location of testing and exact configuration of tested components and systems, including interconnecting cables, connections to electrical power distribution system, and connections to interfacing devices used during normal plant operation.</p> <p data-bbox="1377 695 1892 846">d. Test results that show the component or system is qualified for its application and remains qualified after being subjected to the range of normal and abnormal test conditions specified above.</p> <p data-bbox="1377 865 1892 954">The plan establishes separate test regimes for each element of EMC, using the following approaches:</p> <p data-bbox="1377 974 1892 1284">a. EMI and RFI Protection. An EMC compliance plan for each component or system identified in the design commitment includes tests to ensure that equipment performs its functions in the presence of the specified EMI/RFI electrical noise environment, including the low range of the EMI spectrum, without equipment damage, spurious actuation, or inhibition of functions.</p> |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--|--|--|
| <p data-bbox="260 342 615 370"><i>Electromagnetic Compatibility</i></p> <p data-bbox="149 394 327 422">12. (continued)</p> | <p data-bbox="737 394 919 422">12. (continued)</p> | <p data-bbox="1331 394 1520 422">12a. (continued)</p> <p data-bbox="1423 428 1896 610">As part of the pre-operational test program, the EMC compliance plan calls for each system to be subjected to EMI/RFI testing. Tests cover potential EMI and RFI susceptibility over four different paths:</p> <ol data-bbox="1423 630 1692 792" style="list-style-type: none"> <li data-bbox="1423 630 1667 657">(1) Power feed lines <li data-bbox="1423 673 1671 701">(2) Input signal lines <li data-bbox="1423 717 1692 745">(3) Output signal lines <li data-bbox="1423 761 1583 789">(4) Radiation <p data-bbox="1423 808 1885 959">The test program includes sensitivity of components identified in the design commitment to radiation from plant communication transmitters and receivers.</p> <p data-bbox="1373 984 1896 1227">b. ESD Protection. An EMC compliance plan for each component or system identified in the design commitment includes tests to ensure that equipment performs its functions in the presence of the specified ESD environment without equipment damage, spurious actuation, or inhibition of functions.</p> |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--|--|---|
| <p data-bbox="262 341 619 365"><i>Electromagnetic Compatibility</i></p> <p data-bbox="151 389 325 414">12. (continued)</p> | <p data-bbox="739 389 913 414">12. (continued)</p> | <p data-bbox="1327 389 1522 414">12b. (continued)</p> <p data-bbox="1423 422 1894 576">The plan is structured on the basis that ESD protection is confirmed by factory tests that determine the susceptibility of instrumentation and control equipment to electrostatic discharges.</p> <p data-bbox="1423 592 1879 747">The EMC compliance plan includes standards, conventions, design considerations, and test procedures to ensure ESD protection of the plant instrumentation and control equipment.</p> <p data-bbox="1423 763 1858 885">The plan requires test documentation confirming that, for each component tested, the following conditions have been met:</p> <ul style="list-style-type: none"> <li data-bbox="1423 901 1858 966">(1) No change in output signal status was observed during the test. <li data-bbox="1423 982 1894 1039">(2) The equipment performed its normal functions after the test. |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|--|--|
| <p data-bbox="262 341 619 373"><i>Electromagnetic Compatibility</i></p> <p data-bbox="151 389 325 422">12.(continued)</p> | <p data-bbox="739 389 924 422">12. (continued)</p> | <p data-bbox="1375 389 1900 641">c. SWC Protection. An EMC compliance plan for each component or system identified in the design commitment includes tests to ensure that equipment performs its functions for the specified SWC environment without equipment damage, spurious actuation, or inhibition of functions.</p> <p data-bbox="1423 657 1900 820">The EMC compliance plan includes standards, conventions, design considerations, and test procedures to ensure SWC protection of the plant instrumentation and control equipment.</p> <p data-bbox="1423 836 1900 998">The plan is structured on the basis that SWC protection is confirmed by factory tests that determine the surge withstand capability of the plant instrumentation and control equipment.</p> <p data-bbox="1423 1015 1900 1161">The plan documents the level of compliance of each system with the grounding and shielding practices of the standards specified under this certified design commitment.</p> |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--|--|--|
| <i>Setpoint Methodology</i> | | |
| <p>13. Setpoints for initiation of safety-related functions are determined, documented, installed and maintained using a process that establishes a plan for:</p> <ul style="list-style-type: none"> 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. <p>The setpoint methodology plan requires that activities related to instrument setpoints be documented and stored in retrievable, auditable files.</p> | <p>13. Inspections will be performed of the setpoint methodology plan used to determine, document, install, and maintain instrument setpoints.</p> | <p>13. The setpoint methodology plan is in place. The plan generates requirements for:</p> <ul style="list-style-type: none"> 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), 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. |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|--|--|
| <i>Setpoint Methodology</i> | | |
| 13. (continued) | 13. (continued) | 13. (continued) |
| 14. Qualification of safety-related I&C equipment is implemented by a program that assures this equipment is able to complete its safety-related function under the environmental conditions that exist up to and including the time the equipment has finished performing that function. Qualification specifications consider conditions that exist during normal, abnormal, and design basis accident events in terms of their cumulative effect on equipment performance for the time period up to the end of equipment life. | 14. A review will be conducted of the equipment qualification program. | 13. (continued) <ul style="list-style-type: none"> e. Documented evaluation of replacement instrumentation which is not identical to the original equipment. 14. An I&C equipment qualification program is in place. Documentation for the I&C EQ program is recorded in a product qualification file that includes a list of safety-related I&C equipment accompanied by the following I&C equipment information: <ul style="list-style-type: none"> a. Performance specifications under conditions existing during and after design basis accidents. These include voltage, frequency, load, and other electrical characteristics that assure specified equipment performance. b. Environmental conditions at the location where the equipment is installed. These conditions include: <ul style="list-style-type: none"> (1) Number and /or duration of equipment functional and test cycles/events. (2) Process fluid conditions (where applicable to the I&C equipment) |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--|--|---|
| <p data-bbox="296 342 579 370"><i>Equipment Qualification</i></p> <p data-bbox="149 394 327 422">14. (continued)</p> | <p data-bbox="741 394 919 422">14. (continued)</p> | <p data-bbox="1331 394 1509 422">14. (continued)</p> <ul style="list-style-type: none"> <li data-bbox="1423 427 1881 516">(3) Voltage, frequency, load, and other electrical characteristics of the equipment. <li data-bbox="1423 532 1835 589">(4) Dynamic loads associated with seismic events. <li data-bbox="1423 605 1835 670">(5) Dynamic loads associated with hydrodynamic conditions. <li data-bbox="1423 686 1801 751">(6) System transients and other vibration inducing events. <li data-bbox="1423 768 1856 800">(7) Pressure, temperature, humidity. <li data-bbox="1423 816 1745 873">(8) Chemical and radiation environments. <li data-bbox="1423 889 1814 922">(9) Electromagnetic compatibility <li data-bbox="1423 938 1556 971">(10) Aging. <li data-bbox="1423 987 1738 1019">(11) Submergence (if any). <li data-bbox="1423 1036 1892 1117">(12) Consideration of synergistic effects that have significant effect on equipment performance. <li data-bbox="1423 1133 1814 1198">(13) Consideration of margins for unquantified uncertainty. <p data-bbox="1373 1214 1881 1304">c. One (or a combination) of the following testing methods used to qualify the equipment:</p> |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--|------------------------------|--|
| <p><i>Equipment Qualification</i></p> <p>14. (continued)</p> | <p>14. (continued)</p> | <p>14.(continued)</p> <ul style="list-style-type: none"> (1) Type testing of an identical item of equipment under identical or similar conditions with a supporting analysis to show that the equipment to be qualified is acceptable. (2) Type testing of a similar item of equipment with a supporting analysis to show that the equipment to be qualified is acceptable. (3) Experience with identical or similar equipment under similar conditions with a supporting analysis to show that the equipment to be qualified is acceptable. (4) Analysis in combination with partial type test data that supports the analytical assumptions and conclusions. <p>d. Documented results of the qualification that show the equipment performs its safety function when subjected to the conditions predicted to be present when it must perform its safety function up to the end of its qualified life.</p> |

Table 3.4 Instrumentation and Control (Continued)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|--|---|---|
| <i>Equipment Qualification</i> | | |
| <p>15. A program exists whose objective is to verify that the installed configuration of safety-related I&C equipment is bounded by the test configuration and test conditions or that an analysis exists which concludes that any differences will not affect the safety function of the I&C equipment.</p> | <p>15. A review will be conducted of the program established for as-built verification of safety-related I&C equipment.</p> | <p>15. A program for as-built verification of safety-related I&C equipment is in place and contains requirements for a documented evaluation that the installed configuration is bounded by the test configuration and conditions or that an analysis exists which concludes that any differences will not affect the safety function of the I&C equipment.</p> |
| <p>16. Diversity is provided, as described in Section 3.4C, in the form of hardwired backup of reactor trip, diverse display of important process parameters, defense-in-depth arrangement of equipment, and equipment diversity.</p> | <p>16.</p> <p>a. Tests will be performed using simulated input signals for items 5, 9, and 11 in Section 3.4C. For items 9 and 11 only, turn off power to SSLC equipment in four divisions.</p> <p>b. Inspection of the as-installed configuration of items 1, 2, 3, 4, 6, 7, 8, 10, and 12 in Section 3.4C, will be performed.</p> | <p>16.</p> <p>a. Item 5, Section 3.4C: Refer to Item 4 of Table 3.4 for results of ATWS tests. Item 9, Section 3.4C: Each independent display indicates its specified parameter or responds to its specified alarm setpoint as tabulated in Section 3.4C. Item 11, Section 3.4C: HPCF system initiation signals that duplicate those produced by SSLC are produced at the outputs of the hardwired, diverse signal path.</p> <p>b. The features listed as items 1, 2, 3, 4, 6, 7, 8, 10, and 12 in Section 3.4C, are implemented as hardwired, diverse, and independent of SSLC, as specified in the table.</p> |