7C Defense Against Common-Mode Failure in Safety-Related, Software-Based I&C Systems

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

STD DEP T1 3.4-1 (Figure 7C-1)

STD DEP Admin

7C.1 Introduction

STD DEP T1 3.4-1

STD DEP Admin

As described in Chapter 7 ~~and Appendix 7A,~~ the ABWR Safety System Logic and Control (SSLC) and ~~Essential Multiplexing System (EMS)~~ Essential Communication Function (ECF) *designs use programmable digital equipment to implement operating functions of the interfacing safety systems. A controlled process for software development and implementation is employed to ensure that the highest quality software is produced. The development process for safety-related* configurable logic devices, and for safety-related *software and its integration into read-only memory (ROM) as firmware includes a formal verification and validation (V&V) program, which is described in ~~Appendices 7A and~~* Appendix 7B*. The V&V program, under control of the Software Management Plan, is applied to software that is developed for maximum reliability and efficiency, using a set of design techniques directed towards generating the simplest possible code to be used as firmware in dedicated, real-time microcontrollers*

Despite the use of simple, reliable software; formal V&V; and built-in self-diagnostics, there is a concern that software design faults or other initiating events common to redundant, multi-divisional logic channels could disable significant portions of the plant's automatic standby safety functions (the reactor protection system and engineered safety features systems) at the moment when these functions are needed to mitigate an accident. Mitigation of these common mode failures, as described in the following sections, is provided by the following diverse features:

(a) *Manual scram and isolation by the operator in the main control room in response to diverse parameter indications.*

(b) *Core makeup water capability from the diverse feedwater, CRD, and condensate systems.*

(c) *Availability of manual high pressure injection capability.*

(d) *Long term shutdown capability provided in a conventionally hardwired, 2-division, ~~analog~~ remote shutdown system* using a technology diverse from other safety systems*; local displays of process variables in RSS*

are continuously powered and so are available for monitoring at any time.

7C.2 [Design Techniques for Optimizing ABWR Safety-Related Hardware and Software

STD DEP T1 3.4-1

(c) *Microprocessors with minimal instruction sets and a simple operating system* and configurable logic devices with minimal instruction sets *are used. The "lost" computing power is not needed and the limited instructions minimize inadvertent programming and operational errors. This aids in verification and validation and further enhances reliability.*

7C.3 Defense Against Common-Mode Failure

STD DEP T1 3.4-1

A strong V&V program can reduce the probability of common mode failure to a very low level because the simple modules used in each division, although identical in some cases, can be thoroughly tested during the validation process. In addition to software V&V, however, SSLC contains several system level and functional level defenses against common mode failure, as follows:

(1) System Level Defenses Against Common Mode Failure

(a) Operational defenses

(i) Asynchronous operation of multiple protection divisions; timing signals are not exchanged among divisions

(ii) Automatic error checking on all ~~multiplexed~~ data *transmission paths. Only the last good data is used for logic processing unless a permanent fault is detected, thereby causing the channel to trip and alarm.*

The functional program logic in the SSLC controllers also provides protection against common mode failures, as follows:

(1) Functional Defenses Against Common Mode Software Failure

(c) ~~Multiplexing and other data~~ Data *transmission functions ~~use standard, open protocols that are verified to industry standards and~~ are ~~also~~ qualified to Class 1E standards*

7C.4 Common Mode Failure Analysis

STD DEP T1 3.4-1

JUNE, 1993

As of the week of June 7, 1993, the staff indicated that, with the addition of the hardwired HPCF manual control in the MCR, the issue of I&C diversity would be closed, pending the staff's final review of the results of the analyses that were re-done to incorporate manual HPCF initiation. Within the U.S. licensing material, manual HPCF Loop C initiation will be presented as a manual switch hardwired to a programmable logic controller (PLC) device that is independent of Safety System Logic and Control (SSLC) and the ~~Essential Multiplexing System (EMS)~~ Essential Communication Function (ECF)*. SSLC and ~~EMS~~* ECF *will continue to provide the automatic software-based initiation logic for HPCF Loop C [see reference 7C-6(7)].*

The SSLC design also uses hardwired control switches to perform manual system start of the other systems in ECCS. However, these switches are hardwired only from the operator's control station to the ~~microprocessor~~ logic in SSLC, where ~~EMS~~ ECF *then provides the transmission path for control signals from SSLC to the actuated devices. Control switch signals for individual control of pumps and valves are ~~multiplexed~~* transmitted *from the operator's control station to SSLC and then through ~~EMS~~* ECF *as stated above.*

7C.5 [Details of Final Implementation of Diversity in ABWR Protection System

STD DEP T1 3.4-1

To maintain protection system defense-in-depth in the presence of a postulated worst-case event (i.e., undetected, 4-division common mode failure of all communications or logic processing functions in conjunction with a large break LOCA), diversity is provided in the form of hardwired backup of reactor trip, diverse display of important process parameters, defense-in-depth arrangement of equipment, and other equipment diversity as outlined below (many of these features were included in the original protection system design; refer to Figure 7C-1 for details of how those additional diverse features, added as a result of the CMF analyses discussed in the previous section, have been implemented). Note that diverse equipment can be in the form of digital or non-digital devices as long as these devices are not subject to the same common mode failure as the primary protection system components:

(2) Defense-in-depth configuration:

(a) Fail-safe RPS and fail-as-is ESF in separate processing channels

(b) Control systems ~~supporting diverse injection~~ are independent of RPS and ESF in separate ~~triplicated processing network~~ communication functions *using diverse hardware and software from the ~~Essential Multiplexing System~~* Essential Communication Function (ECF) *network*

(3) Equipment diversity

(d) HPCF manual start in loop C (Division III) is implemented in equipment that is diverse from the automatic start function. All interconnections are hardwired and control and interlock logic is provided in the form of either

discrete logic gates or programmable logic that is diverse from the automatic start logic. The signal path of the manual logic is independent from that of the automatic logic up to the actuated device drivers (e.g., motor control centers or switchgear). The manual start function is not implemented in the automatic logic~~; however, the logic reset switch is common to both the automatic and manual logic~~. In addition to the manual start function, which performs all necessary control actions as a substitute for automatic start, other supporting hardwired functions are provided in loop C as follows:

(v) Remote shutdown system (~~analog~~ diverse, hardwired) provides shutdown cooling functions and continuous local display of monitored process parameters.

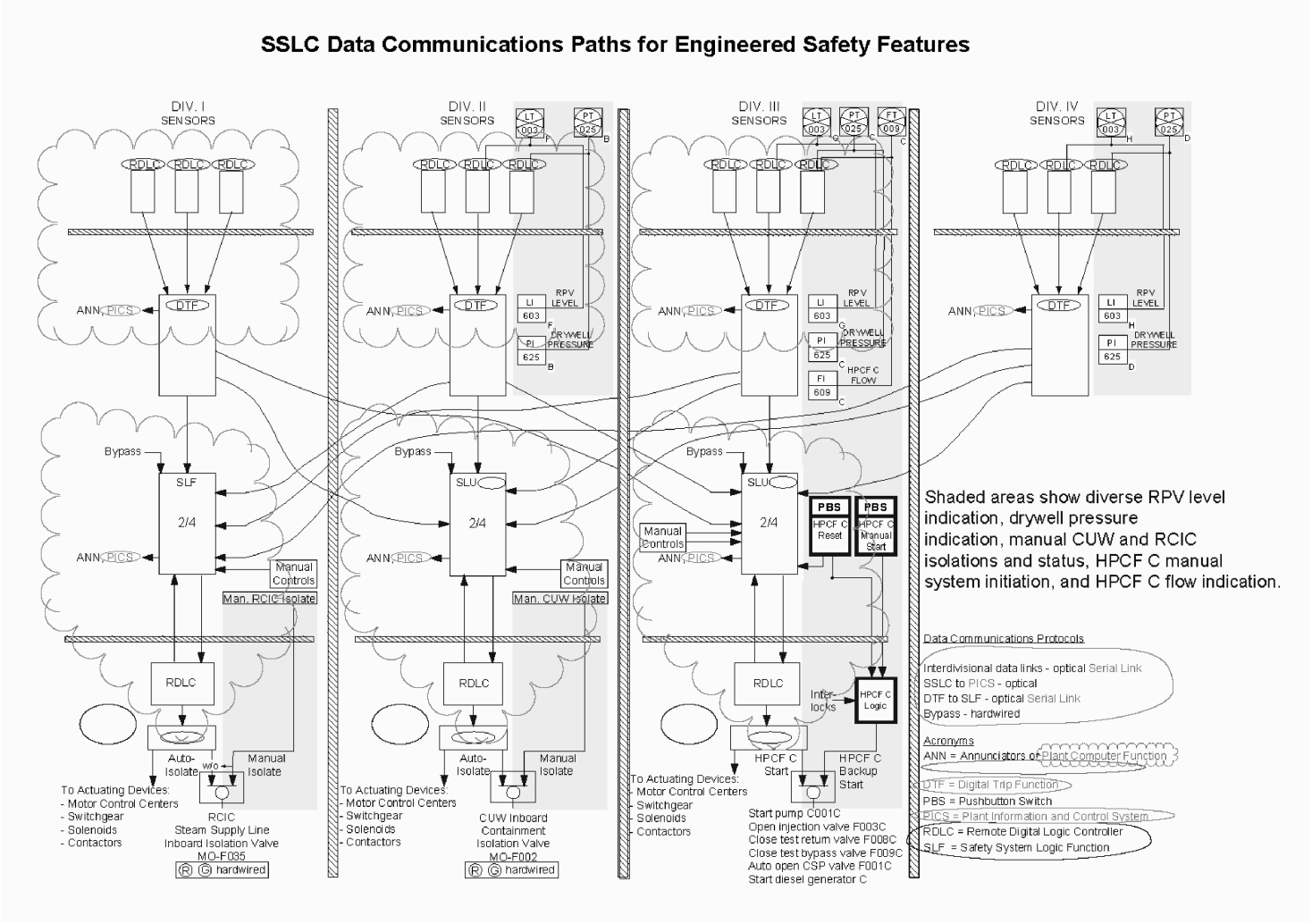

Figure 7C-1 Implementation of Additional Diversity in SSLC to Mitigate Effects of Common-Mode Failures