7A Design Response to Appendix B, ABWR LRB Instrumentation and Controls

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

STD DEP T1 2.14-1 (Table 7A-1)

STD DEP T1 3.4-1 (Table 7A-1, Figure 7A-1)

STD DEP 1.8-1

STD DEP 7.1-1

STD DEP Admin

7A.1 Introduction

STD DEP T1 3.4-1 (Table 7A-1, Figure 7A-1)

The instrumentation and control (I&C) systems of the ABWR use state-of-the-art fiber optic~~s,~~ -based communication equipment ~~multiplexing~~ and computer controls.

In Appendix B to the GE Advanced Boiling Water Reactor Licensing Review Bases (LRB), dated August, 1987, the NRC staff indicated that guidance in this area had not been developed. However, GE committed to address the standards and criteria currently specified in the SRP, and to use the documents and criteria identified in Appendix B.

The NRC requested considerable additional information specific to this equipment in Appendix B. The NRC requests, along with ~~GE's~~ responses as revised, are provided in this appendix to Chapter 7.

A Failure Modes and Effects Analysis (FMEA) of the Essential ~~Multiplexing System~~ Communication Functions (ECFs) is provided in Appendix 15B.

[The following two Items must be addressed when any change is made in the commitments of the ~~EMS~~ ECFs and Safety Systems Logic and Control (SSLC) systems Design:

(1) Table 10 of DCD/Introduction identifies the commitments for ~~EMS~~ ECFs performance specifications and architecture which, if changed, requires NRC Staff review and approval prior to implementation. The applicable portions of the Tier 2 sections and tables, identified on Table 10 of DCD/Introduction for this restriction, are italicized on the sections and tables themselves.

(2) *Table 11 of DCD/Introduction identifies the commitments for SSLC* systems *hardware and software qualification which, if changed, requires NRC Staff review and approval prior to implementation. The applicable portions of the Tier 2 sections and tables, identified on Table 11 of DCD/Introduction for this restriction, are italicized on the sections and tables themselves.]* *

7A.2 [Multiplexing Systems~~]~~

STD DEP T1 3.4-1 (Table 7A-1, Figure 7A-1)

STD DEP 1.8-1

STD DEP Admin

NRC Request (1)*—Provide a complete list of components (pumps, valves, etc.) whose actuation, interlock, or status indication is dependent on the proper operation of each Class 1E multiplexer.*

Revised ***Response (1)***—Class 1E multiplexers are not used in more modern I&C systems. Safety-related data communication is performed as an integral function of the SSLC systems. ~~*The*~~ A typical *list* of components whose actuation, interlock, or status indication depends on the proper operation of SSLC equipment implementing these essential communication functions (ECFs) *is provided as Table 7A.1. It was obtained by extraction from ~~the multiplexer~~* an early version of the ABWR *I/O database which reflects information* that was *available on the system P&ID and IBD drawings* at the time of design certification. The inventory of components satisfying this criteria is subject to change as the detailed design is implemented.

NRC Request (2)*—For the components cited above, describe the means of remote or local control (other than by cutting wires or jumpering) that may be employed should the multiplexer fail.*

Revised ***Response (2)***—Class 1E multiplexers are not used. Safety-related data communication is performed as an integral function of the SSLC systems. *All Class-1E ~~multiplex~~* SSLC *hardware is designed to meet the single-failure criteria. Systems which employ such hardware have redundant ~~channels~~* divisions of equipment *such that no single failure of any ~~MUX unit~~* SSLC component, including those implementing the ECFs, *could jeopardize any safety system action. In addition, local control is provided, via the Remote Shutdown System, to bring the reactor to shutdown conditions in event of multiple safety system failures or evacuation of the control room. The Remote Shutdown System is hard-wired and therefore provides diversity to the ~~MUX~~* SSLC *interfaces.*

NRC Request (3)*—Describe the multiplexer pre-operational test program.*

Revised ***Response (3)***—Multiplexers are not used. Safety-related data communication is performed as an integral function of the SSLC systems. Non-safety

* *See Section 3.5 of DCD/Introduction.*

data communication is performed by the Plant Data Network (PDN) and dedicated system level communication links. *The pre-operational test program will test the ~~multiplexers~~* data communication functions (DCFs) *concurrently with instrumentation and control functional loop checks. As each input to ~~a remote multiplexing unit (RMU)~~* an input/output (I/O) device *is simulated using a suitable input device, the required outputs shall be verified correct. In this manner, all hardware and software are confirmed concurrently.*

Equipment verifications of the individual ~~multiplexing units~~ I/O devices *are performed at the factory and typically include detailed component level tests which require special test apparatus and technical expertise. Any malfunctioning not found during factory testing will be detected during pre- operational tests of instrument loops.*

~~Testing shall include~~ Preoperational testing includes *instrument loop checks*, and *calibration verification tests ~~and response time verification tests~~ as described in ANSI/IEEE-338.* Factory testing includes response time verification tests on the digital logic processing equipment. *~~If possible, the entire instrument loop shall be tested from sensor to output device(s). Otherwise, suitable input devices shall be used to simulate process inputs and the system outputs verified to be acceptable.~~*

In addition to the testing described above, tests shall be developed to verify system ~~redundancy and~~ electrical independence (ITAAC Table 3.4-1 Item 3).

***NRC Request (4)**—Describe the test and/or hardware features employed to demonstrate fault tolerance to electromagnetic interference.*

Revised ***Response (4)**—One major deterrence to electromagnetic interference (EMI) in the ~~multiplexing system~~* ECFs *is the use of fiber optic data links as the transmission medium. Optical fiber, being a non- electrical medium, has the inherent properties of immunity to electrical noise (EMI,* radio frequency interference *(RFI), and lightning), point-to-point electrical isolation, and the absence of conventional transmission line effects. Fiber optic ~~multiplexing~~* media *is also unaffected by the radiated noise from high voltage conductors, by high frequency motor control drives, and by transient switching pulses from electromagnetic contactors or other switching devices.*

However, the electrical-to-optical interface at the transmitting and receiving ends must still be addressed to ensure complete immunity to EMI. The control equipment containing the electrical circuitry use standard techniques for shielding, grounding, and filtering and are mounted in grounded equipment panels provided with separate instrument ground buses. Panel location, particularly in local areas, is carefully chosen to minimize noise effects from adjacent sources. The use of fiber optic cables ensures that current-carrying ground loops will not exist between the control room and local areas.

The use of redundancy provides the other major deterrence to EMI effects. ~~The safety-related multiplexing system uses redundant optical channels within each separated electrical division.~~ The ~~systems~~ divisions *are independent and will run asynchronously with respect to each other with ~~no~~* limited *communication between divisions. ~~However, data communication and transfer is synchronized within each division itself.~~ This*

arrangement provides fault tolerance to EMI or other noise occurring in isolated locations.

During normal operation, ~~multiplexing system~~ data communication *performance will be monitored by online* diagnostic *tests such as parity checks, ~~data checks (boundary and range), and transmission timing. If response time requirements permit, error correcting algorithms may be applied to mask noise effects. Periodic surveillance using offline tests such as bit error rate will be used to verify overall system integrity.~~*checksum verification or the reception of a keep-alive signal.

As part of the ~~pre-operational~~ equipment qualification *test program [see Request (3)], the ~~systems~~* equipment qualification type test specimen *will be subjected to EMI testing. EMI and RFI test measurements will be developed using the guidelines described in ANSI/IEEE-C63.12, "American National Standard for Electromagnetic Compatibility Limits—Recommended Practice." For testing susceptibility to noise generation from portable radio transceivers, tests will be developed from ANSI/IEEE-C37.90.2, "IEEE Trial-Use Standard, Withstand Capability of Relay Systems to Radiated Electromagnetic Interference from Transceivers." Section 5.5.3 of this standard describes tests for digital equipment using clocked logic circuits.*

~~With the system connected, each~~ The type test specimen *~~multiplexing unit (one at a time)~~ will be required to demonstrate immunity to the defined conducted and radiated tests. Units shall also comply with standard surge withstand capability tests, as follows:*

(a) ANSI/IEEE-C62.41—"Guide for Surge Voltages in Low-Voltage AC Power Circuits."

(b) ANSI/IEEE-C62.45—"Guide on Surge Testing for Equipment Connected to Low- Voltage AC Power Circuits."

The interconnecting fiber optic links of the ~~multiplexing system and~~ SSLC systems *are not subject to EMI effects.*

For design guidance and additional test development guidance, the following military standards shall be used:

(a) MIL-STD-461~~C~~ E*—"Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference."*

~~(b) MIL-STD-462—"Measurement of Electromagnetic Interference Characteristics."~~ Not Used

Due to the comprehensive nature of these documents, their applicability to ground, airborne, and shipboard equipment, and the differences in requirements for the Army, Navy and Air Force, the use of these standards shall be limited to the susceptibility requirements and limits for class A3 equipment and subsystems (ground, fixed). Within these limits, the guidelines for Army procurements only shall be used. Tests for transmitting and receiving equipment, power generators, and special purpose military devices are not applicable.

[To facilitate achieving electromagnetic compatibility (EMC) compliance, system and equipment grounding and shielding practices will follow the guidance of the standards listed below:

(a) EEE Std. 518, "Guide for the Installation of Electrical Equipment to Minimize Electrical Noise Inputs to Controllers from External Sources."

(b) EEE Std. 1050, "Guide for Instrumentation and Control Equipment Grounding in Generating Stations."] *

NRC Request (5)*—Describe the interconnection, if any, of any Class 1E multiplexer to non-Class 1E devices such as the plant computer.*

Revised *Response* (5)—Class 1E multiplexers are not used. Safety-related data communication is performed as an integral function of the SSLC systems. *The interconnection of Class 1E ~~multiplexers~~ communication devices to non-Class 1E devices is done using fiber optic cable. The fiber optic cable will provide the necessary isolation.*

~~The plant process computer is~~ Non-Class 1E devices are *connected to a buffer module (memory storage module). Information is stored in this module by ~~the~~ 1E ~~MUX units~~* communication interface equipment *for access by ~~the process computer~~* non-Class 1E devices*, thus preventing any interruption by ~~the~~ Non 1E ~~process computer~~* devices *on the 1E* communication functions.

NRC Request (6)*—Describe the online test and/or diagnostic features that may be employed, including any operator alarms/indicators and their locations.*

Revised *Response (6)* *~~The EMS self-test system relies on the Safety System Logic and Control (SSLC) test control unit, though it has also its own local self-test system. Local self-test in each EMS unit continues to provide diagnostic readout even if the test control unit fails.~~* (An EMS is not used.)

*~~A c~~*C*ontinuously operating ~~self-test system~~*diagnostics *check~~s~~ all data transmission*s *and provide~~s~~ operators with fault information and fault location through ~~dedicated~~ alarm~~s~~ ~~and computer output~~. The ~~self-test system~~* diagnostics *operation or its failure cannot harm the operation of the safety systems.*

~~Figure 7A-1 shows the general concept of the EMS interface with the test control unit.~~ The ~~online~~ test and diagnostic features including operator alarms and location are detailed as follows:

- *Self ~~-test~~* diagnostics and periodic testing *locates a fault down to the processing module level and provides positive local identification of the failed device.*
- *A periodic, ~~automatic~~ test feature verifies proper operation of the ~~EMS~~* ECFs*.*

* *See Section 7A.1(2) ~~amd~~and 7A.1(1).*

- *Detection of fatal (affects signal transmission) and non-fatal (does not affect signal transmission) errors is annunciated ~~and relayed to the computer~~. Operators are informed on the type of malfunction and its location.*

- *~~Local self test~~* Self- *~~is~~* diagnostics are *continuous. System end-to-end test is initiated* as an off-line test *in one division at a time~~ by communication between test units in each division.~~*

- *~~The logic returns to its original state after the test sequence is completed.~~ Indication~~s~~ of test ~~status (normal or in test) and~~ results (pass, fail) is provided.*

- *The ~~test~~* diagnostic *function does not degrade system reliability.~~ The test circuitry is physically and electrically separated and isolated from the functional circuitry insofar as possible. Testing~~* The diagnostic function *will not cause actuation of the driven equipment.*

- *~~Automatic initiation signals from plant sensors override an automatic test sequence and perform the required safety function.~~*

- *~~Failure of the test control unit does not affect the safety system functional logic.~~*

NRC Request (7)*—Describe the multiplexer power sources.*

Revised ***Response (7)***—Multiplexers are not used. Safety related data communication is performed as an integral function of the SSLC systems. *The ~~multiplexer system~~* equipment implementing the ECFs *receives its power from the four-divisional battery-*backed *125 ~~VDC~~* VAC *buses (*uninterruptible*). These are discussed in Subsection 8.3.2 and illustrated in Figure 8.3-4.*

NRC Request (8)*—Describe the dynamic response of the multiplexers to momentary interruptions of AC power.*

Revised ***Response (8)***—Multiplexers are not used. Safety-related data communication is performed as an integral function of the SSLC systems. *Each of the four divisions of the ~~multiplexer system~~ SSLC systems is fed by the corresponding division of the 125 VDC battery. Therefore, the ECFs will not be affected by momentary interruption to the AC power. Extended losses of power in any division would not affect operations of safety functions because of multiplicity of divisional power (Figure 8.3-3).*

If ~~EMS~~ there is a loss of *power ~~is interrupted and subsequently restored, then the EMS unit reinitializes automatically and the system reconfigures to accept the signal transmission~~* to the ELCS system, it will assume a predefined safe state*.*

NRC Request (9)*—Describe the applicability of the plant Technical Specifications to multiplexer operability.*

Revised ***Response (9)***—Multiplexers are not used. Safety-related data communication is performed as an integral function of the SSLC systems. *The applicability of the plant Technical Specifications to the ~~four-division multiplexer~~* SSLC

systems *operability will be a section in the specifications that will include limiting condition for operation, and surveillance requirements.*

The limiting condition is expected to be similar to that for a loss of a divisional electrical power supply.

***NRC Request (10)**—Describe the hardware architecture of all multiplexer units.*

Revised *Response (10)*—Multiplexers are not used. Safety-related data communication is performed as an integral function of the SSLC systems. ~~*The multiplexer units are of two types:*~~

~~*(1) Remote Multiplexing Units (RMU)*~~

~~*(2) Control Room Multiplexing Units (CMU)*~~

System Configuration

For the RTIS, input and output signals are directly connected to the RTIS equipment for each protective division.

In each ELCS *protection division,* ~~*RMUs*~~ remote DLCs (RDLCs) *are located in local plant areas to acquire sensor data and transmit it to the control room for processing. The* ~~*RMUs*~~ *RDLCs also receive processed signals from the control room for command of safety system actuators.* ~~*CMUs are located in the control room to transmit and receive data for the logic processing units of the safety protection system (RPS and ESF). Response time constraints may dictate RPS outputs be hardwired (not multiplexed) to the load drivers.*~~

~~*All*~~ RDLC *interconnections are fiber optic data links.* ~~*Within each division, the system uses redundant links (either in a hot standby configuration or a bi-directional, reconfigurable arrangement) for greater reliability.*~~

The safety-related ~~*multiplexing systems*~~ equipment implementing the ECFs *in each division are separated and independent.*

ELCS *Hardware Configuration*

(1) ~~*(1)RMU*~~ RDLC

(a) Microprocessor-based, ~~*bus-oriented architecture with control program in ROM (i.e., firmware)*~~programmable controller with control program stored in non-volatile memory.

(b) Modular design: Plug-in modules or circuit boards with distinct functions on separate modules ~~*(CPU, memory, I/O)*~~*. Redundant low voltage power supplies are used for greater reliability.*

(c) Input modules acquire safety-related analog and digital data from process transmitters and equipment status contact closures,

respectively. Analog input modules perform signal conditioning and A/D conversion. Digital input modules perform signal conditioning (filtering, voltage level conversion).

(d) Output modules transmit processed control signals to equipment actuator circuits (output signals may be contact closures or voltage levels to drive relays or solid-state load drivers).

(e) ~~*(e) Communications interface modules format and transmit input signals as serial multiplexed words via fiber optic data links from local areas to the control room multiplexing units. These modules also receive processed signals from the control room and demultiplex and prepare output signals for interfacing to actuators.*~~ Section 7.9S explains the methods used to communicate data between all DLCs.

(f) ~~*CPU and memory*~~ Controller *modules coordinate I/O and communication functions and perform peripheral tasks such as self-test and calibration.*

(g) ~~*Front panel interface (isolated from safety-critical signal path) permits*~~ A maintenance and test panel (MTP) is provided for each ELCS protective division. The MTP provides the interfaces for *technician access to calibration and diagnostic functions.*

[The development of the ~~***essential multiplexing***~~ **SSLC systems shall assure that the ECFs are implemented** ~~***as a***~~ **using a *deterministic,*** ~~***dual redundant, fiber optic ring structure***~~ **design.** ~~***shall follow the Fiber Distributed Data Interface (FDDI) protocol as described in the following American National Standards Institute (ANSI) reference documents:***~~

~~***(a) ANSI X3.166, "Fiber Distribution Data Interface (FDDI) - Physical Layer Medium Dependent (PMD)."***~~

~~***(b) ANSI X3.148,"Fiber Distributed Data Interface (FDDI) - Token Ring Physical Layer Protocol (PHY)."***~~

~~***(c) ANSI X3.139, "Fiber Distributed Data Interface (FDDI) - Token Ring Media Access Control (MAC)."***~~

~~***(d) ANSI X3T9.5/84-49, "FDDI Station Management (SMT)," Preliminary Draft.]***~~*~~*~~

~~*For portions of the safety systems where the data throughput requirement is less than 5M bit/s, IEEE 802.5, Token Ring Access Method and Physical Layer Specifications, may be implemented as an alternative, using either coaxial, twisted pair or fiber optic cable as the transmission medium. Both networks conform to ISO 7498, Open Systems Interconnection Basic Reference Model, as the Data Link Layer and Physical*~~

* *See Sections 7A.1(2) and 7A.1(1).*

~~*Layer. For the Data Link Layer, IEEE 802.2, Standard for Local Area Networks: Logical Link Control, shall be used with either network to define the protocols necessary to move data to the higher levels of the ISO model.*~~

~~*Communications protocols used for data transmission in other parts of the safety system and for transferring data to the non-safety systems shall also conform to ISO 7498.*~~ Section 7.9S provides information on the design of the data communication functions.

NRC Request (11)*—Describe the "firmware" architecture.*

Revised Response (11)*—The "firmware" (software contained in* ~~*ROM*~~non-volatile memory*) architecture depends upon knowledge of a specific hardware/software combination for the* ~~*multiplexer units*~~ I/O devices*. Since Tier 2 is to be independent of specific vendor's hardware and is, instead, based upon system level requirements, the exact configuration of software for the* ~~*multiplexer units*~~ I/O devices *is not specified. However, software development will follow a process consistent with the safety-related nature of the* ~~*multiplexing system*~~ ELCS, including their ECFs*.*

The software must also support the following characteristics of the ~~*multiplexing system*~~ ELCS*:*

(1) The ~~*multiplexing system is a*~~ ELCS ECFs are implemented as *real-time control application*s *configured as* ~~*a*~~ point to point, unidirectional~~*, fiber optic local area network*~~ data links*.*

(2) Because time response for some functions is critical to safety, system timing must be deterministic and not event-driven. ~~*A typical industry standard communications protocol that is likely to be used is FDDI (Fiber Distributed Data Interface), a token-passing, counterrotating ring structure with data rates to 100M bit/s. Hardware communications interfaces to this protocol are available, thus reducing the need for special software development.*~~

(3) The safety-critical system functions are analog and digital data acquisition, signal formatting, signal transmission, ~~*demultiplexing,*~~ *and control signal outputs to actuators. Peripheral functions are self-*~~*test*~~diagnostic *features, periodic testing and system calibration* ~~*(e.g., adjustment of A/D converters)*~~*.*

(4) During system initialization or shutdown and after loss of power, control outputs to actuators must fail to a safe state (fail safe or fail-as-is, as appropriate for the affected safety system). System restart shall not cause inadvertent trip or initiation of safety- related equipment (i.e., system output shall depend only on sensed plant inputs).

(5) The system must be fault-tolerant to support the single-failure criterion. Multi-division duplication of the system will provide this feature~~*; however, within each division, the system will also be redundant for high availability. Thus, the software must perform failure detection and automatic switchover or reconfiguration in case of failure of one multiplexer channel .*~~

High quality software is the most critical aspect of microprocessor-based designs for safety systems. The software must be of easily proven reliability so as not to degrade the reliability and availability of the overall system. When installed as "firmware", the software should become, in effect, another high quality hardware component of the control equipment~~, especially, since the program in ROM is protected from being changed by external sources~~.

Software development will, in general, follow Regulatory Guide 1.152, which endorses ANSI/IEEE ANS-7-4.3.2. These documents emphasize an orderly, structured, development approach and the use of independent verification and validation to provide traceable confirmation of the design. Validation must verify a predictable and safe response to abnormal as well as normal test cases. A software-based design must also support the testability, calibration and bypass requirements of IEEE ~~279~~603.

To meet the above requirements, the software will be developed as a structured set of simple modules. Each module will perform a prescribed task that can be independently verified and tested. ~~Modules shall have one entry and one exit point.~~ The software requirements specification and design specification will define structures of external files used and interfaces with other programs. ~~In place of a formal operating system, an "executive" control program or real-time kernel will monitor, schedule, and coordinate the linking and execution of the modules.~~ The integration of the modules into the control program will be another activity to be independently verified and validated.

The overall program structure will be a hierarchy of tasks. Separate modules will be created for safety- critical tasks, calibration functions, and self-test functions, with self-test running in the background at the lowest priority. Highest priority functions will always run to completion. The use of interrupts will be minimized to prevent interference with scheduled tasks.

On detection of communication *faults, retry ~~or rollback to the last known correct state~~ will be permitted within system time constraints. If the fault is permanent~~ and potentially unsafe~~, the ~~system~~* module *shall ~~recover (or fail)~~ to a ~~safe~~* predefined *state and the operator shall be alerted. ~~The redundant multiplexing channels shall be repairable online if one channel fails.All processor memory not used for or by the operational program shall be initialized to a pattern that will cause the system to revert to a safe state if executed.~~* System level diagnostics verify memory is not changed after initial loading.

The software shall permit online calibration and testing ~~with the outputs to the safety systems bypassed~~ consistent with the requirements of the Technical Specifications*.*

The software design shall prevent unauthorized access or modification.

Software development to achieve program operation as described above and to document and verify this operation shall conform to the following standards:

(1) [IEEE-828, "IEEE Standard for Software Configuration Management Plans"

(2) IEEE-829, "IEEE Standard for Software Test Documentation"

(3) IEEE-830, "IEEE Standard for Software Requirements Specifications"

(4) IEEE-1012, "IEEE Standard for Software Verification and Validation Plans"

(5) IEEE-1042, IEEE Guide to Software Configuration Management] *

NRC Request (12)*—Provide an explicit discussion of how the systems conform to the provisions of IEEE-279, Section 4.17.*

Response (12)—Also reference IEEE-603 Sections 5.1, 6.2, and 7.2. *The ~~multiplexing system~~* ECFs *for safety systems ~~only acquire~~* support the acquisition of *data from plant sensors (pressure, level, flow, etc.) and equipment status contact closures (open, close, start, stop, etc.) that provide automatic trip or initiation functions for RPS and ESF equipment.*

*Manual initiation inputs for protective action*s such as reactor scram, *are implemented by direct, hardwired or optical connections to the safety system logic*. Manual initiation inputs for other protective actions *(e.g., ECCS, containment isolation*, except for MSIV isolation) depend on the ECFs for communication to the safety system logic*. Initiation outputs for ECCS and isolation functions (except MSIV) are ~~multiplexed~~* communicated *to the actuators* using the ECFs*. Manual scram (reactor trip) is provided by breaking the power source to the scram pilot valve solenoids external to the ~~multiplexing system~~* equipment implementing the ECFs *and safety system logic. Manual reactor trip and manual MSIV closure in each division are available even with ~~multiplexing system~~ failure* of the ECFs*, since these outputs are not ~~multiplexed~~* communicated *to the actuators* via the ECFs*.*

However, because the ~~multiplexing system~~ design is fault tolerant (replicated in four divisions and redundant within each division) [see the responses to Requests (4), (10), and (11)], a single failure will not degrade data communications in any division.

Therefore, the requirements of IEEE-279, Section 4.17 (IEEE-603 Section 5.1)*, are satisfied, since a single failure will not prevent initiation of protective action by manual or automatic means.*

The last sentence of Section 4.17 states that "manual initiation should depend upon the operation of a minimum of equipment". The first paragraph has shown that manual initiation of *reactor trip and MSIV ~~initiation~~* isolation *do not depend at all on the ~~multiplexing system~~* ECFs. ~~m~~Manual initiation of *ECCS ~~initiation~~ and isolation ~~initiation~~ other than MSIV do ~~not~~ depend on ~~multiplexing~~* ECFs *for sending inputs to the logic*, but can tolerate the single failure of one division of ECFs*. ~~and~~* They *depend on the operation of only one channel of ~~multiplexing~~* ECFs *in each division to send outputs to actuators.*

* *See Sections 7A.1(2) and 7A.1(1~~1~~).*

NRC Request (13)*—Provide an explicit discussion of how the systems conform to IEEE 279, Paragraph 4.7.2, as supplemented by Regulatory Guide 1.75 and IEEE 384.*

Response (13)*—The safety-related ~~multiplexing system~~* ECFs*, which ~~is~~* are *part of the protection system, ~~has~~* have *no direct interaction with the control systems. Sensor and equipment status data are ~~multiplexed~~* communicated *only to protection system logic. However, ~~two~~ signals are sent from the protection system logic to ~~the Recirculation Flow Control System: Reactor Water Level 2 Trip and Recirculation Pump Trip~~* non-safety systems*. The signals are transmitted via fiber optic data links~~, which are not part of the multiplexing system. An isolating buffer (gateway) transfers these signals to the non-safety-related network of the control systems.~~* or through qualified isolation devices.

Fiber optic transmission lines are not subject to credible electrical faults such as short-circuit loading, hot shorts, grounds or application of high AC or DC voltages. Adjacent cables are not subject to induced fault currents or to being shorted together. The effects of cable damage are restricted to signal loss or data corruption at the receiving equipment. Cables and control equipment of different systems or assigned to different divisions are kept separated only to prevent simultaneous physical damage.

Thus, the ~~multiplexing system~~ SSLC systems ECFs design *conforms to IEEE-279, paragraph 4.7.2* (IEEE-603 paragraph 5.6.3.1(2))*, in that no credible failure at the output of an isolation device can "prevent the protection system ~~channel~~ from meeting minimum performance requirements specified in the design bases."*

To meet the requirements of IEEE-384 and Regulatory Guide 1.75, the protective covering of the fiber optic cables are flame retardant. The cables are passed through physical, safety class barriers, where necessary, for separation of Class 1E circuits and equipment from other Class 1E equipment or from non-Class 1E equipment. The fiber optic ~~multiplexing network is~~ data communication paths are *independent in each protection division~~ and does not transmit or receive data between divisions~~.* Limited data communication does occur between divisions, for example, to provide signals needed for 2-out-of-4 voting logic. However, dedicated fiber optic cables are used for this purpose, thereby providing electrical isolation and preserving divisional independence. *However, the ~~multiplexing~~ equipment* implementing the ECFs *is* otherwise *kept physically separate to minimize the effects of design basis events.*

NRC Request (14)*—Provide confirmation that system level failures of any multiplexer system detected by automated diagnostic techniques are indicated to the operators consistent with Regulatory Guide 1.47. (i.e., bypass and inoperable status indication).*

Revised ***Response (14)****—*Multiplexers are not used, and there is no multiplexer system. Safety-related data communication is performed as an integral function of the SSLC systems. *Each safety-related ~~multiplexing system~~* SSLC system *contains online self-diagnostics ~~implemented in software and hardware~~ that will ~~continuously~~ monitor system performance*, including its associated ECFs. *~~Within each control station~~*As an example, for each ELCS controller*, the following typical parameters are monitored: (1) status of the CPU, (2) ~~parity checks~~*Cyclic Redundancy Checks (CRC)*, (3) ~~data~~*

~~plausibility checks~~communication keep-alive signal, (4) watchdog timer status, (5) ~~voltage levels in control unit circuitry~~power supply status, (6) memory ~~(RAM and ROM)~~ checks, and (7) data range and bounds checks. ~~Hardware is provided prior to transmission and following reception to detect transmission errors at the Remote Multiplexing Units and the Control Room Multiplexing Units.~~ Self-~~test~~diagnostics will indicate faults to the module board replacement level.

~~Each multiplexing system has~~ The RDLC ECFs are implemented with dual communication channels for fault tolerance~~ and is provided with automatic reconfiguration and restart capability~~. A detected fault is automatically annunciated to the operator~~ at both the system and individual control station level. If one transmission loop is completely out of service, that will also be annunciated~~. Total shutdown of an ~~multiplexing system~~ RDLC ECF is indicated by a separate alarm~~; however, individual control stations are repairable online without taking the entire system down~~.

The above actions indicate conformance to Regulation Guide 1.47, Section C.1 (Automatic system level indication of bypass or deliberately induced inoperability).

~~After repair, the system automatically re-initializes to normal status when power is restored to any unit and automatically resets any alarms.~~ Power loss to any control station is separately monitored and annunciated to aid in troubleshooting and to alert the operator when power is ~~deliberately~~ removed from a unit when being serviced. Power loss will cause the fault or out-of-service alarms described previously to activate. This indicates conformance to Regulation Guide 1.47, Section C.2 [Automatic activation of indicating system of C.1 when auxiliary or supporting system (in this case, power source) is bypassed or deliberately rendered inoperable].

Bypassed or inoperable status of any one ~~multiplexing system~~ division of ECFs can not render inoperable any redundant portion of the protection system. Each ~~multiplexing system~~ division of ECFs is independent ~~in each division~~ of ECFs in the other divisions. Inoperable status in one division will cause the appropriate safe-state trips in that division, but the other divisions will continue to operate normally. Faults in another division simultaneously will indicate according to the previous discussion. The resulting safe-state trips will result in the required protective action. Thus, the requirements of Regulation Guide 1.47, Section C.3, are satisfied.

During periodic surveillance, the system-level out-of-service indicators can be tested manually. This satisfies the requirement of Regulation Guide 1.47, Section C.4.

NRC Request (15)—Provide an explicit discussion of the susceptibility of the multiplexer systems to electromagnetic interference.

Revised *Response (15)*—Multiplexers are not used, and there is no multiplexer system. Safety-related data communication is performed as an integral function of the SSLC systems. ~~Each~~The ~~control station of the multiplexer system either in the control room or in local areas is electrically powered and contains solid-state logic and, therefore, is potentially susceptible to the effects of EMI. However, the effects on the overall network are reduced because of the dual, fiber optic, data transmission network that is used between stations~~ELCS equipment is contained in EMI resistant

enclosures. Proper grounding and shielding practices are used. The lack of susceptibility of ELCS equipment is verified during qualification testing. Fiber optics are used to communicate with equipment external to the cabinet*. Fiber optics are not subject to induced electrical currents, eliminate ground loops, and also do not radiate electrical noise. Thus, the isolated and distributed nature of the system, which is also replicated in four divisions, tends to reduce EMI effects.*

Response (4) indicates several common techniques (shielding, grounding, etc.) used to minimize EMI in the electrical control circuitry. Proper physical placement, especially for the ~~Remote Multiplexing Units~~ I/O devices*, is essential to eliminate interference from high current or high voltage switching devices.*

~~Data checking software~~ Self-diagnostics *at the ~~RMUs~~* controllers *~~and in the control room at the Control Room Multiplexing Units~~ monitor~~s~~ data transmission to ensure that faults do not propagate into the safety protection logic. Bad data transmission will cause a system alarm~~, and, possibly, a system shutdown if the fault does not clear within defined time constraints~~.*

Response (4) also discusses various tests that the system will undergo to demonstrate immunity to EMI.

7A.3 Electrical Isolators

STD DEP T1 3.4-1 (Table 7A-1, Figure 7A-1)

NRC Request (1)*—For each type of device used to accomplish electrical isolation, provide a description of the testing to be performed to demonstrate that the device is acceptable for its application(s). Describe the test configuration and how the maximum credible faults applied to the devices will be included in the test instructions.*

Revised ***Response (1)****—This response is limited to fiber optic data links, which are the only type of isolation device used for electrical isolation of logic level and analog signals between protection divisions and from protection divisions to non-safety-related equipment.*

Testing is of two types:

(1) Optical characteristics

(2) Signal transmission capability

Optical characteristics are checked by an optical power meter and a hand-held light source to determine the optical loss from one end of the fiber optic cable to the other. In an operational system, an optical time domain reflectometer measures and displays optical loss along any continuous optical fiber path. Any abrupt disruption in the optical path such as a splice or connector is seen as a blip on the display. This technique is especially useful for troubleshooting long runs of cable such as ~~in the multiplexing system~~ those used to implement the DCFs*. Cable terminations are visually inspected under magnification to determine if cracks and flaws have appeared in the optical fiber surfaces within the connector.*

Transmission characteristics are ~~tested by bit generation. This test method determines bit error rate by generating a random stream of bits at the transmitter and verifying them at the receiver to determine the reliability of the fiber optics. Data rate is set at the maximum throughput required by the system. Proper transfer of analog signals is determined by analog-to-digital conversion of test signals at the transmitting end, and monitoring of the digital-to-analog conversion at the receiving end for linearity over the full scale range. Frequency of the test signals is set at the maximum required by the system.~~ monitored in the system by the self diagnostics.

Maximum credible electrical faults applied at the outputs of isolation devices do not apply to fiber optic systems. The maximum credible fault is cable breakage causing loss of signal transmission. Faults cannot cause propagation of electrical voltages and currents into other electrical circuitry at the transmitting or receiving ends. Conversely, electrical faults originating at the input to the fiber optic transmitter can only damage the local circuitry and cause loss or corruption of data transmission; damaging voltages and currents will not propagate to the receiving end.

***NRC Request (5)**—Provide a commitment that the isolation devices will comply with all environmental qualification and seismic qualification requirements.*

Revised ***Response (5)**—Fiber optic isolation devices are expected to have less difficulty than previous isolation devices in complying with all qualification requirements due to their small size, low mass, and simple electronic interfaces. The basic materials and components, except for the fiber optic cable itself, are the same as those used in existing, qualified isolation devices.*

A major advantage of fiber optics is that signals can be transmitted long distances and around curves through the isolating medium; thus, the physical, safety-class barrier required for separation of Class 1E devices may be provided by just the cable length if the protective covering and any fill materials of the cable are made properly flame-retardant. For short distances, the fiber optic cable can be fed through a standard safety class structure.

~~Details of the type of cable, transmitter, and receiver combinations that will provide optimum compliance with qualification requirements must await the guidance to be developed by the NRC staff/EG&G studies (see Section 4).~~

***NRC Request (7)**—Provide information to verify that the Class 1E isolation devices are powered from a Class 1E power source(s).*

Revised ***Response (7)**—~~When using fiber optic devices as Class 1E isolation devices, only the input side of the transmitting device and output side of the receiving device use electrical power. The low voltage power supplies for these devices use the same power source as the logic that drives the isolating device. For ABWR safety systems, this power is:~~*

~~(1) Divisional 120V Vital AC (UPS) For Reactor Protection System (RPS) logic and Main Steam Isolation Valve (MSIV) logic.~~

~~(2) 125V Plant DC Power Supply For ECCS logic and Leak Detection and Isolation System (LDS) logic.~~

Fiber optic cable is used for Class 1E isolation and does not use any electrical power to accomplish that function.]*

7A.5 ~~[Programmable Digital Computer Software†~~

~~**NRC Request** Provide a comparison of the design with the following:~~

~~**(1) [ANSI/IEEE-ANS-7.4.3.2, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations."]‡~~

~~(2) Regulatory Guide 1.152, "Criteria for Programmable Digital Computer System Software in Safety Related Systems of Nuclear Power Plants," November 1985~~

~~(3) NUREG-0308, "Safety Evaluation Report Arkansas Nuclear 1, Unit 2," November 1977~~

~~(4) NUREG-0493, "A Defense in Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," May 1985~~

~~(5) NUREG-0491, "Safety Evaluation Report of RESAR-414," February 1979~~

7A.6 ~~Programmable Digital Computer Hardware ƒ~~

~~**NRC Request** Provide a comparison of the design with the following:~~

~~(1) IEEE-603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"~~

~~(2) NUREG-0308, "Safety Evaluation Report Arkansas Nuclear 1, Unit 2," November 1977~~

~~(3) Regulatory Guide 1.153, "Criteria for Power, Instrumentation and Control Portions of Safety Systems"~~

~~(4) NUREG-0493, "A Defense in Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," May 1985~~

~~(5) NUREG-0491, "Safety Evaluation Report of RESAR-414," February 1979~~

---

* See Section 7.A.1(1).

† ~~Responses to Sections 7A.5 and 7A.6 above are grouped in various combinations, as appropriate, in Subsection 7A.7~~

‡ ~~See section 7A.1(2) and 7A.1(1).~~

ƒ ~~Responses to Sections 7A.5 and 7A.6 above are grouped in various combinations, as appropriate, in Subsection 7A.7~~

7A.7 Revised Responses to Subsections 7A.5 & 7A.6; Computer Hardware and Software

STD DEP T1 3.4-1 (Table 7A-1, Figure 7A-1)

STD DEP 7.1-1

Items 7A.5(3) and 7A.6(2)

The ABWR design of the Reactor Protection System utilizes ~~microprocessor~~ configurable logic *technology for logic decisions based on analog input from various sensors.~~ This philosophy is much the same as that of GESSAR II and the Clinton BWR, except in those designs, solid-state CMOS accepted digital signals from analog trip modules (ATM). In the ABWR design, the microprocessors perform the functions of both the CMOS and the ATM.~~*

The~~ important distinction is that the~~ ABWR uses a modern form of a *digital ~~computer~~ device ~~(i.e., microprocessors)~~ for the same reasons relays and solid-state devices were used in earlier designs (i.e., making simple logic decisions); not for making complex calculations for which protective action is dependent.*

Items 7A.5(4) and 7A.6(4)

The guidelines of NUREG-O493 have been used to perform analysis of several possible different configurations of the Safety System Logic and Control (SSLC) network. Analyses have been performed at the system design level to assure adequate defense-in-depth and/or diversity principles were incorporated at acceptable cost. It is recognized that such requirements are in addition to positions on safety-related protection systems (such as the single failure criterion) taken previously in other Regulatory Guides.

In order to reduce plant construction costs and simplify maintenance operation, the ABWR protection systems are designed with a partially *"shared sensors" concept. The ~~SSLC~~* RTIF System *is the central processing mechanism ~~and~~* that *produces logic decisions for both RPS and* MSIV isolation functions. The ELCS is the central processing mechanism that produces logic decisions for all *ESF safety system functions. Redundancy and "single failure" requirements are enhanced by a full four-division modular design using two-out-of-four voting logic on inputs derived from LOCA signals which consist of diverse parameters (i.e., reactor low level and high drywell pressure). Many additional signals are provided, in groups of four or more, to initiate RPS scram (Table 7.2-2).*

With its inherent advantages, it is also recognized that such design integration (i.e., shared sensors) theoretically escalates the effects of potential common-mode failures (CMF). Therefore, the architecture of the *SSLC System*s *~~architecture~~ is designed to provide maximum separation of system functions by using separate digital trip ~~modules~~* functions *(~~DTMs~~* DTFs*) and trip logic ~~units~~*functions *(~~TLUs~~*TLFs*) for RPS/MSIV logic processing and for LDS/ECCS logic processing within each of the four*

essential power divisions. Thus, setpoint comparisons within individual ~~DTMs~~ DTFs are associated with logically separate initiation tasks.

Sensor signals are sent to each ~~DTM~~ DTF on separate or redundant data links such that distribution of ~~DTM~~ DTF functions results in minimum interdependence between echelons of defense. For reactor level sensing, the RPS scram function utilizes narrow-range transmitters while the ECCS functions utilize the wide-range transmitters. The diverse high drywell signals are shared within the two-out- of-four voting logic. In addition, all automatic protective functions are backed up by manual controls. ~~These concepts are illustrated in Figure 7A-1.~~

~~As a general rule, shared sensors for protection systems are not used for control systems (i.e., feedwater, recirc, etc.). However, the end-of-cycle (EOC) recirc pump trip signals originate from the same turbine stop valve closure or turbine control valve fast closure sensors which contribute to scram. These are Class 1E sensors, but they are not shared with other protection systems and the interface with the recirc system is naturally isolated via fiber optic cable.~~

~~Another use for some of the protection shared signals involves the ATWS trip which activates the Fine Motion Control Rod Drive (FMCRD) run-in and alternate rod insertion (ARI) as diverse backup to hydraulic scram. However, this Class 1E-to-non-Class 1E isolated interface is a special case for mitigation of ATWS and is not a control system interface.~~

~~The ABWR demonstrates strong multi-system diversity in its capability to shut down and cool the reactor core. There are four distinct systems for controlling reactivity and four distinct systems for cooling the core.~~

~~Reactor Shutdown Systems~~

(1) ~~The RPS "failsafe" (i.e., scram on loss of power or data communications) hydraulic scram (Subsection 7.2.1.1.4).~~

(2) ~~The ATWS-mitigating DC-power-actuated air header dump valves (alternate rod insertion [ARI]) scram (Subsection 7.2.1.1.4.5).~~

(3) ~~The ATWS-mitigating rod run-in function utilizing fine-motion control rod drive (Subsection 7.7.1.2.2).~~

(4) ~~The Standby Liquid Control System (Subsection 7.4.1.2).~~

~~Reactor Core Cooling Systems~~

(1) ~~The Feedwater Control System (Subsection 7.7.1.4).~~

(2) ~~The High Pressure Core Flooder System (Subsection 7.3.1.1.1.1).~~

(3) ~~The turbine-driven Reactor Core Isolation Cooling System (Subsection 7.3.1.1.1.3).~~

(4) ~~The low pressure flooder mode of RHR (Subsection 7.3.1.1.4).~~

~~The Remote Shutdown System (RSS) also provides an independent means of actuating core cooling functions diverse from the plant main control room.~~

~~In summary, the ABWR design has incorporated defense-in-depth principles through maintaining separation of control and protection functions even though sensors are shared within protection systems. In addition, the shared sensors are designed within a full four division architecture with two-out-of-four voting logic.~~

~~Diversity principles are incorporated at both the signal and system levels: (1) diverse parameters are monitored to automatically initiate protective actions which are also manually controllable; and, (2) multiple diverse systems are available to both shut down the reactor and to cool its core.~~

~~Therefore, the ABWR fully meets the intent of NUREG-0493.~~

Items 6(1) and 6(3)

IEEE-603 has been reviewed, as has Regulatory Guide 1.153 which endorses IEEE-603.

The ~~microprocessor~~ hardware and software which make up the Safety System Logic and Control (SSLC) systems *is designed to make logic decisions which automatically initiate safety actions based on input from instrument monitored parameters for several nuclear safety systems. ~~As shown in Figure 7.1-2 of Section 7.1 and Figure 7A-1, the SSLC is not a nuclear safety system of itself, but is a means by which the nuclear safety systems accomplish their functions.~~ In that sense, the SSLC ~~is a component that~~* systems *integrate~~s~~ the nuclear safety systems.*

Most positions stated in IEEE-603 (as endorsed by RG 1.153) pertain to the nuclear safety systems, and are similar to those of IEEE-279, which are addressed for each system in the analysis sections of Chapter 7. Safety system design bases are described for all I&C systems in Section 7.1, beginning at Subsection 7.1.2.2. ~~Setpoints and margin may be found in Chapter 16~~ The methods for calculating setpoints and margins are described in the Bases for Chapter 16*.*

The safety system criteria in Section 5 and the functional and design requirements in Section 6 *of IEEE-603 are not compromised by the introduction of the SSLC. All positions regarding single-failure, completion of protective actions, etc., are designed into the protection systems. All SSLC components associated with the protection systems are Class 1E and are qualified to the same standards as the protection systems.*

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

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

* See Section 7A.1(1).

Table 7A-1 List of Equipment Interface with ~~*Essential MUX*~~ ECFs Signals (Typical)

Device	Div	Description
~~*U41-D107*~~	~~*3*~~	~~*FCS ROOM (A) HVH*~~
~~*U41-D108*~~	~~*2*~~	~~*FCS ROOM (B) HVH*~~