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

7C.1 Introduction

The key feature of successful electronic instrumentation design for the ABWR is the application of state-of-the-art design techniques to modern, proven components that can be easily qualified to the required regulatory guidelines.

This is particularly true for microprocessors. Most of the effort in newer designs has been to do more functions at the highest possible speeds, which requires complex hardware and associated complex software. However, safety system logic in the ABWR uses only simple gating and interlock functions and does not require processing of complex algorithms. These functions can be very effectively accomplished by simpler microprocessors or microcontrollers, where high reliability and hardware simplicity become the key objectives.

Consistent with this philosophy is the use of state-of-the-art program design methods to achieve highly reliable software. These methods use simple data structures and modular, top-down programming to produce easily verifiable and testable programs that provide predictable performance.

This simplicity does not sacrifice the requirements for high speed data flow, fast time response, and good error detection, since modern microprocessors and microcontrollers fully support these requirements.

As described in Chapter 7 the ABWR Safety System Logic and Control (SSLC) and 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 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, 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.

Note that random failures are mitigated by the divisional sensor channel and output trip channel bypass capability of SSLC. Either bypass places the remaining divisions in a 2-out-of-3 coincident logic condition such that another failure in a remaining division will not disable system operation.

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

Before considering methods used to protect against common mode failure, several techniques that are employed to ensure system reliability by minimizing both random and common mode failure probabilities are outlined below:

(a) Design of self-test, surveillance, and calibration functions are performed as part of the initial design. These functions cannot successfully be added on to the basic functional hardware.

(b) The total amount of hardware is minimized to assure highest reliability.

(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.

(d) The highest quality, high precision components are used to gain reliability. Designs with these components minimize manual calibration, simplify reliability analysis, and maximize surveillance intervals.

(e) To improve maintainability, self-diagnostics are implemented to locate any problem to a single assembly.

(f) The man-machine interface is implemented such that the equipment is structured into small units, with enough diagnostics so that a user can repair equipment by replacing modules and can operate the equipment by following straightforward instructions.

(g) The software design process specifies modular code

(h) Modules have one entry and one exit point and are written using a limited number of program constructs, as specified by **[*DOD-STD-2167*]** *

(i) Code is segmented by system and function

(i) Program code for each safety system resides in independent modules which perform setpoint comparison, voting, and interlock logic

(ii) Code for calibration, signal I/O, self-diagnostics, and graphical displays is common to all systems

(iii) Fixed message formats are used for plant sensor data, equipment activation data and diagnostic data. Thus, corrupted messages are readily detected by error-detecting software in each digital instrument.

(j) Software design uses recognized defensive programming techniques, backed up by self-diagnostic software and hardware watchdog monitors

(k) A full-scope operating system is not used. The operating system for each instrument is a small, real-time kernel customized to perform only the required scheduling functions

(l) Software for control programs is permanently embedded as firmware in controller ROMs

(m) Commercial development tools and languages with a known history of successful applications in similar designs are used for software development.

(n) Automated software tools are used to aid in verification and validation

The most important factor, however, in implementing reliable software is the quality of the design and requirements specifications. These documents are also controlled under the formal V&V program.

7C.3 Defense Against Common-Mode Failure

SSLC performs several simple, repetitive tasks continuously and simultaneously in four independent and redundant divisions of logic: setpoint comparison, 2-out-of-4 voting logic,

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

interlock logic, I/O, and self-test. As a practical matter, the development of common software modules for many of these functions has several advantages in producing reliable programs:

(a) Promotes standardization and code reusability

(b) Minimizes program design errors

(c) Minimizes timing differences among channels

(d) Reduces software life cycle cost

(i) Simplifies verification

(ii) Reduces maintenance costs

(iii) Simplifies future changes

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 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.

(iii) Daily operator cross-check of redundant sensor inputs, in addition to automatic cross-checking

(iv) Quarterly surveillance of trip functions (on-line with division bypass capability)

(v) Continuous self-test with alarm outputs in all system devices

(b) Functional Defenses

(i) Instantaneous, simultaneous, and undetected failure on a common mode error is unlikely

(ii) Automatic error detection permits graceful shutdown

(iii) Separation and independence protect against global effects (EMI, thermal, etc.)

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

(a) Control programs are not completely identical in each division

(i) Interlock logic for ESF pumps and valves varies in each division

(ii) Each division has different quantities and types of inputs and outputs

(iii) Redundant sensors have data messages with unique identifications and time-tags in each division

(b) Modules that are identical are simple functions such as setpoint comparison and 2-out-of-4 voting that can be readily verified

(c) Data transmission functions are qualified to Class 1E standards

Due to this extensive diversity that exists at the protection system and plant levels, the use of hardware and software diversity among the redundant channels of the protection system was not considered practical for the following reasons:

(1) Diverse software is more error prone during development and does not guarantee that the resulting system will be error-free

(2) Diverse hardware and software increases V&V and system integration costs

(3) The different types of hardware increases spares inventory

(4) Maintenance and surveillance require more time and attention because the diverse equipment may perform differently

(5) System revision costs are prohibitive because of additional V&V and documentation

(6) Performance of redundant channels may not be consistent]*

7C.4 Common Mode Failure Analysis

JANUARY, 1988 THROUGH SEPTEMBER, 1991

As part of the initial efforts to support the licensing of the ABWR design in the U.S., GE provided the NRC staff with the results of evaluations demonstrating that the probability of a common-cause failure leading to the inability of the Safety System Logic and Control (SSLC) equipment to perform its safety functions was extremely low and, therefore, did not need to be considered further in the licensing process. These analyses considered the defined SSLC configuration (e.g., 2-out-of-4 safety system logic and segmentation of functions performed

* See Section 7A.1(1).

with the multiple microprocessors of a safety division), system functions (e.g., automated self-test), and qualification of the equipment to the applicable standards (e.g., hardware qualification and software verification and validation (V&V).

During this initial period of ABWR design certification activities, the NRC staff was striving internally to define the methods that they should use to review and evaluate the acceptability of broad scope digital-based safety systems such as those which are incorporated into the ABWR design. Although the staff had some experience in reviewing and licensing individual systems and components that used advanced digital technologies (e.g., GE's NUMAC family of products), they had no experience in the review of broad scope integrated digital systems such as the SSLC design. In addition, the staff's past practice for the review of digital-based equipment was to review the actual implemented equipment hardware and software. For the ABWR design certification, the scope of their review specifically excluded the review of any particular implementation of equipment and, as a consequence, the NRC staff had no precedents to guide them in their review of ABWR licensing submittals regarding digital safety systems.

With the issuance of NRC paper SECY 91-292 (September 16, 1991), the staff indicated that they would require some type of I&C diversity in those plants that chose to implement broad scope digital systems in safety-related applications. The formal rationale presented by the staff indicated that the incorporation of such I&C diversity would provide additional "defense-in-depth" and that such an approach was already being taken in other countries (e.g., France).

OCTOBER, 1991

The NRC staff contracted with Lawrence Livermore National Laboratory (LLNL) to perform a "worst-case" common-mode failure (CMF) analysis of ABWR digital safety systems. LLNL defined "worst-case" to be an undetected, simultaneous, 4-division failure such that all safety actions are inhibited at the time that these actions are required by the coincident occurrence of a design basis event (accident or transient). The methodology to be used would be based on NUREG-0493 (1979).

MARCH, 1992

LLNL provided their first results to the NRC in March of 1992. Based upon the LLNL work, the staff formulated a position which included the requirement that "a set of safety grade displays and manual controls, independent of the computer system(s) and located in the main control room, shall be provided for system-level actuation and monitoring of critical safety function parameters..." and that "the displays and manual controls shall be conventionally hardwired to as low a level in the system architecture as possible." [See reference 7C-6(2) for the final version of the LLNL report.]

MAY, 1992

GE responded with arguments to the staff that the LLNL analyses were based upon entirely incredible CMF sequences and, in addition, the analyses did not correctly reflect operator manual actions, the diverse capability of the Remote Shutdown System (RSS), or the operation of non-safety grade systems. In discussions with the staff, all of GE's arguments were accepted with the exception that the staff maintained the position that, for these evaluations of digital safety systems, the "worst-case" CMF sequences, like those modeled by LLNL, should be used as the basis of evaluation. GE committed to re-perform the basic analyses previously completed by LLNL using the following bases, in concurrence with the staff:

- The analyses presented in Chapter 15 of Tier 2 would be re-done with the modeling assumption that a worst-case postulated CMF of the digital safety systems would be considered concurrently with each of the individual design basis events.
- The analyses would be done using "realistic" modeling as opposed to standard "licensing basis" modeling, which can have significant additional margin inherent in the modeling.
- The analyses could take credit for non-safety controls and instrumentation if that equipment was independent of the postulated CMF in the digital safety systems.
- The analyses could take credit for operator actions at the RSS after one hour, but prior to that one hour period, all operator actions would be limited to those which could be performed in the main control room, using equipment that was independent of the postulated CMF.

JUNE, 1992

GE completed the evaluations and provided the results to the NRC staff. The evaluations took credit for the control room operation of the feedwater system and CRD hydraulic system to maintain RPV water level, and the use of a small set of "hardwired" displays and controls in the main control room for the purpose of the scram and containment isolation functions, which need to be accomplished in a relatively short time (i.e., at least within the first hour of the postulated event scenarios considered). To demonstrate that at least one hour of operation from only the control room was achievable, three of the most limiting scenarios were evaluated in detail, and the analyses were terminated after two hours of the scenario had been evaluated. The results of those evaluations (which were performed using the SAFR computer code) showed that even in the case where all operator actions are confined to just the control room, the fuel peak clad temperature (PCT) could be maintained at less than 1204°C such that no additional hardwired functions beyond the small set considered in the analyses were needed. That small set of "hardwired" control and display functions was as follows:

CONTROLS

- Manual scram (included in standard design)
- Manual MSIV control (included in standard design)

- CUW line inboard isolation valve manual initiation (for CUW LOCA outside the primary containment)
- RCIC steamline inboard isolation valve manual initiation (for RCIC steam line break outside the primary containment)

DISPLAYS

- RPV water level
- RPV water level 3 alarm
- Drywell pressure
- Drywell pressure high alarm
- CUW line inboard isolation valve status
- RCIC steamline inboard isolation valve status
- MSIV status

Also in June of 1992, top GENE management met with the NRC commissioners and presented GE's position that the ABWR design already included adequate diversity and that the NRC staff's approach to requiring significant "hardwired" functions in the main control room was not technically justified.

SEPTEMBER, 1992

In a letter to the chairman of the NRC [see reference 7C-6(3)], the Advisory Committee on Reactor Safeguards (ACRS) rejected the NRC staff's position regarding the requirement for hardwired backup for the digital safety systems in the main control room (MCR). The ACRS position, which was consistent with the position that had been taken by GE and others in the nuclear industry, was that there are many potentially acceptable methods of implementing diversity that could be used to mitigate postulated CMF of digital safety systems, and, thus, the NRC staff position which specifically required hardwired functions in the MCR was not technically justified.

OCTOBER, 1992

The staff modified its position on hardwired functions [see reference 7C-6(4)] and acknowledged that other methods (including diverse digital equipment) could be used to satisfy their requirement for mitigating postulated CMF of digital safety systems.

DECEMBER, 1992

The staff released the draft Final Safety Evaluation Report (FSER) on the ABWR. In that document, the staff presented their new list of diverse MCR displays and controls required for the ABWR. That list was essentially the same as the list developed by GE (see above) with one exception: The staff still required diverse HPCF manual initiation and flow indication in the MCR. In addition, the staff required that the feedwater system (FWS) be designed and tested to demonstrate high reliability. The rationale that the staff presented for requiring these additional diverse functions and capabilities was that, although the analyses submitted by GE in June 1992 had frequently taken credit for the operation of the FWS, the staff felt uncomfortable with placing such reliance on that system because past experience with single channel analog feedwater control system performance in U.S. plants had not been good.

JANUARY, 1993

In a meeting with the NRC staff, GE discussed the staff position presented in their draft FSER. GE argued that since the ABWR had incorporated a triplicated fault-tolerant architecture for the feedwater control system (FWCS), the reliability of feedwater control was significantly improved over past single-channel analog systems. The staff countered that, if GE was going to take credit for the feedwater system in the I&C common-mode failure analyses, they would then require that the FWCS be essentially designed and tested as though it were a safety-related system. In addition, the staff would still require that at least one division of HPCF manual initiation be provided in the MCR as redundant backup to the feedwater system.

During the January 1993 discussions, GE provided the staff with the results of new analyses that had been performed with the additional modeling assumption that the FWCS was assumed to have failed concurrent with the postulated initiating design basis event and the postulated worst-case CMF of the digital safety systems. In those analyses, only the operation of the CRD hydraulic system and the condensate system from the MCR were considered for the first two hours of the event. The results were still less than the 1204°C PCT limit. These analyses were used to demonstrate that even if the FWCS was assumed to have failed, there would still be adequate capability in the MCR (without hardwired manual HPCF initiation) to support operator actions to maintain the reactor in a safe condition and provide sufficient time for an operator to move to the remote shutdown system to initiate core make-up systems from that location. The staff accepted these arguments and agreed that the requirements they had proposed regarding FWCS reliability and HPCF manual initiation capability could be deleted. However, the staff requested that three additional design basis events be evaluated using the same type of modeling assumptions, including the postulated concurrent failure of the FWCS. Together with the previous analyses, these additional evaluations would comprise a bounding set of Chapter 15 events regarding the consequences of common mode failure on the digital protection system.

FEBRUARY, 1993

GE submitted to the staff the results of the three additional analyses [see reference 7C-6(5)]. All results were again less than the defined 1204°C PCT limit.

MARCH, 1993

The staff contacted GE to discuss some questions they had regarding the analyses previously provided by GE. The analyses included consideration of actions that would be taken by the operators in the MCR during the postulated events. These operator actions were defined based upon the ABWR Emergency Procedure Guidelines; the timing of these assumed operator actions was supported by operator performance test data from training simulators. The question raised by the Human Factors Branch of the NRC staff was basically: "How sensitive are the results of the GE analyses to the timing of the assumed operator actions?" More specifically, as an example, GE's analyses modeled that the operator would initiate condensate system operation within 5 minutes after the RPV water level dropped below level 2. The NRC staff's question was: "After how much longer would the analysis results still be acceptable?" GE agreed to re-perform the three most limiting analyses with the objective of trying to determine how long the operator could wait to take his first action. With the time margin for operator action quantified, and assuming this margin was sufficient, the staff agreed that the issue of I&C diversity would finally be closed with GE's incorporation of the small set of MCR displays and controls presented above.

These final analyses were performed using the TRAC computer code. TRAC was used instead of the SAFR code employed in the previous analyses because the additional modeling assumption of a delayed operator action time causes a longer period of operation with a depressed RPV water level; the TRAC code was considered to do a better job of modeling these conditions. Note that the SAFR code is an approved Level 2 code for the performance of Design Basis LOCA analyses in which the ECCS initiates automatically and the period of core uncovery nominally lasts no longer than about 100 seconds. However, in these special analyses, the period of core uncovery would last for 1000 seconds or more and, therefore, were beyond the scope of the existing SAFR code qualification. During the conduct of these evaluations using the TRAC code, it was determined that the previous analytical results obtained with the SAFR code were not correct and were non-conservative. Upon realization that the previous results were invalid, the entire set of six events previously analyzed in June 1992 were re-analyzed. The results of these TRAC analyses showed that the CRD hydraulic system and condensate system alone were not adequate to maintain the core within the 1204°C limit under the conditions postulated in those analyses. In order to maintain the core within the 1204°C limit for these postulated event scenarios, it was necessary to take credit for operation of one division of HPCF [see reference 7C-6(6)].

MAY, 1993

GE advised the staff that manual control of HPCF Loop C (Division III) and the display of HPCF Loop C flow would be added to the list presented above of hardwired displays and controls provided in the MCR. (Manual control of HPCF Loop B (Division II), with local display, is already provided at the RSS.)

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 Communication Function (ECF). SSLC and 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 logic in SSLC, where 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 transmitted from the operator's control station to SSLC and then through ECF as stated above.

JULY, 1993

The final NRC staff position on I&C diversity is stated in NRC document SECY-93-087, Section II.Q. This position has been approved by the NRC commissioners, with minor changes, in item 18 of a staff requirements memorandum (SRM), dated July 15, 1993. GE's design for safety-related I&C, as described in the above chronology and discussed in detail in the following section, fully meets the staff requirements.

7C.5 [DETAILS OF FINAL IMPLEMENTATION OF DIVERSITY IN ABWR PROTECTION SYSTEM

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:

(1) Protection system diversity

(a) Manual, hardwired, two-button scram

(b) Manual division trip via diverse, non-microprocessor logic

(c) Scram when reactor mode switch is placed in shutdown (hardwired)

(d) Manual MSIV closure (hardwired)

(e) ATWS mitigation [Alternate Rod Insertion (ARI) and FMCRD run-in, ADS inhibit, automatic Standby Liquid Control System initiation and feedwater runback] (hardwired and diverse digital system)

(2) Defense-in-depth configuration:

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

(b) Control systems are independent of RPS and ESF in separate communication functions using diverse hardware and software from the Essential Communication Function (ECF) network

(3) Equipment diversity

(a) Output logic units use discrete gate logic and provide trip seal-in and reset, division bypass, and manual trip functions

(b) The operator is provided with a set of diverse displays separate from those supplied through the safety-related, software-based logic. The displays listed below provide independent confirmation of the status of major process parameters:

(i) RPV water level

(ii) RPV water level 3 alarm

(iii) Drywell pressure

(iv) Drywell pressure high alarm

(v) CUW isolation valve status

(vi) RCIC steam line isolation valve status

(vii) HPCF flow

(c) Two containment isolation functions implemented with hardwired controls from the control room are also provided:

(i) CUW line inboard isolation valve manual initiation (for CUW LOCA outside the primary containment)

(ii) RCIC steam line inboard isolation valve manual initiation (for RCIC steam line break outside the primary containment)

(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. 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:

(i) Suction source selection

(ii) Manual open/close valve control of suppression pool suction valve F006

(iii) Manual open/close valve control of condensate storage pool suction valve F001

(iv) RPV level control

(1) Manual open/close valve control of injection valve F003

(2) Automatic minimum flow valve operation (F010)

(3) Hardwired thermal relay bypass logic

(4) Alarms and indicator lights for diverse logic status

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

If the protection system is disabled because of common mode failure, the operator is expected to enter the emergency operating procedures at the appropriate points as determined by the indications on the hardwired backup displays and manipulate the control functions described above.

Additional diversity is available at the plant level even if SSLC is disabled because of common mode failure. The same common mode failure would not be expected to affect the feedwater control system, which, although not safety-related, is operated by a highly reliable, triplicated fault-tolerant control system that is diverse in both hardware and software from the safety systems. Similarly, makeup water is also available from CRD purge flow and condensate pumps. These additional sources of water will generally mitigate all Chapter 15 events, as discussed in the analyses described in section 7C.4 above; however, a channel of manually-initiated HPCF, as shown in item (4) above, has been added to meet worst-case conditions.]*

7C.6 References

(1) Not Used

* See Section 7A.1(1).

(2) J. Palomar, et al., "A Defense-in-Depth and Diversity Assessment of the GE ABWR Instrumentation and Control Systems, Version 3", UCRL-ID-114000, Lawrence Livermore National Laboratory, April 30, 1993.

(3) Letter, David A. Ward to Ivan Selin, "Digital Instrumentation and Control System Reliability", NRC, Sept. 16, 1992.

(4) Letter, James M. Taylor to David A. Ward, "Defense Against Common Mode Failures in Digital Instrumentation and Control (I&C) Systems", NRC, Oct. 23, 1992.

(5) Letter, J. Fox to C. Poslusny, "Submittal Supporting Accelerated ABWR Review Schedule-I&C Diversity", Docket No. STN 52-001, Feb. 26, 1993.

(6) Letter, J. Fox to C. Poslusny, "Submittal Supporting Accelerated ABWR Review Schedule-I&C Diversity Issue, DFSER Open Item 7.2.6-2", Docket No. STN 52-001, June 18, 1993.

(7) Letter, J. Fox to C. Poslusny, "Submittal Supporting Accelerated ABWR Review Schedule-I&C Diversity (Issue #46)", Docket No. STN 52-001, July 9, 1993.

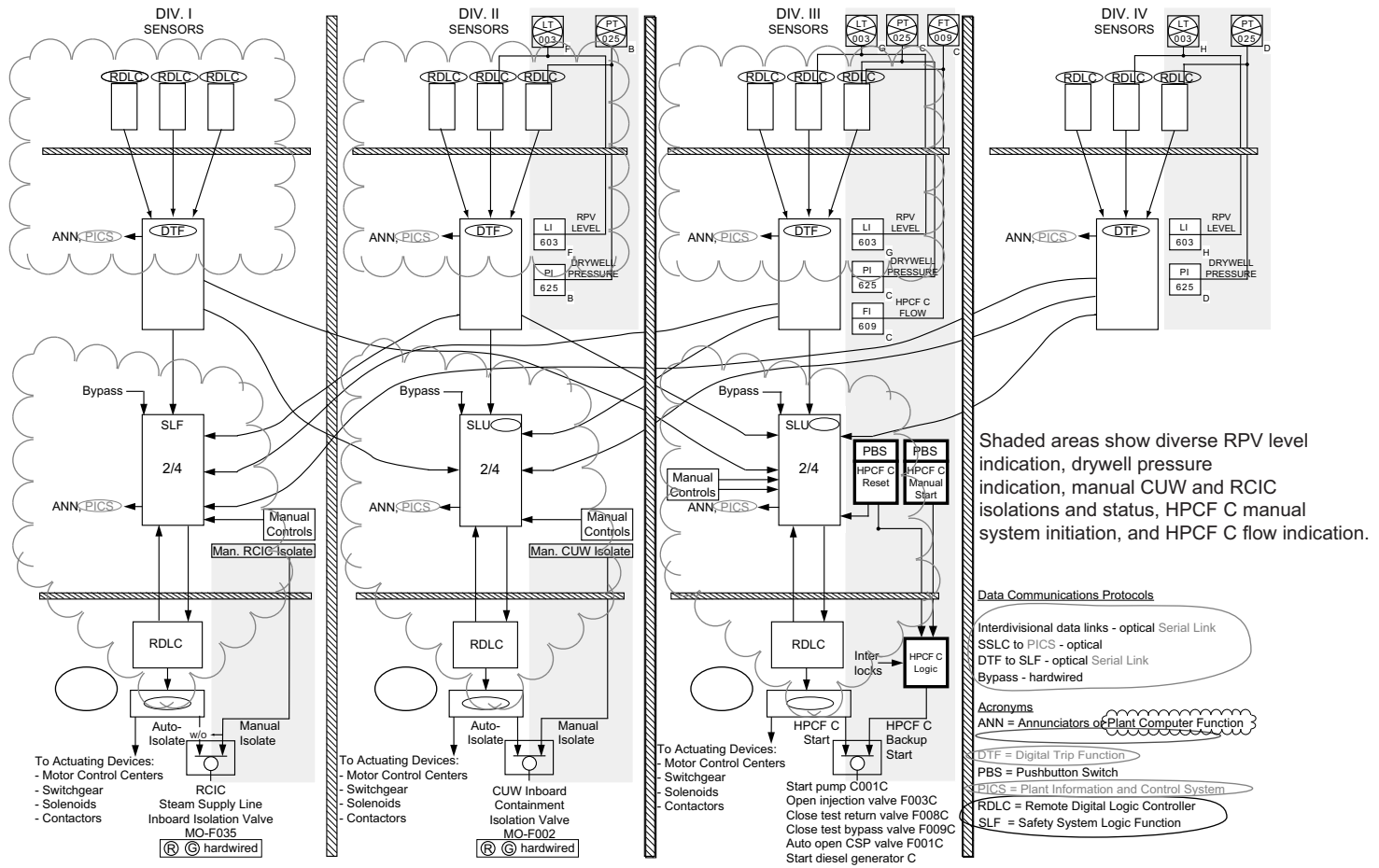

Figure 7C-1 Implementation of Additional Diversity in SSLC to Mitigate Effects of Common-Mode Failures