GE Nuclear Energy

General Electric Company
175 Curtner Avenue, San Jose, CA 95125

March 26, 1993

Docket No. STN 52-001

Chet Poslusny, Senior Project Manager
Standardization Project Directorate
Associate Directorate for Advanced Reactors
and License Renewal
Office of the Nuclear Reactor Regulation

Subject: **Submittal Supporting Accelerated ABWR Review Schedule - I & C ITAAC Section 3.4**

Dear Chet:

Enclosed is a preliminary version of the proposed design certification material covering ABWR instrumentation and control (I&C) issues. This material will be included as Section 3.4 of the ABWR design certification material and is intended to cover the processes that will be used in the development, testing, and installation of safety-related digital I&C software and hardware. The enclosed material includes:

1. The complete structure of the proposed Section 3.4.
2. Completed material covering the Safety System Logic and Control, Software Development, and Electromagnetic Capability.

GE is still preparing material to cover Instrument Setpoint Methodology and Equipment Qualification. We anticipate having preliminary versions of this material available for staff review by approximately mid-April, 1993. This additional material will reflect NRC requests regarding the scope and content of design certification entries for these subjects.

Sincerely,

Jack Fox

Jack Fox
Advanced Reactor Programs

cc: Norman Fletcher (DOE)
Tony James (GE)
Barry Simon (GE)

See attached list

JF93-67

2222

1/1

3.4 Instrumentation and Control

Introduction

The following sections comprise the Tier 1 descriptions of the hardware and software process used in the development, testing, and installation of safety-related, digital, instrumentation and control (I&C) equipment and supporting implementation methodologies

3.4.1 Safety System Logic and Control

Design Description

Safety System Logic and Control (SSLC) integrates the automatic and manual decision-making and trip logic functions associated with the safety actions of the safety-related systems. These safety-related systems, taken together, include the hardware and circuitry, from sensor to actuation device input terminals, that generate signals associated with plant protection. The protective function signals are those that activate reactor trip and those that provide safety-related mitigation of consequences of reactor accidents. The relationship between SSLC and systems for plant protection is shown in Figure 3.4.1a.

System redundancy is provided by four divisions. Each independent division correlates protective action for reactor trip, containment isolation, and emergency core cooling inputs and outputs (emergency core cooling outputs are located in three divisions). Separate divisions are established by their physical relationship to the reactor vessel, which is divided into four quadrants. The sensors, logic, and output actuators of the various systems are allocated to these divisions.

SSLC equipment comprises microprocessor-based, software-controlled, signal processors that perform signal conditioning, setpoint comparison, trip logic, 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, although SSLC is not by itself a system. SSLC is an assemblage of the signal processors for several safety-related systems. SSLC hardware and software is classified as safety-related, Class 1E, and Seismic Category 1.

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 are transmitted from the instrument racks in the Reactor Building to the SSLC equipment in the Control Building via the Essential Multiplexing System (EMS). Both analog and discrete sensors are connected to Remote Multiplexing Units (RMUs) in local areas, which 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. The RMUs are limited to acquisition of sensor data and the output of control signals. Trip decisions and other control logic functions are performed in SSLC processors in the main control room area.

SSLC Signal Processing

The basic hardware configuration of one division of SSLC is shown in Figure 3.4.1b. 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:

(1) The digitized sensor inputs received in the control room are decoded by a microprocessor-based function, the Digital Trip Module (DTM). For each system function, the DTM compares these inputs to the preprogrammed levels (setpoints) for possible trip action.

(2) For 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 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 output occurs on loss of signal or power to the DTM, but, because of the 2–out-of-4 logic format in the TLU, a trip state does not appear at the output of the TLU. Loss of signal or power to a TLU also causes a trip state, but the 2–out-of-4 configuration of actuator load drivers prevents actual de-energization of the pilot valve solenoids.

(3) 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 switch inputs, 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. The TLU performs the trip setpoint comparison function as required.

(4) For Leak Detection and Isolation System (LDS) functions (except MSIV), ECCS functions, and auxiliary ESF functions, logic processing is performed as above, but in separate DTMs and 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). Loss of power or equipment failure will not cause a trip or initiation action except for containment isolation signals, which are in fail-safe format. Besides the 2–out-of-4 voting logic, the SLUs also perform interlock logic functions for each supported safety system.

(5) For reactor trip or MSIV closure, if a 2–out-of-4 trip condition is satisfied, all four divisions' trip outputs will produce a simultaneous coincident trip signal (for example, reactor trip) and transmit the signal via isolators and load drivers to the actuators for protective action. 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. For ESF functions, the trip signals in three divisions are transmitted via the Essential Multiplexing System to the Remote Multiplexing Units, 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.

(6) Upon loss of AC or DC power, functions which are normally energized, such as reactor trip or MSIV closure, provide fail-safe trip action. For normally-de-energized functions, such as ECCS, power failures leave the state of the actuated equipment unchanged. Subsequent restoration of power does not introduce transients that could cause an inadvertent change of state in the actuated equipment.

(7) The DTM, TLU, and OLUs for RPS and MSIV in each instrumentation division are powered from the divisional vital AC sources (Class 1E 120 VAC UPS). The DTMs and SLUs for ESF 1 and ESF 2 in Div. I, II, and III are powered from the divisional plant DC sources (Class 1E 125 VDC, Div. I, II, III).

Division-of-sensors Bypass

Bypassing of any single division of sensors (i.e., those sensors whose trip status is confirmed by 2–out-of-4 logic) is 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.

Bypass status is indicated to the operator until the bypass condition is removed. An electrical interlock rejects attempts to bypass more than one SSLC division at a time.

Division-out-of-service Bypass

Bypassing of any single division of output trip logic (i.e., taking a logic channel out of service) is also accomplished by means of the Bypass Unit. This type of bypass is limited to the fail-safe (de-energize-to-operate) reactor trip and MSIV closure functions, since removal of power from energize-to-operate signal processors is sufficient to remove that channel from service.

When a division-out-of-service bypass is made, the TLU 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.

Bypass status is indicated to the operator until the bypass condition is removed. An electrical interlock rejects attempts to remove more than one SSLC division from service at a time.

Testability

The SSLC has the following test capability:

(1) Internal, automatic, on-line self-test of each signal processing module from input to output. This test does not affect trip outputs.

(2) Manually-initiated off-line self-test that toggles trip outputs.

(3) Passive monitoring of power supply voltages and equipment interlocks.

(4) A surveillance test control unit to perform off-line, semi-automatic, simulation testing of SSLC functional logic, including trip, initiation, and interlock logic.

Inspection, Test, Analyses and Acceptance Criteria

Table 3.4.1 provides a definition of the visual inspections, tests and analyses, together with associated acceptance criteria, which will be used by SSLC.

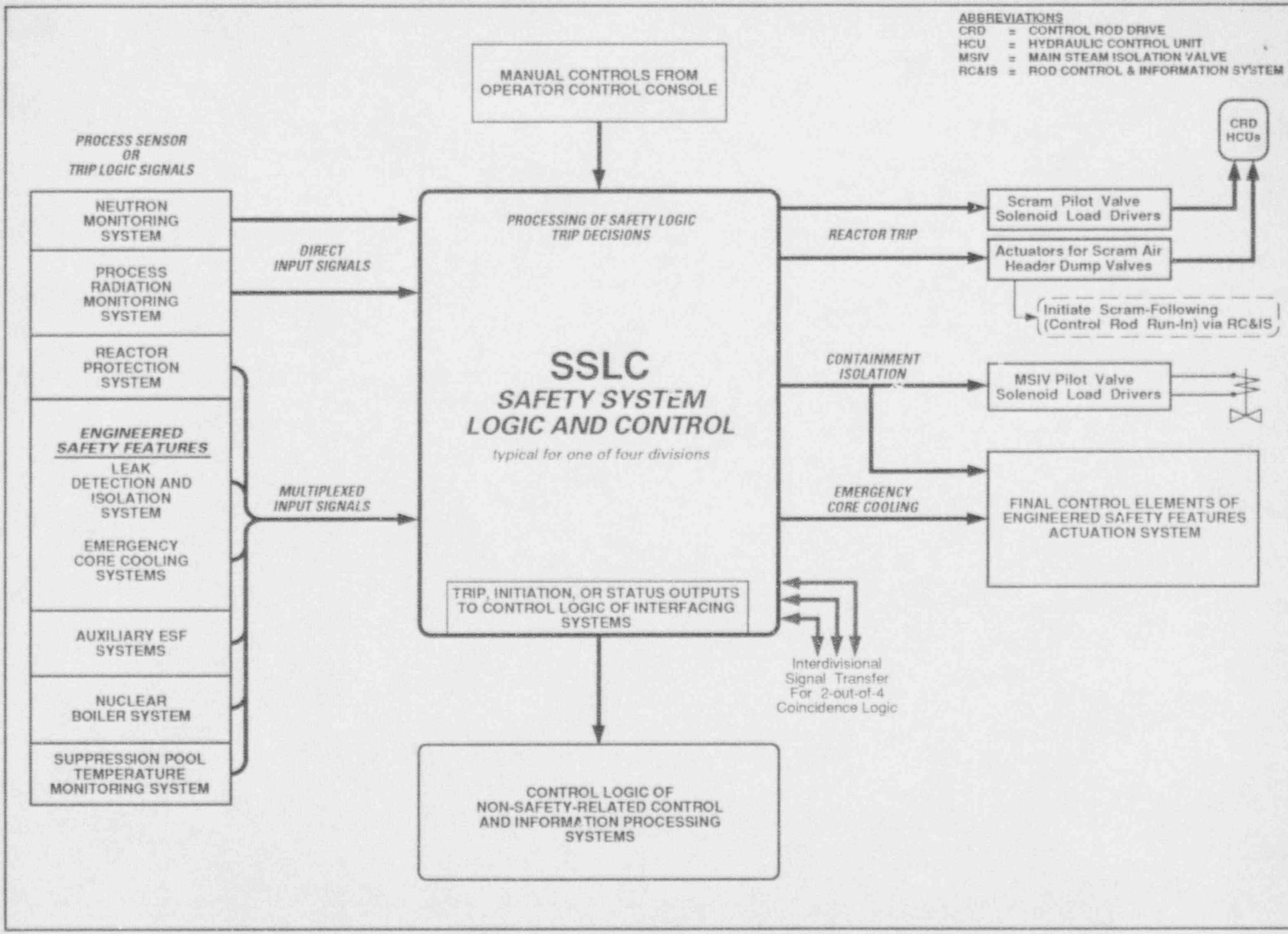
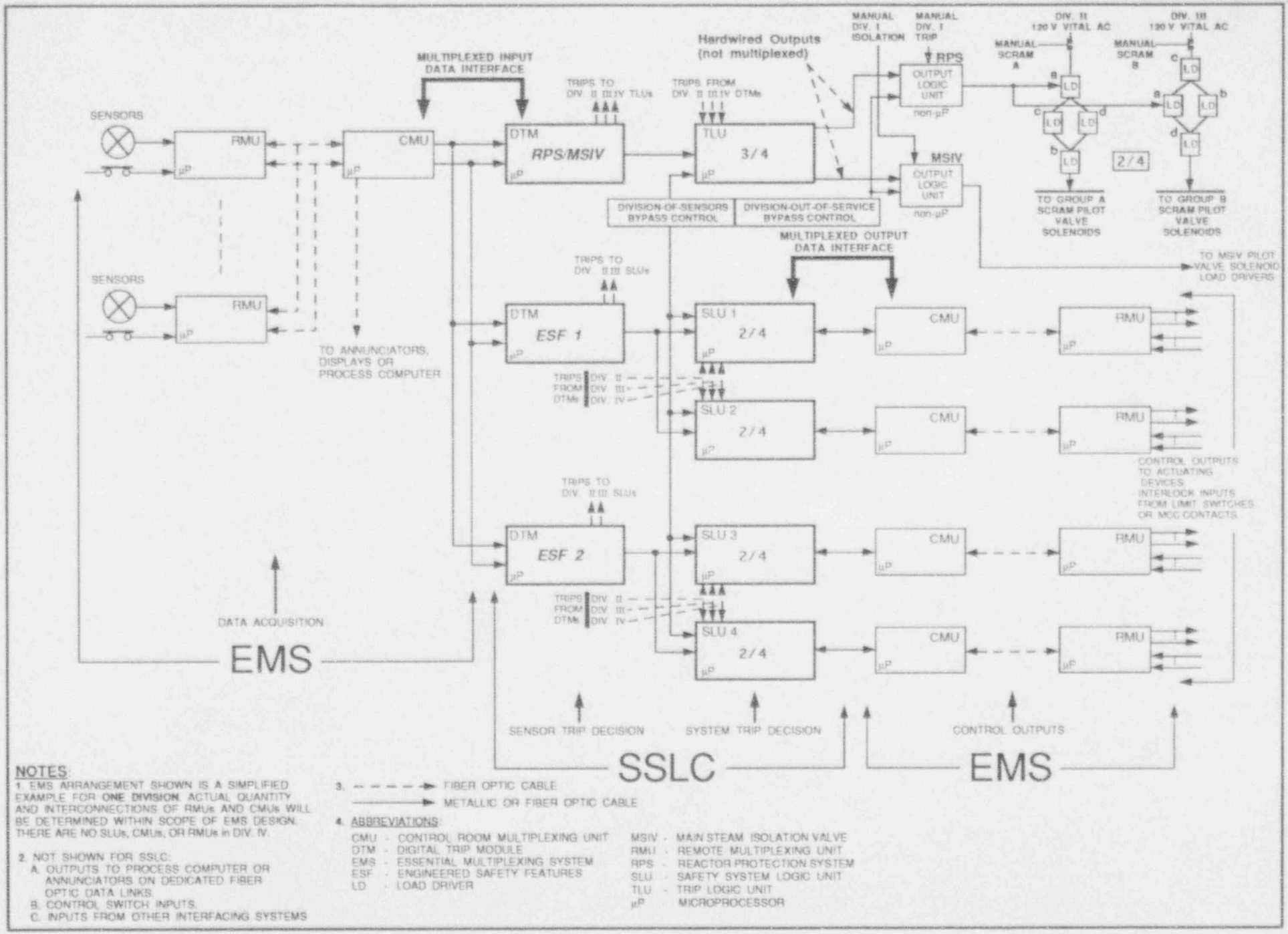


Figure 3.4a Safety System Logic and Control (SSLC) Interface Diagram



NOTES:

1. EMS ARRANGEMENT SHOWN IS A SIMPLIFIED EXAMPLE FOR **ONE DIVISION**. ACTUAL QUANTITY AND INTERCONNECTIONS OF RMUs AND CMUs WILL BE DETERMINED WITHIN SCOPE OF EMS DESIGN. THERE ARE NO SLUs, CMUs, OR RMUs in DIV. IV.
2. NOT SHOWN FOR SSLC:
   - A. OUTPUTS TO PROCESS COMPUTER OR ANNUNCIATORS ON DEDICATED FIBER OPTIC DATA LINKS.
   - B. CONTROL SWITCH INPUTS.
   - C. INPUTS FROM OTHER INTERFACING SYSTEMS
3. ---- FIBER OPTIC CABLE
   ——— METALLIC OR FIBER OPTIC CABLE
4. ABBREVIATIONS:

CMU - CONTROL ROOM MULTIPLEXING UNIT	MSIV - MAIN STEAM ISOLATION VALVE
DTM - DIGITAL TRIP MODULE	RMU - REMOTE MULTIPLEXING UNIT
EMS - ESSENTIAL MULTIPLEXING SYSTEM	RPS - REACTOR PROTECTION SYSTEM
ESF - ENGINEERED SAFETY FEATURES	SLU - SAFETY SYSTEM LOGIC UNIT
LD - LOAD DRIVER	TLU - TRIP LOGIC UNIT
	μP - MICROPROCESSOR

Figure 3.4b SAFETY SYSTEM LOGIC & CONTROL BLOCK DIAGRAM

3.4.2 Software Development

Design Description

The ABWR design uses programmable digital equipment to implement operating functions of instrumentation and control systems. A controlled process for software development and implementation will be employed. The development process for safety-related software will include a formal verification and validation (V&V) program. Non-safety-related software will be developed using a planned design process similar to the safety-related development program, but with emphasis on periodic design reviews rather than formal V&V.

The primary focus of this section is on software development. While hardware aspects of I&C designs are not discussed, the integration of the developed software with hardware is addressed.

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

An overall software development plan shall establish the requirements and methodology for software design and development. The plan shall also define 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 3.4.2a.

As part of the design of software for safety-related applications, the software development plan, at each defined phase of the software life cycle, shall address 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) which establishes standards, conventions and design processes for the design, development, and maintenance of I&C software. The SMP shall establish the organization for development of the software design, the procedures to be used, and the inter-relationships between software design activities. 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 output of each defined phase shall be a documents that define the current state of that design phase and the design input for the next design phase.

2. A Software Configuration Management Plan (SCMP) which establishes the standards and procedures controlling software design and documentation. The SCMP addresses:

a) Identification of SCMP software documentation
b) Management of software change control
c) Control and traceability of software changes
d) Verification of software to design requirements

3. A software Verification and Validation (V&V) Plan which establishes verification reviews and validation testing procedures. The V&V plan addresses:

a) Independent design verification
b) Baseline software reviews
c) Testing
e) Procedure for software revisions.

Inspections, Tests, Analyses and Acceptance Criteria

Tables 3.4.2 provides a definition of inspections, tests, and analyses, together with associated acceptance criteria, which will be performed to demonstrate compliance with the software-related commitments for the certified design.

Insert Fig. 3.4.2a

3.4.3 Electromagnetic Compatibility

Design Description

Electromagnetic compatibility (EMC) is the ability of equipment to function properly when subjected to an electromagnetic environment, and, in addition, to add minimal electromagnetic energy to that environment. Since the electromagnetic environment is composed of both radiated and conducted energy, EMC incorporates the two aspects of emission and susceptibility.

Electrical and electronic instrumentation and control equipment, particularly controllers using microprocessors to perform logic with software embedded in read-only memory (ROM), can be susceptible to the effects of electrical noise in the plant environment. Moreover, since microprocessors require an active clock to execute their control programs, these devices have an interference-causing potential when operated near other susceptible equipment.

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

a. Characteristics of the sources of electrical noise
b. Means of transmission of electrical noise
c. Characteristics of the susceptibility of the system
d. Techniques to attenuate electrical noise

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

a. Power feed lines
b. Input signal lines
c. Output signal lines
d. Radiation

Susceptibility levels will vary over these paths for different types of noise (common-mode vs. normal mode), different types of waves (electric, magnetic, or electromagnetic), and whether the noise is continuous (from an oscillatory source) or transient (from a lightning strike or switching device).

An EMC compliance plan to confirm the level of immunity to electrical noise will be part of the design, installation, and pre-operational testing of I&C equipment. EMC will be 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:

a. Electromagnetic Interference (EMI)
b. Radio Frequency Interference (RFI)
c. Electrostatic Discharge (ESD)

d. Electrical surge [Surge Withstand Capability (SWC)]

Inspections, Tests, Analyses and Acceptance Criteria

Table 3.4.3 provides a definition of the visual inspections, tests and analyses, together with associated acceptance criteria, which will be used to assess compliance of plant I&C equipment with electromagnetic compatibility requirements.

3.4.4 Instrument Setpoint Methodology

Design Description

3.4.5 Equipment Qualification

Design Description

As-built instrumentation and control 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. These environmental conditions are as follows, as applicable to the bounding design basis events: Expected time-dependent temeperature and pressure profiles, humidity, chemical effects, radiation, aging, submergence, and synergistic effects which have a significant effect on equipment performance.

Electrical equipment environmental qualification will be demonstrated by one of the following means:

a. 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.
b. Testing a similar item of equipment with a supporting analysis to show that the equipment to be qualified is acceptable.
c. Experience with identical or similar equipment under similar coditions with a supporting analysis to show that the equipment to be qualified is acceptable.
d. Analysis in combination with partial type test data supports the analytical aassumptions and conclusions.

Table 3.4 Instrumentation and Control
Section 3.4.1 Safety System Logic and Control
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. Interconnections among divisions, such as data communications for coincident trip logic decisions, use an isolating transmission medium. Outputs to non-safety-related systems also use an isolating transmission medium.	1. Inspections of the as-built SSLC equipment will be performed.	1. Interconnections among divisions and outputs to non-safety-related systems use an isolating transmission medium.
2. SSLC equipment in each division is powered from the divisional, Class 1E, plant AC and DC sources.	2. Power will be applied to an equipment division and self-test on each SSLC controller will be performed.	2. Applied power in a division only energizes controllers in that division.
3. SSLC provides the following bypass functions: a. Division-of-sensors bypass b. Trip logic bypass c. ESF channel bypass	3. Preoperational tests will exercise the SSLC bypass functions	3a. Division-of-sensors bypass: Bypass Unit in a division blocks trip signals from the Digital Trip Modules in that division from being processed in the trip logic of any other division. Bypass status is indicated at main control panel. The Bypass Unit also blocks another division-of-sensors bypass from being applied simultaneously in any other division. 3b. Trip logic bypass: Bypass Unit in a division blocks trip signals from the Trip Logic Unit in that division from de-energizing RPS or MSIV load drivers associated with that division. Bypass status is indicated at main control panel. The Bypass Unit also blocks another trip logic bypass from being applied simultaneously in any other division.

Table 3.4 Instrumentation and Control
Section 3.4.1 Safety System Logic and Control
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
3. (continued)	3. (continued)	3. (continued)
		3c. ESF channel bypass: Affected ESF loop in a division automatically continues operation after simulated loss of one redundant ESF channel in that division. Affected ESF loop also continues operation after manual ESF channel bypass. ESF channel inoperative condition and bypass status are indicated at main control panel.

Table 3.4: Instrumentation and Control
Section 3.4.2 Software Development
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. A Software Management Plan (SMP) shall be instituted which establishes that software shall be developed, designed, evaluated, and documented per a design development process that addresses, for safety-related software, software safety issues at each defined phase of the software development. The SMP shall state that the output of each defined phase shall be documents that define the current state of that design phase and the design input for the next design phase.	1. The Software Management Plan shall be reviewed.	1. The Software Management Plan shall define: 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: (i) identify software requirements having safety-related implications (ii) document the identified safety-critical software requirements in the software requirements specification for the design (iii) incorporate in to the software design the safety-critical software functions specified in the software requirements specification (iv) identify in the coding and test of the developed software, those software modules which are safety-critical (v) evaluate the performance of the developed safety-critical software modules when operated within the

Table 3.4: Instrumentation and Control
Section 3.4.2 Software Development
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. (continued)	1. (continued)	1. b. (continued) constraints imposed by the established system requirements, software design, and computer hardware requirements (vi) evaluate software interfaces of safety-critical software modules (vii) perform equipment integration and validation testing that demonstrate that safety-related functions identified in the design input requirements are operational. c. the software engineering process, which is composed of the following life-cycle phases: (i) Planning (ii) Design Definition (iii) Software Design (iv) Software Coding (v) Integration (vi) Validation (vii) Change control d. the Planning phase design activities, which shall address the following system design requirements and software development plans:

Table 3.4: Instrumentation and Control
Section 3.4.2 Software Development
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. (continued)	1. (continued)	1. d. (continued) (i) Software Management Plan (ii) Software Configuration Management Plan (iii) Verification and Validation Plan (iv) Equipment design requirements (v) Safety analysis of design requirements (vi) disposition of design and/or documentation nonconformances identified during this phase e. the Design Definition phase design activities, which shall address the development of the following implementing equipment design and configuration requirements: (i) equipment schematic (ii) equipment hardware and software performance specification (iii) equipment user's manual (iv) data communications protocol (v) safety analysis of the developed design definition

Table 3.4: Instrumentation and Control
Section 3.4.2 Software Development
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. (continued)	1. (continued)	1. e. (continued) (vi) disposition of design and/or documentation nonconformances identified during this phase 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: (i) Software Design Specification (ii) safety analysis of the software design (iii) 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: (i) software source code (ii) software module test reports (iii) safety analysis of the software coding

Table 3.4: Instrumentation and Control
Section 3.4.2 Software Development
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. (continued)	1. (continued)	1. g. (continued) (iv) disposition of nonconformances identified in this phase's design documentation and test results h. the Integration phase, which shall address the following equipment testing activities that evaluates the performance of the software when installed in hardware prototypical of that defined in the Design Definition phase: (i) integration test reports (ii) safety analysis of the integration test results (iii) disposition of nonconformances identified in this phase's design documentation and test results i the Validation phase, which comprises the development and implementation of the following documented test plans and procedures:

Table 3.4: Instrumentation and Control
Section 3.4.2 Software Development
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. (continued)	1. (continued)	1. i. (continued) (i) validation test plans and procedures (ii) validation test reports (iii) description of as-tested software (iv) safety analysis of the validation test results (v) disposition of nonconformances identified in this phase's design documentation and test results (vi) software change control procedures, and 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.

Table 3.4: Instrumentation and Control
Section 3.4.2 Software Development
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
2. A Configuration Management Plan (CMP) shall be instituted which establishes the methods for maintaining, throughout the software design process, the design documentation, procedures, evaluated software, and the resultant as-installed software.	2. The Configuration Management Plan shall be reviewed.	2. The Configuration Management Plan shall define: a. the specific product or system scope to which it is applicable. b. the organizational responsibilities for software configuration management c. methods to be applied to: (i) identify design interfaces (ii) produce software design documentation (iii) process changes to design interface documentation and software design documentation (iv) process corrective actions to resolve deviations identified in software design and design documentation (v) maintain status of design interface documentation and developed software design documentation

Table 3.4: Instrumentation and Control
Section 3.4.2 Software Development
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
2. (continued)	2. (continued)	2. c. (continued) (vi) 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. the methods for design record collection and retention.

Table 3.4: Instrumentation and Control
Section 3.4.2 Software Development
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
3. 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.	3. The Verification and Validation Plan shall be reviewed.	3. The Verification and Validation Plan shall define: 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. 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. d. that validation shall be performed through controlled and documented testing of the developed software that demonstrates compliance of the software with the software requirements specifications.

Table 3.4: Instrumentation and Control
Section 3.4.2 Software Development
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
3. (continued)	3. (continued)	3. (continued) e. 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. f. 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 1b, above), and that validation testing shall be conducted as part of the baseline review of the Validation phase of the software development life-cycle. g. that validation testing shall be conducted per a documented test plan and procedure. h. that for non-safety-related software development, verification and validation shall be performed through design reviews conducted as part of the

Table 3.4: Instrumentation and Control
Section 3.4.2 Software Development
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
3. (continued)	3. (continued)	3. h. (continued) 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. i. the products which shall result from the baseline reviews conducted at each phase of the software development life-cycle; and that the defined products of the baseline reviews and the V&V Plan shall be documented and maintained under configuration management. j. the methods for identification, closure, and documentation of design and/or design documentation nonconformances. k. that the software development is not complete until the specified verification and validation activities are complete and design documentation is consistent with the developed software.

Table 3.4: Instrumentation and Control
Section 3.4.2 Software Development
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
4. Software development shall be performed in accordance with the software management plan, configuration management plan, and verification and validation plan.	4. Review software development results .	4. Software development has been completed as defined in the SMP, CMP, and V&VP.

Table 3.4: Instrumentation and Control
Section 3.4.3 Electromagnetic Compatibility
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. A plan will be established to assure that electrical and electronic components and systems whose performance can be degraded or whose circuitry can be damaged by exposure to high electromagnetic fields, high electrostatic fields, or electrical current surges occurring at their installed locations will be qualified for the anticipated levels of electrical interference at these locations. The plan will include instrumentation and control equipment in the following systems: a. Safety System Logic and Control b. Essential Multiplexing System c. Non-essential Multiplexing System d. Other microprocessor-based, software controlled systems or equipment as referenced in Table 3.0. The plan will be structured on the basis that I&C equipment will be verified by factory testing and site testing of both individual components and interconnected systems to meet Electromagnetic Compatibility (EMC) requirements for protection against the effects of: a. Electromagnetic Interference (EMI) b. Radio Frequency Interference (RFI) c. Electrostatic Discharge (ESD) d. Electrical surge [Surge Withstand Capability (SWC)]	1. See below.	1. See below.

Table 3.4: Instrumentation and Control
Section 3.4.3 Electromagnetic Compatibility
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. (continued) The plan will require, 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 will be documented in a qualification file and subject to audit: 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: (1) Types of test equipment. (2) Range of normal test conditions. (3) Range of abnormal test conditions for expected transient environment. (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.	1. (continued) See below.	1. (continued) See below.

Table 3.4: Instrumentation and Control
Section 3.4.3 Electromagnetic Compatibility
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. (continued)	1. (continued)	1. (continued)
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. The plan will establish separate test regimes for each component of EMC, using the following approaches:		
a. EMI and RFI Protection. An EMC compliance plan for each component or system identified above will include tests to ensure that all equipment performs its normal functions in the presence of the specified EMI/RFI electrical noise environment without equipment damage, spurious actuation, or inhibition of functions. As part of the pre-operational test program, the EMC compliance plan will call for each system to be subjected to EMI/RFI testing. Tests will cover potential EMI and RFI susceptibility over four different paths: (1) Power feed lines (2) Input signal lines (3) Output signal lines (4) Radiation	a. EMI and RFI Protection. Inspections of the plant pre-operational test program will be conducted to confirm that equipment was tested for EMI/RFI protection using procedures defined in the EMC plan.	a. EMI and RFI Protection. An EMC compliance plan is in place and implements elements described in the Certified Design Commitment.

Table 3.4: Instrumentation and Control
Section 3.4.3 Electromagnetic Compatibility
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. (continued)	1. (continued)	1. (continued)
b. ESD Protection. An EMC compliance plan for each component or system identified above will include tests to ensure that all equipment performs its normal functions in the presence of the specified ESD environment without equipment damage, spurious actuation, or inhibition of functions. The plan will be structured on the basis that ESD protection will be confirmed by factory tests that will determine the susceptibility of instrumentation and control equipment to electrostatic discharges. The EMC compliance plan will include standards, conventions, design considerations, and test procedures to ensure ESD protection of the plant instrumentation and control equipment. The plan will require test documentation confirming that , for each component tested, the following conditions have been met: a. No change in output signal status was observed during the test. b. The equipment performed its normal functions after the test.	b. ESD Protection. Inspections will be performed on factory QA records to confirm that the shipped equipment has been tested for ESD protection using procedures defined in the EMC plan.	b. ESD Protection. An EMC compliance plan is in place and contains the elements described in the Certified Design Commitment.

Table 3.4: Instrumentation and Control
Section 3.4.3 Electromagnetic Compatibility
Inspections, Tests, Analyses and Acceptance Criteria

Certified Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. (continued c. SWC Protection. An EMC compliance plan for each component or system identified above will include tests to ensure that all equipment performs its normal functions for the specified SWC environment without equipment damage, spurious actuation, or inhibition of functions. The EMC compliance plan will include standard. nventions, design considerations, and test procedures to ensure SWC protection of the plant instrumentation and control equipment. The plan will be structured on the basis that SWC protection will be confirmed by factory tests that will determine the surge withstand capability of the plant instrumentation and control equipment. The plan will document the level of compliance of each system with the grounding and shielding practices of the standards specified under this certified design commitment	1. (continued) c. SWC Protection. Inspections will be performed on factory QA records to confirm that the shipped equipment has been tested for surge withstand capability using procedures defined in the EMC compliance plan.	1. (continued) c. SWC Protection. An EMC compliance plan including SWC protection provisions is in place and contains the elements described in the Certified Design Commitment.